



**DESIGN DEVELOPMENT AND EVALUATION OF THE CYBERSECURITY RISK  
TOOL: A CASE OF SMALL AND MEDIUM-SIZED ENTERPRISES IN SOUTH  
AFRICA**

**By**

**TABISA NCUBUKEZI 208217673**

**Thesis submitted in fulfilment of the requirements for the degree**

**Doctor of Engineering in Electrical Engineering**

**in the Faculty of Engineering and the Built Environment**

**at the Cape Peninsula University of Technology**

**Supervisor:** Dr. L. Mwansa

**Co-supervisor:** Prof. F. Rocaries

**Bellville**  
July 2023

**CPUT copyright information**

The dissertation/thesis may not be published either in part (in scholarly, scientific or technical journals), or as a whole (as a monograph), unless permission has been obtained from the University

## DECLARATION

I, Tabisa Ncubekezi, declare that the contents of this thesis represent my own unaided work and that the dissertation/thesis has not previously been submitted for academic examination towards any qualification. Furthermore, it represents my own opinions and not necessarily those of the Cape Peninsula University of Technology.



---

**Signed**

**July 2023**

---

**Date**

## ABSTRACT

The increased convenient use and the openness of cyberspace increased cyberrisks in all institutions. The cybercriminals use innovative ways to gain unauthorised access to systems and leave them vulnerable to cyberthreats and cyberattacks. The common cyberthreats range from intrusion, ransomware, fraud, unauthorized access and modification of information, malicious codes, and denial of service. The exposure of small and medium-sized enterprises (SME) to these cyber attacks compromises business and information systems. When cyber attacks materialize they pose risks that impact SME's business continuity client trust, economic growth and performance. This study designed, developed and evaluated cyberrisk tools for SMEs in South Africa using AgenaRisk package with artificial intelligence (AI) capabilities through the Bayesian network tools.

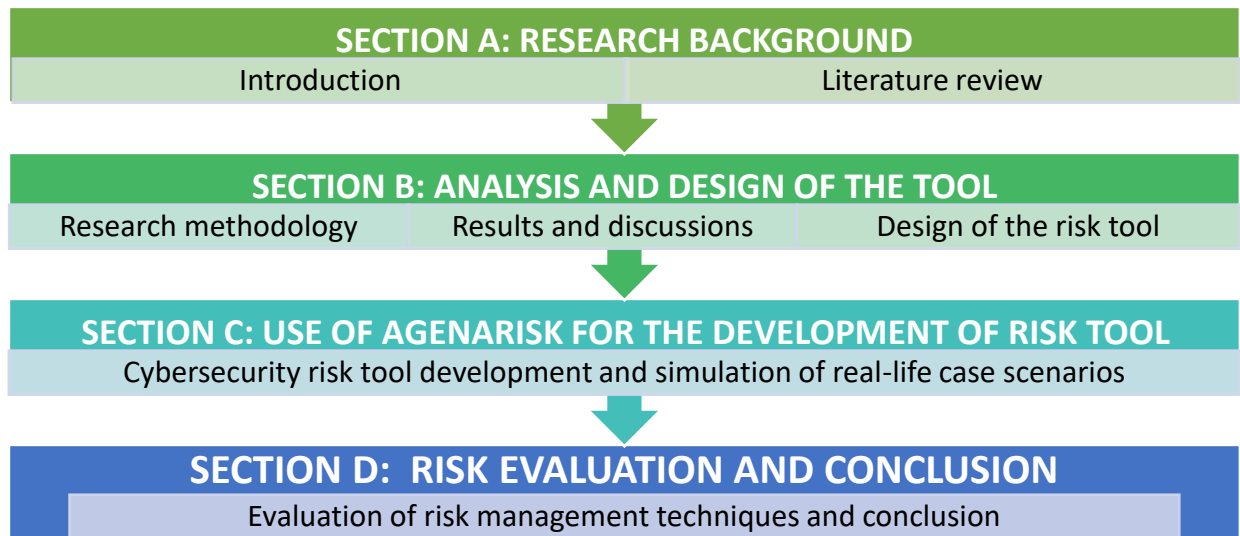
Within the qualitative approach, the study purposive sampling to select 45 respondents (females and males) from the businesses that operated during the Covid-19 pandemic. Data were collected using a questionnaire deployed in Google Forms. The research gathered qualitative and quantitative data about the existing cybersecurity risks, their impact, likelihood and current protection measures. The collected data were analysed and interpreted using thematic analysis and descriptive statistics. In addition, the study used quantitative risk assessment using the modelling and analytical techniques to perform sensitivity analysis, scenario analysis, Tornado graphs, decision trees, and expected monetary value. Lastly, the work adopted the NIST framework to align with the existing cybersecurity controls to improve cybersecurity, employee awareness, and training, aiding the extensive implementation of cybersecurity.

The results indicated that all small businesses have been affected by different cyberthreats and cyberattacks that compromise the entire information systems resulting in cyberrisks. Some risks are planned and some are unplanned. Even though some SMEs implemented mitigation measures, the extent of their usage and implementation still needs to be improved. Simulated cases demonstrated different threat levels, which ultimately led to unauthorised information being accessed. These different cases act as a clear guide showing the threat level, its impact and the risk likelihood. The framework shared insights about cybersecurity risk management and highlighted the strategies to promote the use of cyberspace and improve secure surfing. The developed risk tool illustrated the risk likelihood and the risk impact based on the key dependent and independent variables, prior indicators, as well as posterior indicators. Cyberrisk models demonstrated possible risks that SMEs are exposed to, different connected variables that determined the risk likelihood of the uncertain variables and the risk impact.

Recommendations to improve the state of cybersecurity in the context of SMEs were made, followed by suggestions for future work and a conclusion.

## THESIS STRUCTURE AND SUMMARY

This work is divided into four sections as shown in the figure below.



### SECTION A: INTRODUCTION AND THE BACKGROUND

This section consists of two chapters which are the introductory and the literature review chapter. The introductory chapter presented the research problem, the study's primary aim, and objectives, followed by the research questions, conceptual model, rationale, the significance of the study, the delineation section, and concluding remarks. Chapter 2 reviewed the current and relevant literature to identify the gap in the research problem statement.

### SECTION B: ANALYSIS AND DESIGN OF THE TOOL

This section consists of three chapters that presented the research methodology, analysis of the results, design of the risk tool based on the NIST framework, and AgenaRisk package.

### SECTION C: DEVELOPMENT OF THE TOOL

This section covers Chapter 6 which developed the risk tool using the AgenaRisk package. The chapter also demonstrated the simulated case scenarios that showed the connections between the nodes that link to interdependent variables to illustrate the risk likelihood and impact.

### SECTION D: EVALUATION AND DISCUSSION OF THE TOOL

In this section, there is Chapter 7 and Chapter 8. Chapter 7 evaluated cyberrisks using the risk management processes based on the ISO 31000:2018 standard. The seven risk management phases include communication and consultation, establishing the context, risk analysis and evaluation, risk treatment, monitoring and reviews, and reporting, and these were accounted for. The last chapter reviewed the research objectives concerning the results, reflecting on the researcher's experience during the data collection, followed by the research contribution, future research, and recommendations. This chapter is followed by the list of references used in the study and the appendices.

## ACKNOWLEDGEMENTS

### **I would like to thank and acknowledge:**

- Our Father in Heaven, the Lord Almighty God, for the ability to withstand the journey to complete my studies, even at a point when it seemed that all hope was lost.
- My mom Nozipho and my late dad, Zimasile Ncubukezi. Enkosi bazali, for your continued motivation over the years. Your prayers were never in vain, and your teachings have shaped us. How I wish Dad were still alive to see this milestone.
- Ntombekhaya, Babalwa, Lungile, Mbuzeli, Mpendulo, and Anati, for their unwavering support.
- Sammy for his unwavering support and encouragement to do more. You have made this journey possible. “Enkosi ngento yonke”, which translates as thank you so much for everything.
- Doctor Laban Mwansa for his expertise, guidance, and continued support in developing this work.
- Professor Francois Rocaries for his willingness to supervise, guide, and provide constructive criticism during the development of this work.
- Doctor Angus Brandt and Mr. Vusumzi Moyo for managing and working on the administration system.
- Academic Doctorate Advancement Programme Towards Transformation (ADAPTT) for the support, writing retreat opportunities, and connecting me with other fellow academics from different universities. However, all opinions presented in this study are those of the author and are not attributed to ADAPTT.
- IT departmental head, Doctor Kabaso, and colleagues, especially in the Comnet domain.
- Mr. Martin Mandioma and Mr. Xolisa Piyose for their continued support and encouragement in this journey.
- National Research Foundation (NRF) 2020-2022: Black Academics Advancement Programme (BAAP) Sabbatical Grant for supporting my research project. However, all opinions presented in this study are those of the author and are not attributed to NRF.

## **DEDICATION**

I dedicate this work to Bongeka, Lereko, and Larona Ncubekezi.

# TABLE OF CONTENTS

DECLARATION .....	ii
ABSTRACT .....	iii
THESIS STRUCTURE AND SUMMARY .....	iv
ACKNOWLEDGEMENTS .....	v
DEDICATION .....	vi
TABLE OF CONTENTS.....	vii
GLOSSARY.....	xii
CLARIFICATION OF TERMS .....	xiii
PUBLICATIONS DURING THE STUDY.....	xiv
SECTION A: RESEARCH BACKGROUND.....	xv
CHAPTER 1: INTRODUCTION AND BACKGROUND .....	1
1.1 INTRODUCTION .....	1
1.2 BACKGROUND TO THE PROBLEM .....	5
1.3 A CONCEPTUAL MODEL AS A TOOL.....	8
1.4 RATIONALE.....	9
1.5 SIGNIFICANCE.....	10
1.6 DELINEATION OF THE STUDY .....	10
1.7 CONCLUSION .....	11
CHAPTER 2: LITERATURE REVIEW .....	12
2.1 INTRODUCTION .....	12
2.2 SMALL AND MEDIUM-SIZED ENTERPRISES.....	12
2.3 CYBERSPACE .....	13
2.4 RISK OVERVIEW .....	19
2.5 SMEs' PERCEPTION OF CYBERRISKS .....	24
2.6 CYBERCRIMES .....	25
2.7 CYBERRISK MANAGEMENT FACTORS IN SMES .....	27
2.8 IMPACT OF CYBERRISKS IN THE BUSINESS SECTOR.....	28
2.9 SECURITY MEASURES.....	30
2.10 CONCLUSION .....	31
SECTION B: ANALYSIS AND DESIGN .....	32
CHAPTER 3: RESEARCH METHODOLOGY.....	33
3.1 INTRODUCTION .....	33
3.2 SCOPE OF THE STUDY .....	33
3.3 RESEARCH PHILOSOPHY AND DESIGN .....	33
3.4 RISK ASSESSMENT .....	39
3.5 RELIABILITY AND VALIDITY .....	41
3.6 DATA STORAGE AND MANAGEMENT .....	41
3.7 ETHICAL CONSIDERATIONS.....	42
3.8 CONCLUSION .....	43
CHAPTER 4: RESULTS AND DISCUSSIONS .....	44
4.1 INTRODUCTION .....	44
4.2 SOURCES OF DATA.....	44
4.3 DATA ANALYSIS.....	44
4.4 RESULTS .....	45
4.5 DISCUSSION AND IMPLICATIONS .....	54
4.6 NIST FRAMEWORK RELEVANCE IN MANAGING CYBERSECURITY RISKS .....	59
4.7 APPLICATION OF RISK MANAGEMENT STANDARD.....	60
4.8 ADOPTION OF AGENARISK PACKAGE.....	61
4.9 CONCLUSION .....	62
CHAPTER 5: DESIGN OF THE CYBERSECURITY RISK TOOL .....	63
5.1 INTRODUCTION .....	63
5.2 CYBERSECURITY .....	63
5.3 ROLES OF CYBERSECURITY FRAMEWORKS.....	66
5.4 NIST CYBERSECURITY FRAMEWORK.....	68
5.5 CYBERSECURITY AND CRIMINALS .....	73
5.6 BAYESIAN NETWORK BACKGROUND .....	73
5.7 RELATED WORK .....	76
5.8 AGENARISK WITH BAYESIAN ARTIFICIAL INTELLIGENCE TOOLS .....	77
5.9 APPLICATION OF THE AGENARISK IN THE SME SECTOR.....	78
5.10 AGENARISK PACKAGE FOR CYBERSECURITY TOOL DESIGN .....	80
5.11 CONCLUSION .....	82

SECTION C: TOOL DEVELOPMENT AND SIMULATION OF CASE SCENARIOS .....	83
CHAPTER 6: DEVELOPMENT OF CYBERSECURITY RISK TOOL .....	84
6.1 INTRODUCTION .....	84
6.2 GENERIC MODEL .....	84
6.3 SECONDARY MODEL .....	86
6.4 BETA MODEL AND ITS STRUCTURE .....	90
6.5 ALPHA MODEL .....	93
6.6 DEVELOPMENT OF THE SIMULATED RISK CASES .....	96
6.7 SIMULATED SCENARIOS ANALYSIS .....	97
6.8 SIMULATED SCENARIO 1: OBSERVATION OF END DEVICES .....	100
6.9 SIMULATED SCENARIO 2: OBSERVATIONS OF THE HUMAN ERRORS .....	105
6.10 SIMULATED SCENARIO 3: OBSERVATIONS OF THE MALWARE ATTACK .....	109
6.11 SIMULATED SCENARIO 4: OBSERVATIONS OF THE PHISHING ATTACK .....	112
6.12 SIMULATED SCENARIO 5: ADHERENCE TO POLICIES, GUIDELINES, AND RULES .....	116
6.13 CONCLUSION .....	124
SECTION D: RISK EVALUATION AND CONCLUSION .....	125
CHAPTER 7: RISK MANAGEMENT TECHNIQUES .....	126
7.1 INTRODUCTION .....	126
7.2 RISK MANAGEMENT PROCESSES .....	126
7.3 RISK IDENTIFICATION .....	130
7.4 RISK ANALYSIS TECHNIQUES .....	136
7.5 RISK EVALUATION .....	139
7.6 QUANTITATIVE RISK ANALYSIS .....	146
7.6 RISK TREATMENT .....	168
7.7 MONITORING AND REVIEW .....	170
7.8 RISK REPORTING .....	171
7.9 CONCLUSION .....	176
CHAPTER 8: CONCLUSION AND RECOMMENDATIONS .....	177
8.1 INTRODUCTION .....	177
8.2 RESEARCH IMPLICATIONS CONCERNING THE RESEARCH OBJECTIVES .....	177
8.3 OUTCOMES, OUTPUTS, AND CONTRIBUTION .....	179
8.4 STUDY LIMITATIONS .....	180
8.5 RECOMMENDATIONS .....	181
8.6 IDEAS FOR FUTURE RESEARCH .....	182
8.7 SUMMARY .....	182
8.8 CONCLUSION OF THE STUDY .....	183
REFERENCES .....	185
APPENDIX A: Consent letter .....	202
APPENDIX B: Ethical Clearance .....	203
APPENDIX C: Questionnaire .....	204
APPENDIX D: Interview guide .....	209



## LIST OF FIGURES

Figure 1-1: Conceptual model (Orange areas present the scope) (Own work, 2021) .....	8
Figure 2-2: SME Entities (Author's work, 2018).....	13
Figure 1-3: Top cybersecurity-related threats in SA (adopted from DTSP, 2017) .....	14
Figure 1-4: Common cyberthreats (Own work, 2021).....	17
Figure 2-5: Relationship between the asset, threat, and vulnerability (Source: Moyo, 2014: 47) .....	20
Figure 2-6: Cybercrimes (Lallie et al., 2020) .....	21
Figure 2-7: Top common risks for SMEs (Adapted from Haward, 2018).....	21
Figure 1-8: Customer interaction over the business system (Author's work, 2018).....	24
Figure 1-9: Top Covid-19 scams (Business Tech, 2020) .....	25
Figure 1-10: Africa cybersecurity report (source: Serianu, 2017).....	26
Figure 2-11: Cyber-security briefing (Source: DTSP, 2017).....	26
Figure 2-12: Cybersecurity incidents from November 2015 to December 2016 (adapted from DTSP, 2017) ....	27
Figure 2-13: Cyber harm in business sectors (Source: Agrafiotis et al., 2018).....	29
Figure 3-14: Triangulation of data sources .....	37
Figure 3-15: Risk management processes - ISO Standard 31000:2009 .....	39
Figure 4-16: Participant SME sectors.....	47
Figure 4-17: Age of SMEs .....	48
Figure 4-18: Common Cyberattacks .....	48
Figure 4-19 Business risks .....	49
Figure 4-20: Information system risk likelihood.....	50
Figure 4-21: Human error risk likelihood .....	50
Figure 4-22: Network and power risk likelihood .....	51
Figure 4-23: Device access and encryption risk likelihood .....	51
Figure 4-24: Impact of cyberrisks .....	52
Figure 4-25: Risk impact on hardware, network, and policies.....	53
Figure 4-26: Expected monetary value .....	53
Figure 4-27: Cyberrisk management .....	54
Figure 4-28: Common cyberthreats in the Covid pandemic (Khan, Brohi & Zaman, 2020:395) .....	58
Figure 5-29: NIST Cyber-security Framework 1.1 (NIST, 2018: online).....	68
Figure 5-30: Cybersecurity as the mediating factor between business and criminals.....	73
Figure 5-31: Variables used on the Bayesian network models .....	80
Figure 5-32: Use of the Bayesian network .....	80
Figure 5-33: Validation of the model .....	81
Figure 6-34: Variables for the BN structures .....	84
Figure 6-35: Generic Bayesian model .....	85
Figure 6-36: Second conceptual model or Secondary Model .....	87
Figure 6-37: Beta Model.....	90
Figure 6-38: Alpha Model.....	94
Figure 6-39: User processes during information processing (Source: Ncubekezi, 2021b).....	97
Figure 6-40: Fixed standalone end devices with high protection level .....	101
Figure 6-41: Fixed standalone end devices with low H/W and S/W protection.....	101
Figure 6-42: Portable networked end devices with high device protection .....	102
Figure 6-43: Portable networked end devices with low hardware and software security .....	102
Figure 6-44: Portable networked end devices with low software protection .....	103
Figure 6-45: Portable standalone end devices with high device protection.....	103
Figure 6-46: Portable networked end devices with low device protection level .....	104
Figure 6-47: Human errors in the business system (Source: Ncubekezi and Mwansa, 2021b) .....	105
Figure 6-48: IT user experiences a partially unplanned and planned attack at a 50% protection level.....	106
Figure 6-49: IT user experiences an unplanned attack at the 50% protection level.....	107
Figure 6-50: Normal user with planned and unplanned attacks as high risk likelihood .....	107
Figure 6-51: Normal users experience high and low attacks at a high protection level .....	108
Figure 6-52: Combination of planned and unplanned attacks on normal user .....	108
Figure 6-53: Low protection level of a computer with a virus.....	110
Figure 6-54: Malware at a medium protection level.....	111
Figure 6-55: High protection for a low computer malware infection .....	111
Figure 6-56: High malware infection at a high protection level .....	112
Figure 6-57: No phishing, with high protection level and user awareness .....	114
Figure 6-58: Phishing with high protection level and low user awareness.....	114
Figure 6-59: No Phishing email, high protection & user awareness .....	114
Figure 6-60: Phishing email with high awareness, medium protection .....	115
Figure 6-61: Partial cybersecurity, password, and access to third-party websites.....	117

Figure 6-62: Partial cybersecurity, password, and access to third-party guidelines with medium compliance..	118
Figure 6-63: No cybersecurity, password, and access to third-party guidelines .....	118
Figure 6-64: No password guideline and access to third-party websites.....	119
Figure 6-65: Presence of cybersecurity and user awareness.....	119
Figure 7-66: Risk management process from ISO 31000:2018 .....	127
Figure 7-67: Risk likelihood for planned attacks (Data source: Survey, 2021) .....	148
Figure 7-68: Risk likelihood for unplanned attacks (Data source: Survey, 2021).....	148
Figure 7-69: Tornado graph for planned attack = True.....	149
Figure 7-70: Tornado graph for planned attack = False .....	149
Figure 7-71: CPT for device and technical systems (Data source: Survey, 2021) .....	150
Figure 7-72: Tornado graph for false data breaches and high threats level .....	150
Figure 7-73: Tornado graph for true data breach and medium threats level.....	150
Figure 7-74: Tornado graph for true data breach and low threats level .....	151
Figure 7-75: Virus CPT (Data source: Survey, 2021) .....	151
Figure 7-76: Tornado graph for no virus.....	152
Figure 7-77: Tornado graph for yes virus .....	152
Figure 7-78: Phishing and network CPT (Data source: Survey, 2021).....	153
Figure 7-79: Tornado graph for very low-risk likelihood and high impact .....	153
Figure 7-80: Tornado graph for very low-risk likelihood and medium impact.....	154
Figure 7-81: Tornado graph for very low-risk likelihood and low impact .....	154
Figure 7-82: CPT for lack of policies and guidelines (Data source: Survey, 2021) .....	154
Figure 7-83: Tornado graph for a low impact on a high policy compliance.....	155
Figure 7-84: Tornado graph for a medium impact on a high policy compliance .....	155
Figure 7-85: Tornado graph for a high impact on a high policy compliance.....	156
Figure 7-86: Configuration information for human factors .....	160
Figure 7-87: Human factors' EMV .....	160
Figure 7-88: Configuration information for devices and technical systems .....	160
Figure 7-89: Devices and technical systems' EMV .....	161
Figure 7-90: Configuration information for malware and technological risks.....	161
Figure 7-91: EMV for malware and technological risks .....	162
Figure 7-92: Configuration information for policies and guidelines .....	162
Figure 7-93: Policies and guidelines' EMV .....	162
Figure 7-94: Configuration information for phishing and network scenario .....	163
Figure 7-95: Phishing and network's EMV.....	163
Figure 7-96: Risks associated with planned and unplanned attacks .....	165
Figure 7-97: Device exploitation .....	166
Figure 7-98: Malware attacks .....	166
Figure 7-99: Phishing and network decision tree .....	167
Figure 7-100: No password policy .....	168
Figure 7-101: Managing cyberrisks (Data source: Survey, 2021).....	174

## LIST OF TABLES

Table 1-1: Research sub-questions.....	7
Table 2-2: SMMEs (Adapted from Quartey (2015); Business Tech, 2019).....	12
Table 3-3: Sample Summary.....	36
Table 4-4: Participant demographic.....	47
Table 4-5: The connection between threats, attacks and cybercrimes (Ncubukezi & Mwansa, 2021a).....	57
Table 5-6: Alignment to the NIST Cyber Security Framework 1.1 Core components. (Data source: survey, 2021; NIST, 2018).....	71
Table 6-7: Main node and values.....	85
Table 6-8: Prior indicator nodes and values.....	85
Table 6-9: Measure nodes and values.....	86
Table 4-10: Secondary Model basic nodes and values.....	87
Table 6-11: Secondary prior indicator nodes and values.....	88
Table 6-12: Secondary measure nodes and values.....	89
Table 6-13: Beta Model basic nodes and their values.....	91
Table 6-14: Beta model priority indicators.....	91
Table 6-15: Beta Model measures.....	92
Table 6-16: Alpha basic nodes and their values.....	94
Table 6-17: Alpha Model prior indicator nodes and values.....	95
Table 4-18: Alpha-model measures.....	95
Table 4-19: Summary of the scenario cases.....	122
Table 7-20: Analysis of cyberrisks, their causes and the source (Data source: Survey, 2021).....	132
Table 7-21: Total number of identified risks (Data source: Survey, 2021).....	133
Table 7-22: Ranking of the identified risks (Data source: Survey, 2021).....	136
Table 7-23: Risk probability and impact assessment.....	136
Table 7-24: Definitions of impact values ((Guided by (PMBOK, 2013)).....	137
Table 7-25: Definitions of likelihood values ((Guided by (PMBOK, 2013)).....	138
Table 7-26: Risk likelihood, likelihood score and the risk consequences.....	138
Table 7-27: Risk scoring.....	139
Table 7-28: 5*5 Risk Probability and Impact Matrix.....	139
Table 7-29: Devices and technical systems risk probability, impact and value (Data source: Survey, 2021) ...	140
Table 7-30: Technological/Malware risk probability, impact and value (Data source: Survey, 2021).....	141
Table 7-31: Phishing and network risk probability, impact and value (Data source: Survey, 2021).....	141
Table 7-32: Human factors risk probability, impact and risk value (Data source: Survey, 2021).....	142
Table 5-33: Policies/Guidelines risk probability, impact and risk value (Data source: Survey, 2021).....	143
Table 7-34: Definition of risk classes (Data source: Survey, 2021).....	143
Table 7-35: Matrix that influences vulnerability (Data source: Survey, 2021).....	144
Table 7-36: Description of collected cyberrisks table (Data source: Survey, 2021).....	145
Table 7-37: Asset evaluation.....	157
Table 7-38: EMV for devices and technical systems (Data source: Survey, 2021).....	157
Table 7-39: Phishing and network EMV (Data source: Survey, 2021).....	157
Table 7-40: Human factors EMV (Data source: Survey, 2021).....	158
Table 7-41: Malware and technological risks EMV (Data source: Survey, 2021).....	158
Table 7-42: Policies and guidelines EMV (Data source: Survey, 2021).....	159
Table 7-43: Recommended mitigation techniques (Data source: Survey, 2021).....	175
Table 8-44: The summary of the research outcome, output and contributions.....	180

## GLOSSARY

<b>Acronym</b>	<b>Acronym stands for</b>
AI	Artificial Intelligence
BN	Bayesian Network
BPC	Brutus Password Cracker
CET	Cybersecurity evaluation tool
CPT	Conditional Probability Table
CSF	Cybersecurity Framework
DDoS	Distributed denial of service
DoS	Denial of Service
DTA	Decision tree analysis
DTI	Department of Trade and Industry
DTPS	Department of Telecommunications and Postal Services
EMV	Expected maximum value
EMV	Expected Monetary Value
FSB	Federation of Small Businesses
GDP	Gross Domestic Product
ICT	Information and Communication Technology
IP	Internet Protocol
IS	Information Systems
ISO	International Organization for Standardization
IT	Information Technology
NCSS	National Cyber Security Strategy
NIST	National Institute of Standards and Technology
PCI-DSS	Payment Card Industry Data Security
PGM	Probabilistic Graphical Modelling
PMBOK	Project Management Body of Knowledge
PMI	Project Management Institute
RAM	Risk Assessment Matrix
RM	Risk Management
RMF	Risk Management Framework
RMP	Risk Management Processes
SA	South Africa
SABRIC	South African Banking Risk Information Centre
SMB	Small-Medium Businesses
SME	Small-Medium Enterprise
SMEs	Small-Medium Enterprises
SMME	Small Micro and Medium Enterprises
SMMEs	Small Micro and Medium Enterprises
TPS	Telecommunications and Postal Services
UK	United Kingdom
WCT	Wifi Cracking Tool

## CLARIFICATION OF TERMS

The key terms used.

<b>Term Used</b>	<b>Definition of the term</b>
Artificial intelligence	It is the art of determining the core of intelligence and improving quick, intellectual machines, which help discover methods for solving complex and challenging problems to resolve without applying some intelligence. It makes correct decisions based on the available data pool. (NCSS, 2016).
Conceptual model	It is a set of concepts that support people to recognize, better understand, or demonstrate the meaning of the model.
Cyber-attack	Cyber-attack means an attempt to expose, alter, disable, destroy, steal, or gain unauthorised access to or make unauthorised use of an asset
Cybercrime	The offenses such as intrusion, misuse of business resources, and unauthorized access are committed in cyberspace. (Sutherland, 2017; Dilek <i>et al.</i> , 2015)
Cyber risks	Cyber risks are the possible danger or harm that can affect businesses negatively or positively (Dilek <i>et al.</i> , 2015).
Cyberspace	Internet platform connects individuals and institutions through telecommunication infrastructure and internet-connected devices (NCSS, 2016).
Cybersecurity	Cyber-security refers to securing data in electronic form (IBM, 2018)
Cyber threats	They mainly compromise the state of the data, device and network security (NCSS, 2016).
Information Security	This term can sometimes be called <i>InfoSec</i> , a practice protecting data from unauthorised access, alteration or removal of information.
Risk	Risk represents a given chance of particular exposure to the form of danger, harm and possibly loss of value. Exposure to this risk can lead to two possible states, which are either positive or negative (Koeze, 2017).
Risk Management	Risk management is the process of calculating to reduce risk for an organisation not to fail in its activities or lose money. The activity identifies and manages unknown and known risks (Koeze, 2017).
Risk Management Process	Refers to the process of managing risk: 'communicating, consulting, establishing the context and identifying, analysing, evaluating, treating, monitoring and reviewing risk (ISO, 2018).
Risk Management Framework	RM framework is a written description of a risk management system; an example of a risk management framework includes ISO 31000, which is the risk management standards (Koeze, 2017).
Security awareness training	A formal process of educating employees about the cybersecurity training

## PUBLICATIONS DURING THE STUDY

- Paper A: Ncubekezi, T. 2023. The risk likelihood of the planned and unplanned cyber-attacks in small business sectors: A cybersecurity concern. Conference proceedings: *International Conference on Cyber Warfare and Security*, 18 (1), 179-290.
- Paper B: Ncubekezi, T. 2022. Human errors: A cybersecurity concern and the weakest link to small businesses. Conference proceedings: *International Conference on Cyber Warfare and Security*, 17 (1):395–403. <https://doi.org/10.34190/iccws.17.1.51>.
- Paper C: Ncubekezi, T. & Mwansa, L. 2021. Security of the business activities in cyberspace: An Activity Theory Perspective. *Information Society*, 16: 27–33. <https://doi.org/10.20533/ICITST.2021.0003>.
- Paper D: Ncubekezi, T. & Mwansa, L. 2021. Best practices used by businesses to maintain good cyber hygiene during Covid-19 pandemic. *Journal of Internet Technology and Secured Transactions*, 9: 714–721. <https://doi.org/10.20533/jitst.2046.3723.2021.0086>.
- Paper E: Ncubekezi, T., Mwansa, L. & Rocaries, F. 2021. An analysis of the cybercrimes within the Western Cape small and medium-sized enterprises. *International Conference on Cyber Warfare and Security*, 16: 425–435.
- Paper F: Ncubekezi, T., Mwansa, L. & Rocaries, F. 2020. Review of the current cyber hygiene in small and medium-sized businesses. Conference proceedings: *International Conference for Internet Technology and Secured Transactions*, 15: 283–288.
- Paper G: Ncubekezi, T., Mwansa, L. & Rocaries, F. 2020. A proposed: integration of the Monte Carlo model and the Bayes network to propose a cybersecurity risk assessment tool for small and medium enterprises in South Africa. *International Journal of Innovative Science and Research Technology*, 3(18): 152–155. ISSN 1947-5500.
- Poster 1: Ncubekezi, T. 2021. *An exploration of the malware impact on the end devices*. Conference Proceedings: CPUT Postgraduate Conference: 70.

The above papers (A to G) and the posters (1) contributed during the central thesis study period. Tabisa Ncubekezi was the leading researcher and primary author.

# SECTION A: RESEARCH BACKGROUND

## INTRODUCTION AND BACKGROUND



This section introduces this work by presenting the background to the research problem as well as the main aim and the supporting objectives, followed by the conceptual model, significance and rationale of the study.

In addition, the work reviews the relevant and latest literature about cybersecurity in small and medium-sized enterprises (SMEs). Furthermore, it gives an overview of the SMEs in South Africa (SA), followed by cyberspace and its impact on businesses, risk overview, SME's perception of cybercrimes, cybercrimes, risk management and the impact of cyberrisks and security measures. The chapter concludes with a summary.

## **CHAPTER 1: INTRODUCTION AND BACKGROUND**

### **1.1 INTRODUCTION**

Small and medium-sized enterprises (SMEs) have continuously increased in South Africa (SA) and other countries over the past years. These small businesses come about to alleviate poverty, create job opportunities, and ultimately contribute to the South African economy (Such et al., 2019; Kupec & Pizar, 2021). These features are evident because SMEs provide employment opportunities to 8.9 million people in SA (SEDA, 2018). Marais (2018) shared the information that the chief executive officer of the Small Business Project (SBP), Chis Darroll, had explained that 95% of businesses were SMEs, which ultimately contributed up to 60% to the Gross Domestic Product (GDP). Moola (2020) states that South African SMEs contribute 6% towards corporate taxes, 20% to the GDP, and 47% to the workforce. Most SMEs depend on cyberspace to operate to their full potential, meet market needs and reach more diverse target markets (Reddy, 2016; Van Niekerk, 2017; Adepun, 2018; Lejaka et al., 2019).

Cyberspace comprises the networking infrastructure and Internet-worked end devices (computers) to share applications or resources (Ning et al., 2019; Cisco Cyber Report, 2018). As a platform, cyberspace, also called the Internet, acts as a library of information, entertainment, and social networking. Even though most businesses use the Internet to attract new clients, they also perform business transactions on the Internet (Dzomira, 2014). The convenient increased usage of cyberspace creates open systems resulting in exposure and innovative ways for cyberattackers to engage in cybercrimes (Choo, 2011; Koeze, 2017). Cybercrimes, also computer-oriented crimes, involve end devices like computers, smart devices, tablets, and networks, to commit crimes or as the target point. However, cyberattackers target Internet Protocol (IP) addresses assigned to those end devices. This action ultimately quantified cyberrisks (Olayiwola, 2012), leaving SMEs vulnerable and exposed to cyberattacks.

Despite the increased cyberspace usage, which improves business continuity, the SME sector finds that the lack of cybersecurity negatively influences growth. Studies by Sarre, Lau, and Chang (2018) highlight the gradual increase in cybercrimes, which is a global problem. IT News Africa (2017), SABC News (2017), and Adepun (2018) have explained the gradual increase in cyberattacks in SA, which has yielded a critical point. Adepun (2018) argues that the effects of increased cybersecurity risks have changed the state of businesses in SA and that change affects the rest of Africa.

The current study conducted a cybersecurity risk analysis at SMEs by means of risk management processes to identify the risk matrix, common cyberrisks affecting SMEs and the current safety measures used for mitigation. For a clear understanding of the common cyberrisks and the mitigation



purposes, the study referenced the National Institute of Standards and Technology (NIST) cybersecurity framework and AgenaRisk package which embedded the Bayes network tools.

### 1.1.1 An Overview of Cybersecurity

Cybersecurity is one of the most common, critical, and current issues in all sectors and has gained more recognition in the business space. Increased dependence on cyberspace, including the complex connections of networked devices, has increased cyberrisks for small businesses (Ponsard, Grandclaudon & Dallons, 2018). Cybersecurity presents some form of securing and promoting the well-being of the cyberspace platform known as the 'Internet' and its applications against known and unknown cyberthreats and cyberattacks (Zhang et al., 2021). As used in this study, security refers to the safety of information, assets, people, and the platform or system used to communicate with internal and external stakeholders. A 'secured system' protects business information from the public and conforms to the collective security properties, including confidentiality, integrity, non-repudiation, and privacy. In addition, cybersecurity requires individuals to understand both the technological perspective (for example, database, software, computer programming and networking) and the organisational and human perspective (for example, administrative controls) (NIST Special Publication, 2017; González-Manzano & De Fuentes, 2019).

### 1.1.2 Cybersecurity at SMEs

Neil Cosser, the data protection manager for Africa at Gemalto, explains four critical trends in cybercrimes between 2017 and 2018 in South Africa which threaten data security. Out of these four trends, the first cybercrime is *ransomware*, a malware attack, namely, namely the *crypto*<sup>1</sup> and the *locker*<sup>2</sup> ransomware. As cited by Cosser (2018), ransomware affects two hundred thousand organisations on a global level. The second trend is the *critical data and information breaches*, which took place in 2017 and affected Dropbox, Yahoo, and LinkedIn. This significant cybercrime allowed access to the client's data from various organisations. The third trend in 2017 was the increased use of hacking tools such as the Wifi Cracking Tool and the Brutus Password Cracker, which became available to cybercriminals. Finally, the last trend recorded in 2017 was hackers breaking the set boundaries. This trend includes the cryptocurrency exchanges motivated by Bitcoin, which focus on penetrating victims' mobile devices.

All the cybercrimes committed are equivalent to a currency of the country Sword (2016) cited that the Federation of Small Businesses (FSB) had announced an economic loss amounting to £5.26 billion to the UK economy caused by cybercrimes. Linington (2016) says 8.8 million South Africans have fallen victim to various cybercrimes. The Minister of Telecommunications and Postal Services in South

---

<sup>1</sup> Crypto ransomware aims to deny access to the victim's files by identifying and encrypting valuable files.

<sup>2</sup> Locker ransomware is the computer locker that denies access to the device by locking the device's user interface and then demands ransom from the victim.

Africa, Siyabonga Cwele, estimated 32% of SMEs in the country are affected by cyberthreats and phishing attacks (Peyper, 2016; DTSP, 2017). The government does not have a public or national document that records cyberrisks affecting SMEs. Ashford (2017) says that in the study conducted by the Ponemon Institute in the United Kingdom and the United States, the main cyber-attacks to hit SMEs were due to employees' weak passwords, ransomware, data breaches, and phishing. Asian Pacific SMEs explained that the primary sources of cyberattacks are malfunctioning SME systems affecting business continuity and eventually losing data. However, it is not clear whether data loss is through the system itself or human error at this stage. Human error could either be through the company's loss of information or an employee unintentionally divulging information owing to a lack of skill (Howard, 2018).

There is an extremely high rate at which cyberattackers are active. Some attacks include viruses, worms, Trojans, spyware, botnets, hacking, spam, denial of service, and ransomware. With the high number of cyberattacks, including their high rate, the human mind is generally not enough for regular analysis of an attack and the appropriate intervention. Computer-generated means must intervene where the human mind falls short. The computer-generated agent could promptly manage the entire cyber-attack process. With its intelligence, the agent could quickly detect early warning signs of an attacks, evaluate various attacks and respond to cyberattacks accordingly. The step-by-step process can analyse which cyberattacks are happening at any specific time, the target areas in which the attack is heading, and relevant control measures needed to be applied. Thus, cybersecurity can be managed, improved, and maintained adequately through risk management, cybersecurity framework and a technological means to predict the risk probability.

### **1.1.3 Risk Management**

The Oxford dictionary explains risk management as *the process of calculating and decreasing cyberrisk, for an organization not to lose money or fail*. This explanation carries two bold statements. The first part of the definition calculates the identification of risk, and the second part calculates the probability of risk through risk analysis and assessment. Thus, a risk calculation or assessment as a basis for risk management is relevant to many sectors and is critical for cybersecurity (Jones, 2006). It is essential for businesses to perform regular cyberrisk reviews to analyse, treat, estimate and evaluate risk (Frosdick, 1997). Even though there are several risk management standards, this study is guided by the ISO 31000:2018 standard to establish the context to assess, analyse, evaluate, monitor, treat, review and communicate risks. The application of the risk management standard to the seven phases of risk management, namely communication and consultation, establishing the context, risk analysis, and evaluation, risk treatment, monitoring and reviews, and reporting, is presented thoroughly in Section D.

This study adopted the NIST framework to understand cyber security risks better.

#### **1.1.4 Relevance of NIST Framework to SMEs.**

NIST is the cybersecurity framework that acts as a tool to analyse, organise and eventually improve the state of cybersecurity in organisations (Mahn et al., 2021). The framework consists of guidelines, standards, and best practices for organisations to develop and improve their cybersecurity. In addition, the framework has a list of recommendations and standards that benefit organisations by preparing them to identify and detect the intruding and provoking cyberattacks and threats, as well as providing the guidelines to respond, mitigate and recover from cyberincidents. Section B presents the adoption and relevance of the NIST cybersecurity framework to analyse, organise and improve cybersecurity risks at SMEs.

Even though the study used the NIST framework, Reddy (2016) suggests that businesses must take specific precautionary measures while using the Internet. The increasing advancement of technology and ways to commit cybercrimes leads to the human mind's failure and health systems becoming ineffective in mitigating dynamic and evolving cyberattacks. A technology-based solution is required to illustrate the risk likelihood and impact on managing and reducing cyberrisk. A mitigation technique with AI<sup>3</sup> capabilities and tools is necessary to determine the risk probability and mitigation beyond human measures.

#### **1.1.5 AgenaRisk Package with Bayesian Network Tools**

As cyberattacks and threats increase in cyberspace, there is a high demand to identify, reduce, combat, and minimise cyberrisks. Some cyberrisks can depend on the Internet, independent of or dependent on one other, which ultimately quantifies cyberattacks (McGuire & Dowling, 2013). The situation can result in a high demand for more sophisticated information or technology to improve and minimise cyberrisks as well as managing healthy systems behaviour and detecting and predicting unusual risk likelihood and cybercrimes. Owing to the grave concern for the future of information security and privacy, AI tools show promising techniques that discover the essence of computer intelligence to solve complex problems known and unknown (Hans, 2016). AI suggests improving security in cyberspace (Dilek et al., 2015).

Several studies have used the Bayesian network tools to identify, evaluate and reduce risks. Some authors have used the tools to assess the risk difference, measured by the proportion of failures versus the percentage of losses in the experimental group and predicting the failure rate (Biau et al., 2017). This study adopted the AgenaRisk package with Bayesian network tools to illustrate the risk likelihood and the risk impact. The selected technique uses mathematical formulae to calculate the conditional

---

<sup>3</sup> Artificial intelligence helps to find methods for solving complex and various challenging problems without the application of some intelligence. It is emerging as a next major wave of innovation.

probability of the possible cyberrisks caused by a given observed outcome and performance-sensitivity analysis. The work embedded the Bayesian network tools to identify the dependent and independent variables connected to determine the risk likelihood.

The following section explains the background of the research problem.

## **1.2 BACKGROUND TO THE PROBLEM**

Despite cyberspace's significance and contribution to small businesses, the Internet remains vulnerable to cybercrimes (Barn & Barn, 2016; Van Niekerk, 2017). The primary aim of the cyberthreats is to alter and corrupt business information, to data intrusion, withhold business data and eventually discontinue the business (Van Zyl, 2016; Vermeulen, 2016; Ponsard, Grandclaudon, & Dallons, 2018; Lejaka et al., 2019). Studies indicate that malware, spyware, data breaches, denial of service, and network exploitation trigger cyberthreats (Abomhara, 2015; Eno-akpa, 2016; Van Zyl, 2016). While some cybercrimes are internet-dependent, others are cyberenabled (Barn & Barn, 2016). These cyberattacks target internet platforms, stand-alone or networked computers, smart devices, and external data storage.

A cyberattack on a vulnerable small business causes harm to its reputation, physical damage to the devices, discontinues the entire business, or threatens the business's financial health (Venkatesh, 2016; Van Niekerk, 2017; Adepotun, 2018; Sarre, Lau & Chang, 2018). SABRIC report (Online), which stands for South African Banking Risk Information Centre, states that SA has become the main target for cyberattacks and is rated the third-highest country with the number of cybercrimes globally, losing around R2.2billion a year to cyberattacks. Most small business owners assume that cyberattackers mainly target big and established businesses. The fact is that cyberthreats come in different forms and eventually affect enterprises negatively. Even though small business owners still conduct small online businesses, their activities are still vulnerable to cyberthreats.

Similarly, cyberattackers enjoy the lucrative business benefits of small businesses that grow and generate profit. In one way or another, cyberattacks increase as the business grows (Sen, Ahmed & Islam, 2015). The South African SMEs in 2022 faced a 69% increase in Trojan-PSW (Password Stealing Ware) detections compared to 2021 (Staff writer, 2022). Cybersecurity risks represent a highly ignored field in the small business sector. The reality is that cybersecurity risks are constant and have become a daily topic of conversation. Its nature is current and relevant to the SME sector. Literature indicates that SME owners pay minimal attention to cyber-security (Ngugi, 2016; Xero, 2018). South African SMEs face high cyberspace demands and usage that come with cyberthreats. Cyberthreats are intentional or accidental dangers that could exploit vulnerability leading to a cybersecurity breach and eventually causing possible harm. These cyberthreats may vary from business to business. For example, cyberthreats may come from different cyberattacks ranging from malware (automatic pop-up adverts),

stealing private, sensitive, and critical information (theft), and also causing unexpected network downtime (Ngugi, 2016; Xero, 2018).

Some of these cyberattacks may threaten both individuals and business sectors. These attacks may aim to gain access to the IP address of the networked computer or device. The main aim of the attackers varies. The process of securing these attacks is connected to cybersecurity. Privacy, confidentiality, and safety issues arise when there is a lack of cybersecurity<sup>4</sup> in the businesses: the cause of cyberrisk, the impact, the likelihood, and proximity trigger cybersecurity issues. Any cybersecurity risk happens when the cyberattack threatens the business or system, which eventually causes an effect when the event has taken place. Knowing the cause of the cyberrisk, the impact<sup>5</sup> and likelihood become difficult to define without performing risk management processes. Risk probability<sup>6</sup> helps determine the risk likelihood, then the proximity relates to when exactly a risk happens. The use of cyberrisk management will minimise the costs of risks.

### **1.2.1 Research Problem**

Cyberspace has become every society's central and leading resource, especially during the Covid-19 pandemic. However, its openness compromises trust, security and the safety of many users and systems, ultimately attracting cybercriminals (Chen et al., 2022). The consequences of cyberrisks are a result of higher exposure to cyberthreats because of inherent vulnerabilities. The situation challenges cybersecurity for SMEs and their business partners. The main issue is that larger organisations have mitigation strategies that SMEs don't, making SMEs the primary target for cybercrime activities (Twisdale, 2018). However, SMEs have fewer resources than more prominent organisations (Dahlberg & Guay, 2015). In addition, Chak (2015) has discovered that SMEs predominantly lack funding, knowledge and human resources to defend themselves against various cybercriminals.

Henson and Garfield (2016) posited that with limited resources, there is still much work to be done in the SME sector compared to the large organisations that have made significant progress in their practices. Furthermore, the cyberrisk likelihood within the SME sector is unclear. Abdulrahim (2019) states that there is minimal research conducted on using the technology-based Bayesian Network (BN) tools to illustrate risk likelihood and cyberrisk mitigation, and the security of information for small businesses. As a result, there is a high demand for a technology-based solution to manage and reduce cyberrisk and its impact. So this study designed, developed and evaluate the cyberrisk tool for SMEs. The following section presents the main aim and objectives of this study.

---

<sup>4</sup> Cyber-security refers to securing data in electronic form (IBM, 2018)

<sup>5</sup> Risk impact is the damage, which the cyberrisk attack could cause to the business.

<sup>6</sup> Risk probability is the random chance that a risk can occur or a probability of a loss.

### 1.2.2 Aim and Objectives

This work aims to design, develop and evaluate the cybersecurity risk tool for SMEs in SA. The supporting objectives of this work are to:

- a) Conduct qualitative cyberrisk assessment to determine the risk matrix based on the risk profile and the risk register of common cyberrisks.
- b) Conduct a quantitative cyberrisk assessment using modelling and analytical techniques to perform sensitivity analysis, scenario analysis, Tornado graphs, decision trees, and EMV.
- c) Develop and evaluate a cybersecurity risk tool for SMEs in SA using the AgenaRisk package with Bayesian network tools
- d) Develop five different cyberrisk scenarios using the AgenaRisk package to demonstrate the risk likelihood and the risk impact.

### 1.2.3 Research Question and Sub-Questions

In line with the research problem, the main research question has sub-questions.

**Research Question 1:** How can the AgenaRisk with Bayesian network tools be used to develop a cybersecurity model demonstrating cyberthreat indicators, measures, and relationships with variables for ultimate data breaches for SMEs in SA?

The following table illustrates the research sub-questions.

**Table 1-1: Research sub-questions**

SUB-QUESTIONS	APPROACH	OBJECTIVE	TYPE	SECTION
a) <b>What does the risk matrix for cybersecurity risks look like based on the common threats SMEs face?</b>	<ul style="list-style-type: none"> <li>• Qualitative</li> <li>• Risk Analysis</li> </ul>	A	Knowledge	Sections A, B, and D
b) <b>What can the quantitative results look like when performing sensitivity analysis, calculating the expected monetary value, and using the decision trees?</b>	<ul style="list-style-type: none"> <li>• Risk Analysis</li> </ul>	B	Knowledge/ Design	Section D
c) <b>How can the AgenaRisk package develop a tool with prior indicators and security measures to predict the cyberrisks leading to data breaches?</b>	<ul style="list-style-type: none"> <li>• AgenaRisk package with Bayesian network tools</li> </ul>	C	Design	Section C
d) <b>How can the AgenaRisk package develop a real-life case scenarios with prior indicators and security measures to predict the cyberrisks leading to data breaches?</b>	<ul style="list-style-type: none"> <li>• AgenaRisk package with Bayesian network tools</li> </ul>	D	Design	Section C

### 1.3 A CONCEPTUAL MODEL AS A TOOL

The study developed a cybersecurity conceptual model for SMEs in SA. The model shows all the elements, such as the intentional and accidental threats leading to a data breach, prior indicators, security measures, and the post-threat indicator. Every business experiences cyberattacks and threats that pose a risk to its assets. For this study, threats are initiated through employee errors and accidental and intentional actions of criminals. Even though some cyberthreats yield a diverse impact, this study's interest lies in the threats resulting in data breaches. Cyberthreats to businesses affect the safety and security of the company, which ultimately results in a significant data breach that dents the business growth, profit, and reputation of the business.

Figure 1-1 presents the conceptual model for SMEs. The model offers business elements that are affected by the data breach process. Some cyberattacks do not result in data breaches; instead, those attacks still become complicated, costly, and a waste of time-solving. The conceptual model illustrates the model's relationship between dependent and independent variables. The model shows that the business data and information are based on an organisation's assets, which the protection measures should protect. The business information includes client information, finances, and product or business information. However, if the protection measures are ineffective, the attackers may threaten the business system and eventually cause a data breach. The attackers may use information, network threats, BYOD (Bring Your Own Device), and malware to gain unauthorised access to the business system. An incident would be an example of a case where an attack could have taken place. The presence of an attack or threat can be detected through a prior indicator showing initial abnormalities in the system. Without adequate protection measures, the business would experience a post-indicator data breach. If the protection measures are updated and practical, the incidents will not escalate further. The study focused on the orange variables, the prior indicators, protection measures and the data breach, as illustrated below.

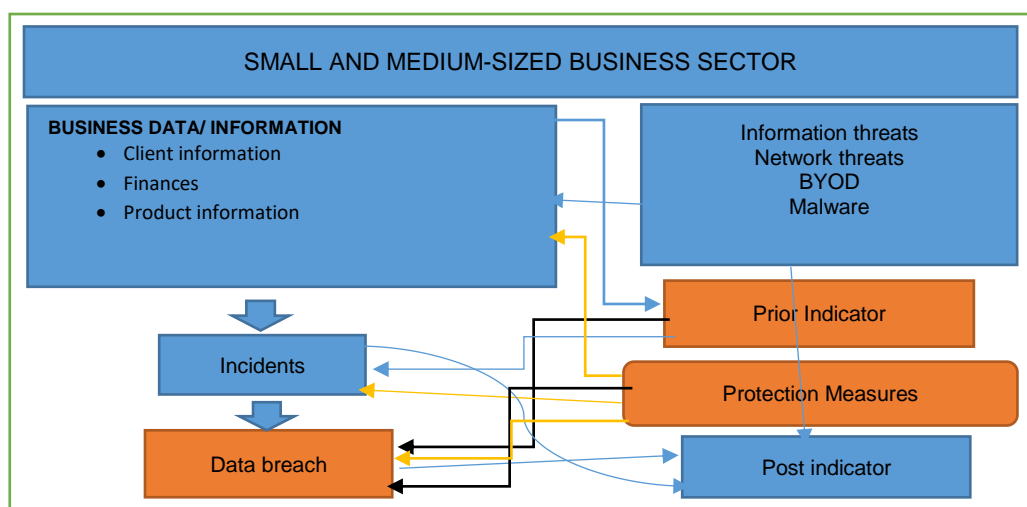


Figure 1-1: Conceptual model (Orange areas present the scope) (Own work, 2021)

The protection measures include physical, and technical systems, devices, procedures and encryption. The prior indicators represent various threats that are motivated and gain the opportunity to attack the business and ultimately cause the data breach. Lastly, the posterior indicators are the results of the cyber-attack.

#### **1.4 RATIONALE**

A global shift resulted in people and small and medium businesses changing the way they functioned. The transition forced all institutions to use cyberspace for all daily activities. Most businesses use cyberspace for information-searching, finding new business prospects or marketing services, making business transactions, and developing a competitive advantage (Jordaan, 2014; Gheorghică & Croitoru, 2019). While these SMEs depend on cyberspace, the rapid increase of cyberattacks and cybersecurity for small businesses remains the problem. Studies reveal that cyberattacks do not target a certain size or a specific business sector; instead, cyberattacks are after the business's lucrative benefits (Huang, Siegel & Madnick, 2018; Lejaka et al., 2019).

Some authors have shared their views about cybersecurity in the SME sector. For example, Paulsen (2016) reveals that most SMEs do not have a system to combat cyberattacks. For some SMEs, cybersecurity is not a consideration, resulting in the financial loss (Sarre, Lau, & Chang, 2018). Goldenson and Goldenson (2018) explain that cybersecurity in the SME sector receives minimal attention because the security aspect of SMEs is disregarded. Almeida, Carvalho, and Cruz (2018) explain that many small–medium enterprises do not take as much notice of the different aspects of security in the way that large businesses do; instead, SMEs have ignored this. Studies by Sarre, Lau, and Chang (2018) suggest that academics should conduct investigations and be involved with cybersecurity research and prevention.

The ignorance and impact of cybersecurity could reduce business operations and limit SME potential, yet studies only address the development of cybersecurity assessment tools and evaluate the feasibility of cyberattacks. Most of these studies have not combined the risk management standards, cybersecurity framework, and the AgenaRisk package with Bayesian tools to determine the risk likelihood at SMEs. This study will triangulate the methods for determining the likelihood of risk at SMEs. Furthermore, the work proactively addresses risk management to pre-empt known and unknown cyberattacks. Therefore, this work analyses, designs, and develops the cybersecurity risk model for the SME sector in South Africa.



## **1.5 SIGNIFICANCE**

This work's significant contribution is the design, development, and evaluation of a cybersecurity risk model illustrating the risk probability and the impact to benefit SMEs in their quest to implement cybersecurity risk response plans and their attainment and maintenance of cyberhygiene. Other benefits include minimising risk brainstorming meetings and time and money spent on cybersecurity risk management activities. In addition, the AgenaRisk package with embedded Bayesian network tools will introduce proactive cyberrisk response measures and save SMEs considerable resources.

Furthermore, this study benefits various business sectors using Information and Communication Technology (ICT) for business production and daily operations. For example, academics and scholars will benefit from this work's outcomes and findings as it contributes significantly towards and incorporates cybersecurity, risk management, a cybersecurity framework and AgenaRisk with a Bayesian network in its design. The AgenaRisk package determines the risk probability and effect based on independent and dependent risk causes or variables. In addition to this, SMEs can be more prepared when exposed to cyberattacks and threats leading to the ultimate cyberrisk. Third, the study results encourage researchers in the cybersecurity field to enlarge the research field to embrace AI's attractive properties. Also, government institutions may introduce innovative ways to finance SMEs' cybersecurity policies, standards, and regulations. This study provides risk managers with benchmarks to help adjust security resources to position ideal protection levels. Finally, IT management consultants may find the analytical instruments helpful with its creative ways to structure and develop cybersecurity measures tailored for SMEs to mitigate future cybersecurity threats.

## **1.6 DELINEATION OF THE STUDY**

This study carried out the primary research aim with detailed objectives and questions. The work analysed, designed, developed and evaluated a cybersecurity risk model for SMEs in SA. These SMEs will be from any business sector using ICT for business transactions and activities. The study used ISO 31000:2018 as the risk management standard, cybersecurity framework, and an embedded AgenaRisk package to carry out the research objectives. The package demonstrated the connections between the dependent and independent variables to analyse cyberrisks. The work used AgenaRisk with Bayesian network tools to calculate the probability of cyberthreats for independent and dependent risk causes. The study has only used a sample from small and medium-sized enterprises in SA. Due to time constraints, this work did not use the posterior predictive densities like expected log-predictive density (ELPD) or information criteria such as Akaike information criterion (AIC) and widely applicable information criterion (WAIC) to evaluate the Bayesian network algorithms.

## **1.7 CONCLUSION**

The chapter outlined the research background and discussed the SME's challenges, the research problem, the research objectives, the rationale, and the research questions. As discussed, small and medium-sized enterprises play a significant role in SA. The businesses create job opportunities, alleviate poverty and contribute to the GDP. However, these small businesses become the target of cybercrimes and are vulnerable to various cyberrisks relating to end devices (hardware), networks, applications (software), and people (employees). Cyberrisks relate to known and unknown cybercrimes, cyberthreats, and cyberattacks. The number of cybercrimes increases equally as Internet usage and technology advance.

In conclusion, SMEs are one of the targets of various cybercriminals. Their increased use of cyberspace exposes them to a range of cyberattacks which leave them vulnerable. Therefore it becomes essential for small businesses to understand and implement cybersecurity measures that promote the overall protection of their business assets.

## CHAPTER 2: LITERATURE REVIEW

### 2.1 INTRODUCTION

This chapter presents an overview of the relevant literature that relates to the cybercrimes which pose a risk to small and medium-sized enterprises that use cyberspace. The rest of the chapter introduces SMEs, cyberspace, cyber risks, cybercrimes, and their impact on small businesses as well as the security measures that can reduce and mitigate risks.

### 2.2 SMALL AND MEDIUM-SIZED ENTERPRISES

SMEs are the fundamental components of global economic growth and stability (Alahmari & Duncan, 2020). However, to this day, there is no uniform way to describe small–medium enterprises. SMEs represent a single concept with many different elements and sizes (Makina et al., 2015). SMEs across various South African industries range from five as the average number of micro to 200 employees for a medium-sized business. The total annual turnover ranges from R15 million (micro) to R40 million or R50 million (medium) (Mahembe, 2011; Quartey, 2015; Odendaal, 2018). The SME size differs from author to author. For example, if a company has 1–99 employees, that company would fall under the small business sector (World Bank). Quartey (2015) cites a general description of SMMEs varying from medium, small, and very small to micro in the National Small Business Act.

Table 2-2 summarises the number of employees in the business, annual turnover, and gross assets, as referenced in the National Small Business Act. Various businesses are highlighted according to the table, ranging from micro, tiny, and small to medium businesses. Each enterprise has a specific number of employees, an annual turnover represented in South African rand, and gross assets. This study focused on small and medium-sized enterprises with one to 150 employees and a maximum turnover of R2 million. The study selected a sample of SMEs from six of the nine South African provinces: the Eastern Cape, Free State, Gauteng, KwaZulu-Natal, Northern Cape, and Western Cape.

**Table 2-2: SMMEs (Adapted from Quartey (2015); Business Tech, 2019)**

<b>Enterprise Size</b>	<b>Number of Employees</b>	<b>Annual Turnover (in South African Rand)</b>	<b>Gross Assets Excluding Fixed Property</b>
Medium	Fewer than 100 to 200 depending on industry	Less than R4 million to R50 million depending on industry	Less than R2 million to R18 million depending on industry
Small	Fewer than 50	Less than R2 million to R25 million depending on industry	Less than R2 million to R4.5 million depending on industry
Very Small	Fewer than 10 to 20 depending on industry	Less than R200 000 to R500 000 depending on industry	Less than R150 000 to R500 000 depending on industry
Micro	Fewer than 5	Less than R150 000	Less than R100 000

The interest of the study is in small and medium-sized enterprises owing to their business size. The study also focuses on the state of cybersecurity to determine cyberrisks experienced since ICT is the main and central part of businesses.

### 2.2.1 SME Entities

Generally, any business, regardless of size, aims to serve customers or clients face-to-face or through the business platform, which could be the system. The company representative's business personnel would authorise all the activities captured on the system. Figure 2-2 illustrates the customers or clients who support the business daily. These clients become the number one supporter or focus of the day-to-day business operations on a business system. The SME system is used to exchange services for money (Sobihah et al., 2014). The system is connected through ICT, which becomes an integral part of the business. This platform can handle the services and finances at once. It illustrates how these different entities connect through the ICT platform. Thus, these entities are dependent on one other, as can be seen in the following diagram.

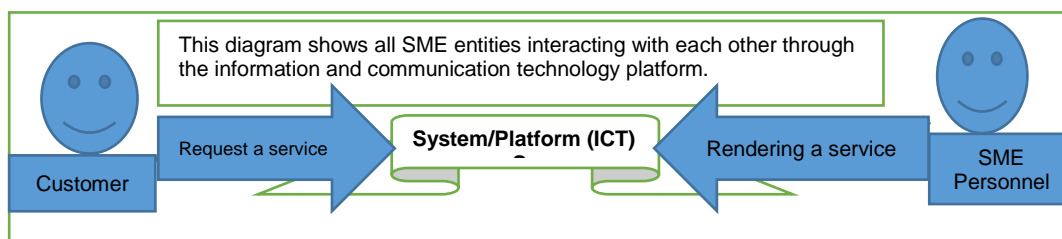


Figure 2-2: SME Entities (Author's work, 2018)

## 2.3 CYBERSPACE

Ngugi (2016) explains cyberspace as an online platform SMEs use to market their existence on the Internet. The term cyberspace is sometimes known as the Internet. Thus, the Internet connects devices using transmission media to share resources or information. However, businesses need to prioritise cybersecurity as big companies connect their devices to the Internet. Therefore, cybersecurity in big companies represents a section of the industry (Almeida, Carvalho & Cruz, 2018). Generally, the literature does not separate the term 'security' from information security because those terms are used jointly (Von Solms & Van Niekerk, 2013). Security refers to the safety of information, company assets, people, and platforms or systems used to communicate with internal and external stakeholders. A secured system protects business information from the public and conforms to the collective security properties, including confidentiality, integrity, non-repudiation, and privacy (Almeida, Carvalho & Cruz, 2018). However, the openness of cyberspace grants access to diversified attitudes and behaviour of people, business structures, and quantified cybercriminals (Salam, Imtiaz & Burhan, 2021) which has left SMEs exposed to various cyberthreats.

### 2.3.1 Top Cybersecurity Threats

As SMEs increase in number and are forced to rely on technology to become visible to the world, the sector becomes more susceptible to cyberthreats and risks. A cyberthreat is a potential action that has a negative and unwanted impact on a computer system or an application. Similarly, cyberattacks attempt to destroy, modify, expose, steal, gain and delete information through unauthorised access to the asset (Jain, Sahoo, & Kaubiyal, 2021). The many entities in the SME field have increased the number of cyberattackers. So, these different cyberattacks affect every SME entity depending on the methods used by multiple criminals on the network. Ngugi (2016) indicates that there is no clear or straightforward form of attack; instead, cyberattacks vary from one criminal to another. Figure 1-3 shows various cyberthreats that affect businesses daily, ranging from threats to information security, abusive content like spam, fraud, malicious codes (malware), illegal information gathering, loss of availability through network malfunctions and intrusion by outsiders, which involves all institutions. These cyberattacks negatively affect the SME systems and carry out certain operations in the SME sector. Therefore, the threats should be classified to identify risks in a structured manner.

Figure 1-3 shows the top cybersecurity-related threats in South Africa, which are discussed below.

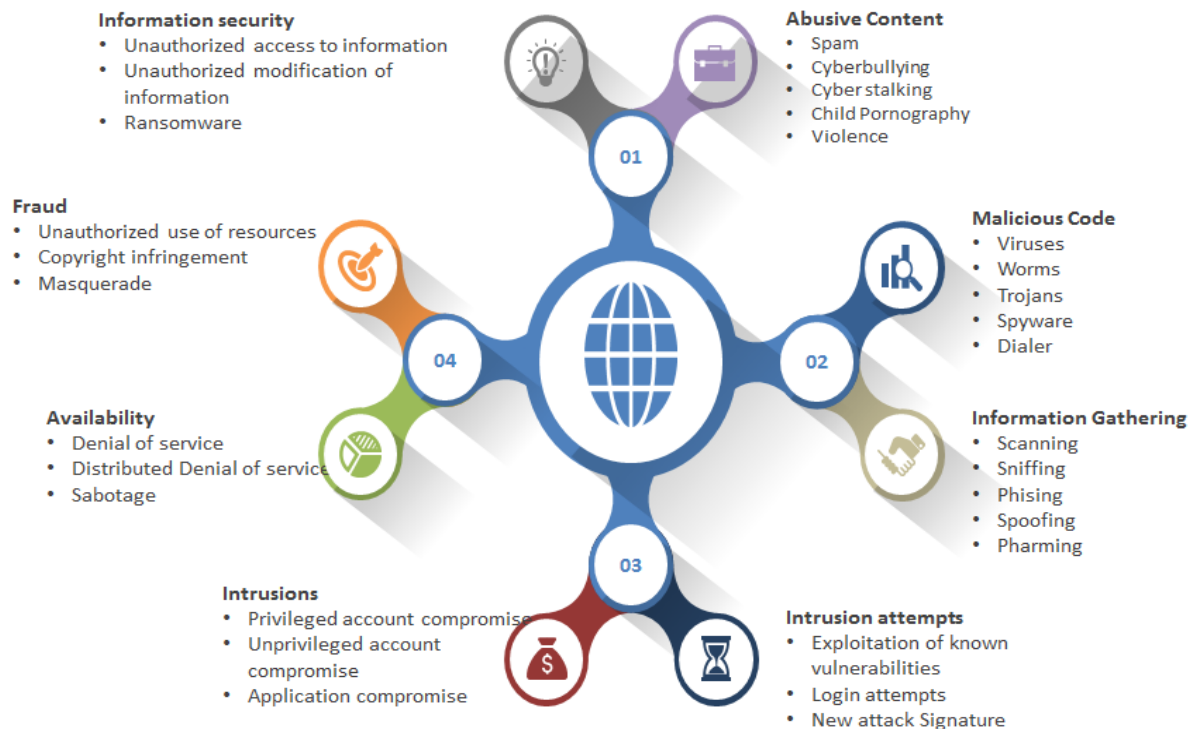


Figure 1-3: Top cybersecurity-related threats in SA (adopted from DTPS, 2017)

### **2.3.1.1 Information Security**

The term 'information security' can be described in various ways. According to Saravanan and Bama, (2019), information security protects confidentiality, integrity, and availability to ensure that information is only changed, read, heard, and used by authorised people. Chudasama, and Rajput (2021) explain the importance of protecting systems and information from unauthorised use, disclosure, access disruption, modification, or destruction. In addition, information security relates to data integrity, confidentiality, and availability. Information security can be clearly explained when connected to the security properties of integrity, confidentiality, and data availability and information. Confidentiality refers to the security of information against theft (Wu, Dwivedi, & Srivastava, 2021), while integrity refers to protecting information against unauthorised modification, stealing, and deletion (Shukla et al., 2022). Lastly, availability means user access to authorised information at all times (Dwivedi et al., 2019).

### **2.3.1.2 Abusive Content**

Small business people connected to cyberspace may be vulnerable to cyberthreats like spam, cyberbullying, cyberstalking, violence, and pornography (Herath, Khanna & Ahmed, 2022). The abusive content can be disturbing and destructive to cyberusers as it is mainly designed to irritate people so they may accidentally click on their content. The abusive content mostly comes up as the intruding pop-up message, which aims to harm the device and results in data modification, loss and deletion. Paulsen (2016) explains that small businesses are the most vulnerable institutions as a result of cybercrimes. Therefore, the small business sectors must become aware and learn to interpret persuasive cybercrimes. Kaigorodova et al. (2019) state that in 2013, cyberrisks were in 15th place among other business risks, explaining further that the level of risks is gradually increasing. When ignored, the nature of the risk can cause uncontrollable damage of various types and magnitudes. Therefore, it is necessary to identify significant and critical risks. The Project Management Body of Knowledge (PMBOK, 2013) and Project Management Institute (PMI, 2008) suggest that many project stakeholders should participate in risk identification. A thorough process of risk identification and analysis is presented in Section D, which is then used to build the risk register.

### **2.3.1.3 Fraud**

One of the common cybersecurity risks is that SMEs are vulnerable to an invasion of the client's credit card. Literature reveals that credit cards are one of the hackers' chief targets (Kshetri, 2006). Hoffower (2018) explains that in 2018, there was an extremely high rate of credit card fraud, which occurred in several of forms of attack. This author explains that modern and innovative hackers use the latest defrauding tricks, including stealing credit card codes, unlike in the old days when attackers grabbed the card. The SABRIC (2014) report showed that credit card fraud had increased by 23% from 2013 to

2014. In monetary value, this cost R366 million in 2013 and R453.9 million in the following year. According to the SABRIC report, most credit card crimes happen through the Internet, where fraudsters apply for credit cards using false details. The fraudsters then receive the card and pin. This type of fraud went from R6.2 million in 2013 to R78.3 million in 2014. In SA, credit card fraud represents 88% of fraudulent transactions.

In the report (SABRIC online, 2014), Pillay, the SABRIC CEO, states:

When debit cards are used outside of South Africa's borders, a high percentage of the cards are used in neighboring countries such as Lesotho, Namibia, Zimbabwe, Mozambique, and Botswana. Gauteng, the Western Cape, and KwaZulu-Natal were responsible for 88% of all credit card fraud losses. Gauteng had the most credit card fraud cases, with 55% of losses in the province. Credit card fraud in Gauteng increased by 49%, from R63.5m in 2013 to R94.7m in 2014. The loss increased by 47% in the Western Cape, from R26.2m in 2013 to R38.6m in 2014. In KwaZulu-Natal, the loss increased by 18%, from R13.5m in 2013 to R15.9m in 2014. Lost or stolen card fraud increased from R7.9m in 2013 to R41.2m in 2014.

Fraud is regarded as among the most troubling and ongoing risks in the country, which requires people to be well-informed and to always be vigilant.

#### **2.3.1.4 Malware**

Malware is malicious software that spreads on computer systems, deleting files, causing system 'crashes', or stealing personal data (Kumhar, Kewat, & Kumar, 2022). It can be destructive and interfere with various computer operations (Kirwan & Power, 2012). The malware attempts can range from viruses such as Trojan, spyware, adware, and dialler. These attacks are commonly used to gain unauthorised access to all institutions. Sometimes, malware can be internally and externally generated. Employees who are not computer-literate can be the main source of malware owing to their ignorance, poor decision-making and lack of enforced cybersecurity rules (Fortuin, 2021). For example, some employees download free software from unknown sites, resulting in malware. Similarly, criminals lure people by deploying malware on attractive and interesting websites to gain unauthorised access.

#### **2.3.1.5 Information Gathering**

Information is the main asset of every organisation. These attacks primarily target gaining access to an SME's business system, which keeps track of customer information and personnel, network applications, or assets (card payment system and business applications) to run a business (Choo, 2011). Examples of information-gathering tools are sniffing, spoofing, phishing, pharming, and scanning tools. These tools are mainly used to gain sensitive and private information about the institutions. With the

rise in Internet usage, cybercriminals find innovative ways to gather data, benefiting themselves. Criminals also deploy techniques to collect private and sensitive information.

### 2.3.1.6 Availability

Non-malicious threats are part of the fundamental threats to availability. These threats can cause hardware to malfunction or fail, the downtime of software or network, and bandwidth-related issues. The criminal's primary aim is to sabotage the business and its processes, eventually harming industries by denying users access to all information systems. The denial of service, including distributed services, has become the leading business problem. When services are unavailable, they delay the business's continuity and production, which causes delayed delivery of services and dissatisfies the business clients.

### 2.3.1.7 Intrusion and Intrusion Attempts

Intrusions continue to threaten computer systems worldwide at a growing rate; for example, some advanced specialists could commit cybercrimes. At the same time, some attackers generally have access to information and tools to commit cybercrimes. Cyberrisks do not have a uniform way of attacking SMEs; instead, the risks vary from one enterprise to another. The developing trends of complex distributed systems and increased cyberspace usage raise questions about confidentiality, information security, and privacy. Owing to the high demand for IP address attacks, cyberinfrastructures become highly vulnerable to intrusions and other threats (Dilek et al., 2015). The dedicated hardware responsible for monitoring and protecting these devices, such as detectors or sensors, is insufficient. Intrusion could be in the form of criminals accessing privileged information or unprivileged applications for their benefit. At the same time, intrusion attempts could be criminals guessing passwords, new signature attacks, exploitation of known vulnerabilities, and login attempts.

The abovementioned threats relate to the ones mentioned in Figure 1-4. These threats are information security, fraud, availability, intrusion, abusive content, malware, and intrusion attempts. Each cyberthreat has its main root cause.

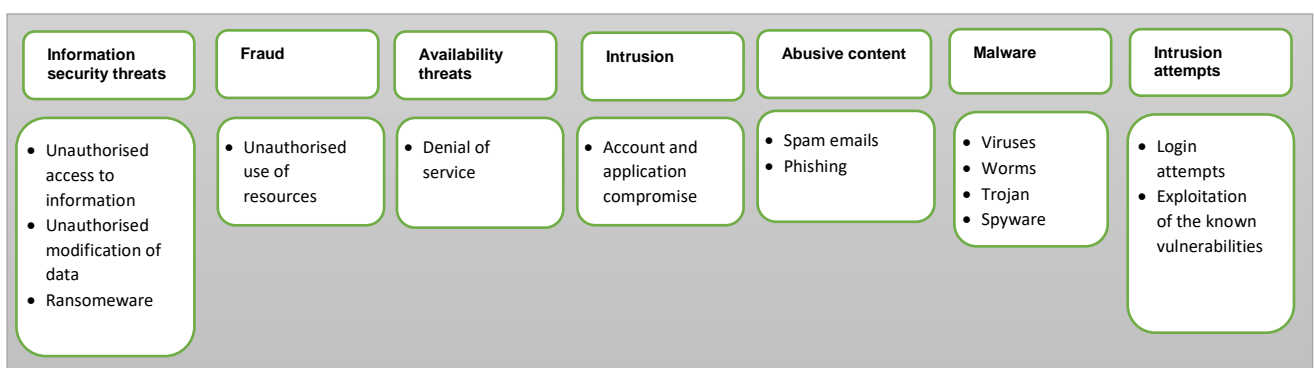


Figure 1-4: Common cyberthreats (Own work, 2021)



### 2.3.2 Security of the Business Assets

Security and safety are critical elements of every business because every business asset is constantly exposed and vulnerable to risk. Since companies use information systems for their daily activities, business assets get affected by several risks ranging from accidents, natural events, and intentional behaviour (Shukla et al., 2022). Managing information security in every business becomes essential based on various risks that expose business assets. The lack of management of business assets causes a significant challenge, leading to a considerable loss caused by unauthorised modification and deletion of information. Despite the nature and source of the risks to assets, it becomes the business owner's responsibility to manage and reduce risks properly to the fullest extent. Various agents contribute to the existence of threats in the growing small business sectors.

Thus, the main target areas in the SME cycle are the SME systems, hardware assets, and stakeholders, which are the SME's main collective components (Cisco Cyber Report, 2018). In the SME structure, the system represents the software used to run the business operating between the SME sector, their clients, and the banking system, which requires clients to transact online. In addition, all aspects of the SME sector are exposed to all sorts of risks. Section A explained that hardware, software, people, processes, and information should always be secured and protected to promote trust, privacy, and healthy surfing in cyberspace (de Araújo Lima, Crema, & Verbano, 2020). This research used information security as the measure to protect the overall components of the system comprising hardware (end devices, networking, and other shared resources), software (application and operating systems), information (processed data), people (system users, clients, and managers) and processes. Various business assets and threat agents are described below.

**Hardware:** As used in this study, infrastructure failures refer to sudden power cuts or failures, in hardware and networking equipment. At times, the user may not be informed of the event of failure until it happens, which would be the time attackers use to access the platform and the system. In addition, some equipment would not give a warning indication of the coming disruption or failure.

**Software:** Many businesses rely on a variety of software to run their businesses. Software forms one of the main components of a successful business. A software component can be an operating systems or application software that is not tangible but instructions that connect the hardware. It gives instructions for the hardware to function.

**People:** According to this study, legal agents can be SME staff members or personnel who fully control the systems. These agents usually have access rights, from access cards to biometric and system login details. As legal or authorised agents, these mediators can affect the system negatively. They can use their given access rights and privileges for their selfish desires. For example, personnel can use the access card or login details to access the business's private sections. This set of agents represents the

unauthorised attackers that aim to use every opportunity to gain lucrative benefits from the systems. Unauthorised attackers mostly use every chance they get just to satisfy their selfish desires. They can aim at gaining access to the software, hardware, system, network and personnel. They achieve their goals without user knowledge.

**Information:** The information, which is then processed data, is one of the business's assets. Some businesses use the information to market their products or as a business service. For any business, it is necessary to protect information from known or unknown risks. All organisations value their information which requires them to increase their security as it grows (Kite, 2009). A range of skills builds a strong foundation and knowledge required to promote the safety and security of information rarely found in small businesses.

**Processes:** Processes present the steps and strategies used in information systems. All business assets and their processes are not immune to risks. Processes include the phases through which data passes through before reaching the destination. For example, data can hijack access to the data storage, transmission medium and end devices, and user practices and behaviours during the transmission period. A general description of risk is explained below.

## 2.4 RISK OVERVIEW

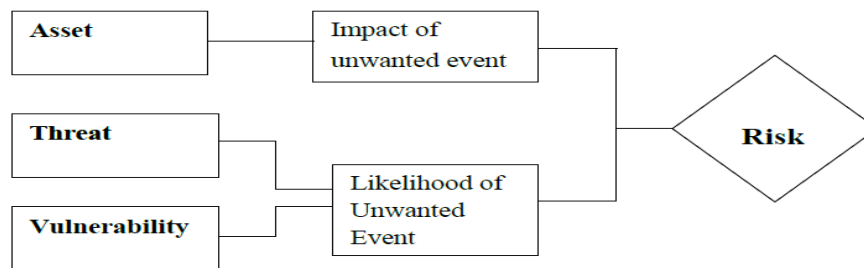
Risk indicates a negative impact, danger or possible harm, or malicious act (Crovini, Santoro & Ossala, 2020). As described by ISO Guide 73, 2009, the term is used by both people and businesses to take measures or control of a particular situation. Thus, risk management is when one acts appropriately. The term 'risk' can be used differently by various disciplines. For instance, risk can be both a loss and a profit in a financial field. As a result, there are two possible risk outcomes, which are adverse or specific risks (Wen et al., 2021). For example, when a company trades with a particular portion of the money, which brings profit, it becomes a real risk. The risk is equivalent to the expected loss. It can also be a mixture of the likelihood of an event and the impact it has (ISO, 2002) with the probability of a negative outcome (Graham & Weiner, 1995).

A risk is a quantitative measure of potential damage caused by a specific threat. It is an adverse risk when the company trades and loses what it has put in. ISO Guide 73 (2009) defines risk as the likelihood of loss and the probability of an outcome different from the one expected. At the same time, the likelihood of a breach or a security incident is a function of a threat appearing and the probability that the threat will be successful (which is relative to successfully exploiting a vulnerability in the system) (IBM, 2018). Some authors believe that the rate of interest, supply chain risks, growth risks, prices of the raw material risks, electronic business and technological risks, and employees and management risks are the main types of risks that SMEs generally face (Falkner & Hiebl, 2015; Alahmari & Duncan, 2020). On the same note, the risk presents a business uncertainty with regard to meeting the objectives

(ISO, 2009). This study focuses on electronic business and technological risks, mostly known as cyberrisks or cybersecurity risks. These cyberrisks are presented below.

### 2.4.1 Cyberrisks

The Covid-19 pandemic introduced an instant transition from using face-to-face to online platforms of communication. All institutions were forced to rely upon and use the convenient cyberspace to perform daily business activities, which exposed SMEs to various risks relating to threats, exposure, and vulnerability (Eybers, & Mvundla, 2022). As long as SMEs rely on technology for productivity and day-to-day operations, this business sector will have cyberrisks. A threat presents a hazard, which exposes assets to threats and renders them asset vulnerable (Tiwari, 2010). Crichton (2009) describes the risk triangle as a hazard, exposure, and vulnerability. Figure 2-5 shows the links between the business assets, their exposure to threats, and vulnerability.

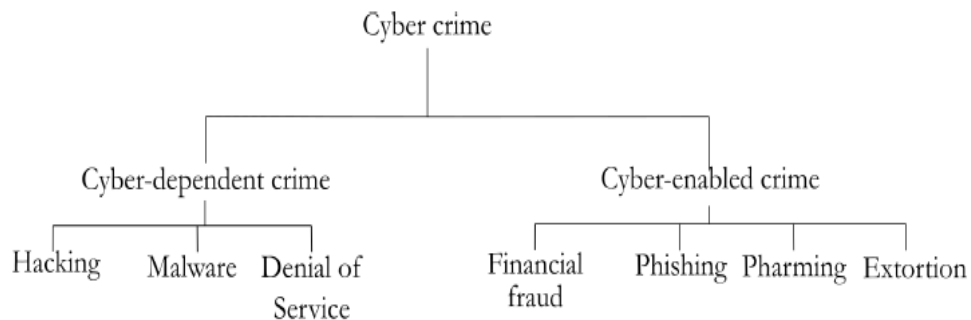


**Figure 2-5: Relationship between the asset, threat, and vulnerability (Source: Moyo, 2014: 47)**

Cyberrisk is any risk or ‘financial loss, disruption or damage to the reputation of an organisation’ from any failure in their IT systems (Goldenson & Goldenson, 2018:2). It is how cyberattackers gain access to businesses and problems caused by people (Steve, 2017). However, SMEs are not like big companies that make risk management an integral part of their business components. Goldenson and Goldenson (2018) explain that cybercrime represents incidents that aim at any form of attack in a business. As network users mostly use social platforms to communicate, cybercrimes could represent the computer-generated activities that attack the service (Choo, 2011).

Choo (2011) cited cybercrimes on networked computers. These would include computers that are used to commit common crimes. These cybercrimes include child pornography, theft of intellectual property, computer network crimes, and common crimes where the evidence is digital (Broadhurst & Chang 2013). These crimes differ from one business to another. Cybercrimes occur regardless of the size and physical location of the business. The risk could bring either an opportunity or a threat to the business sector. To gain more money and competitive exposure, SMEs take chances when they take a business from one level to another, thereby exposing the business to cyberthreats and eventually leaving them vulnerable.

Some literature explains that risk is possible exposure to harm or danger, resulting in the loss of value or assets to the business (Richards, 2017). Figure 2-6 illustrates cybercrimes that can depend on and be enabled by the Internet. Examples of cyber-dependent crimes are malware, hacking, and denial of service. Cyber-enabled crimes include financial fraud, phishing, pharming, and extortion.



**Figure 2-6: Cybercrimes (Lallie et al., 2020)**

In reality, exposure to cyberrisk can have two possible positive or negative outcomes. A positive outcome is the results that are expected, while negative results are from the cyberattacks that intruded onto the system to gain unauthorised access (Eybers, and Mvundla, 2022). SMEs cannot separate their businesses from the Internet platform because cyberspace has become the driving tool for both SMEs and hackers. As explained earlier, cyberspace acts as a channel for positive and negative risks. Figure 2-7 shows the top common risks in 2017 that SMEs experienced (Haward, 2018).

Rank		Percent	2017 rank
1	Business interruption (incl. supply chain disruption)	33%	2(27%)
2	Cyber incidents (e.g. cyber crime, IT failure, data breaches)	30%	6(22%)
3	Natural catastrophes (e.g. storm, flood, earthquakes)	28%	4(25%)
4	Market developments (e.g. volatility, intensified competition/new entrants, M&A, market stagnation, market fluctuations)	27%	1(32%)
5	Changes in legislation and regulation (e.g. government change, economic sanctions, protectionism, Brexit, Euro-zone disintegration)	22%	3(26%)

**Figure 2-7: Top common risks for SMEs (Adapted from Haward, 2018)**

South Africa has become a victim of cybercrimes. The estimated rate is one in three businesses has been hit by cybercrime (IOL, 2017). The estimated cost of cyberrisks in this country is R2.2 billion a year, making it among the top three countries to be attacked in the world. As the country’s businesses are gradually adopting and using technology, the research indicated further that SA businesses are among the top victims of cyberattacks among other African countries. The Cisco Cyber Report (2018) shows

that ransomware contributes to cyberrisks in the SME sector. Some literature suggests that some cyberthreats are unknown and not published owing to the business's fear of a reaction. Fripp (2014) states that if cybercrime were a nation, it would have been the 27th biggest regarding GDP and cost the global economy \$445 billion a year. In SA, cybercrime has an economic impact equal to 0.14% of the national GDP – about R5.8 billion a year.

In the same manner, cyberattacks increase daily in Africa and other continents. The evidence is after realising that hackers and cyber-attackers have implemented new strategies, as discussed at the third Africa Cyber Security Conference in Abidjan, Ivory Coast (Adepetun report online, 2018). Micheal Bobillier explained that cyberattackers had formed traditional societies with 'real structured ecosystems, with a great deal of money and technology.' At the same conference, Auguste Diop, a speaker, and the managing director, added: 'Cybercriminals worldwide amassed a staggering \$ 3,000 billion (2,600 billion €) in 2015', a sum he expected to double by 2021 (Adepetun report online, 2018).

With these statistics, there is a very high need to conduct cyberrisk analysis in SMEs. Risk analysis reviews potential risks that could serve as a threat in a specific sector. Cyberrisks can be qualitative or quantitative; they can be analysed primarily to identify and manage significant threats that could negatively affect the business (Shuttleworth, 2017). However, risk analysis cannot be separated from risk management in the business sector. Risk analysis involves identifying all possible business threats ranging from assets to existing and emerging threats, as well as vulnerability. A proper risk analysis saves time, money, and business reputation (Vaughan & Vaughan, 2001). Cyberrisks attack SMEs in this country and affect other SMEs in other countries. The research was also conducted on e-commerce security in the SMEs in Kenya to reveal major cyberthreats and their countermeasures (Ngugi, 2016).

## **2.4.2 Sources of Cyberrisks**

According to Alahmari and Duncan (2020), there are five main sources of cybersecurity risks in SMEs. These cybersecurity risks include the practices, awareness, behaviour, and threats to decision-making. Each of these risks is described below.

### **2.4.2.1 Decision-Making**

Decisions in every business are made by the top management and the business owners. As a result, the top leadership in enterprises is the key driver for implementing cybersecurity. However, poor decisions will be made if the top management is not well informed. Therefore, it is essential for the business and the business owners to acquire detailed information from experts (Barlette, Gundolf & Jaouen, 2017). Furthermore, according to Alahmari and Duncan (2020), decision-making is an essential part of a

successful business; therefore, top management and experts should acquire adequate information and procedures that will help to promote relevant awareness and implementation of cybersecurity.

Even though the Covid-19 pandemic has suddenly forced businesses to rely on convenient Internet use, many companies have fallen into the trap of acquiring information from the open Internet. The acquired data are mainly used for decision-making, which affects the state of their cybersecurity. In such circumstances, quick and unreliable decisions could negatively affect businesses applying security measures. Therefore, the direction SMEs take in their businesses depends solely on the quality of their decision-making. Usually, the abilities of businesses' decision-makers are reflected through their roles (Osborn & Simpson, 2018).

#### **2.4.2.2 SME Cybersecurity Practices**

According to Alahmari and Duncan (2020) and the literature, SMEs lack strategies to combat cybersecurity threats. Even during the challenging time of Covid-19, some SMEs do not have reliable measures to guard against various threats. As a result, most SMEs do not consult professional practice. Internet availability fuelled the situation with free advice from legitimate and unauthorised sources. The bad practice of using available guidance from cyberspace opens a loophole in the businesses, especially since bad practice invites unauthorised parties to contribute to risky practices. The act could be out of a lack of knowledge, which creates opportunities for cybercriminals to benefit. Likewise, poor practices directly affect safety, security, trust, and privacy (Gundu, 2019).

As cited by Dirgiamto, Abdullah, and Ali, (2020), some SMEs do not even reach out to other SME communities, which could help them grow and gain more knowledge to practice. The lack of engagement with other fellow SMEs restricts the efficiency and effectiveness of peer learning to address seasonal cybersecurity threats. Even though some SMEs outsource certain business services, that does not replace the proper and good practice of cybersecurity measures to improve the security of the business. It is suggested that small businesses promote more engaging education and training to bring more awareness that can be measured by best practices (Gundi, 2019; Alahmari & Duncan, 2020). The availability of clear policies and rules should be priorities for promoting safe surfing and good cyber hygiene practice for SMEs.

#### **2.4.2.3 SME Cybersecurity Awareness**

The high ignorance of the user's awareness about cybersecurity opens a loophole, danger and risks to business assets (Alahmari & Duncan, 2020). A lack of knowledge about cyberthreats, vulnerability, attacks, and their impact mainly causes risks to businesses, ultimately affecting user awareness (Osborn & Simpson, 2018). The lack of cybersecurity awareness determines the business's failure or success and

its cybersecurity plan. Their awareness helps to use proactive mitigation strategies to prevent known and unknown security attacks. In the same light, user awareness helps to adopt acceptable behaviour and attitude (Bada, Sasse & Nurse, 2019).

Alahmari and Duncan (2020) believe that businesses mostly require information to make them aware of cybersecurity risks rather than adopting a tool for risk assessment. In this regard cybersecurity awareness programs should be implemented regularly to bring awareness, decrease cyber risks and promote a safe environment. Among other risks with which SMEs are faced, cybersecurity risks have become the main challenge. Even though the literature addressing mitigation strategies have been growing, strategies alone are insufficient. Awareness should also be prioritised and recognised to develop and apply appropriate security measures (Kabanda, 2018). Cybersecurity awareness can also link to the cybersecurity behaviour of business people towards business systems.

#### **2.4.2.4 Behaviour in SMEs**

Most behaviour of employees in the SME sector becomes the primary target of cybersecurity threats. Some SMEs don't pay attention to business policies, guidelines, standards, rules, and procedures. The lack of knowledge of such information ultimately leads to exposure to all sorts of cybersecurity threats. In addition, regular cybersecurity education and training are essential components for improving knowledge (Alahmari & Duncan, 2020). Even though cybersecurity and its risks do not guarantee acceptance and proper behaviour (Gundu, 2019), the commitment and behaviour of all employees contribute to improving the safety and security of all business assets. Literature mentions that some businesses fail to comply with business policies, but the main problem of cybersecurity is a lack of knowledge and awareness that affects behaviour and attitudes negatively (Kaur & Mustafa, 2013). Similarly, employee behaviour and attitude should inform knowledge and awareness of cybersecurity.

#### **2.4.2.5 Threats**

In SA, the healthcare and financial services industries have been the victims of cybercriminals resulting in increased cases and great concern (Blue Turtle Technologies, 2020). With the ignorance and lack of safety practices to promote good cyber hygiene, SMEs remain the target for cyber threats, especially those looking for lucrative benefits from cybercrimes.

### **2.5 SMEs' PERCEPTION OF CYBERRISKS**

The use of the Internet and technologies has increased in this era. Its growth has gradually influenced customers and small businesses to connect to cyberspace fully. In the same way, cybercrimes and risks have found their way into the SME sector. The increased dependency on ICT has benefited both businesses and attackers (Almeida, Carvalho & Cruz, 2018). As used in the study, SME customers and personnel could be any client using the network platform to communicate with the recipient on the other

side. Even though attackers may use various tricky methods to access an individual’s space, these attackers may be using software that seems legitimate for gaining access (Jain, Sahoo, & Kaubiyal, 2021). Attempts to receive authentication from customers and personnel may be a form of attack. In such cases, a user may not know the criminal's plan on the network. The cyberattacker may tamper with the confidentiality of the message while the user may be working on the system, assuming that they are working with the correct recipient (Suh & Han, 2003). Figure 1-8 shows a clear example of such an action and a scenario.

Cyber risks exist regardless of the size of the business. Cyberattackers will live for as long as the company relies on IT and its infrastructure for day-to-day business operations. Despite the whole perception of the SME operation, cyberattackers' reality exists when ICT is an integral part of the business.

## 2.6 CYBERCRIMES

Cybercrime is an umbrella term for unlawful behaviour conducted through networked and stand-alone electronic devices. The behaviour disrupts the operations of the systems and their state of security through intrusion, hacking, data leaks, online scams, software piracy, mobile and money fraud, and cyberterrorism. The exponential growth in the high dependency and use of the Internet during the so-called ‘new normal’ Covid-19 pandemic increased cybercrimes (Setiawan et al., 2018; Eian et al., 2020; Eboibi, 2021). According to Business Tech (2020), the top Covid-19 scams relate to those illustrated in the following chart.

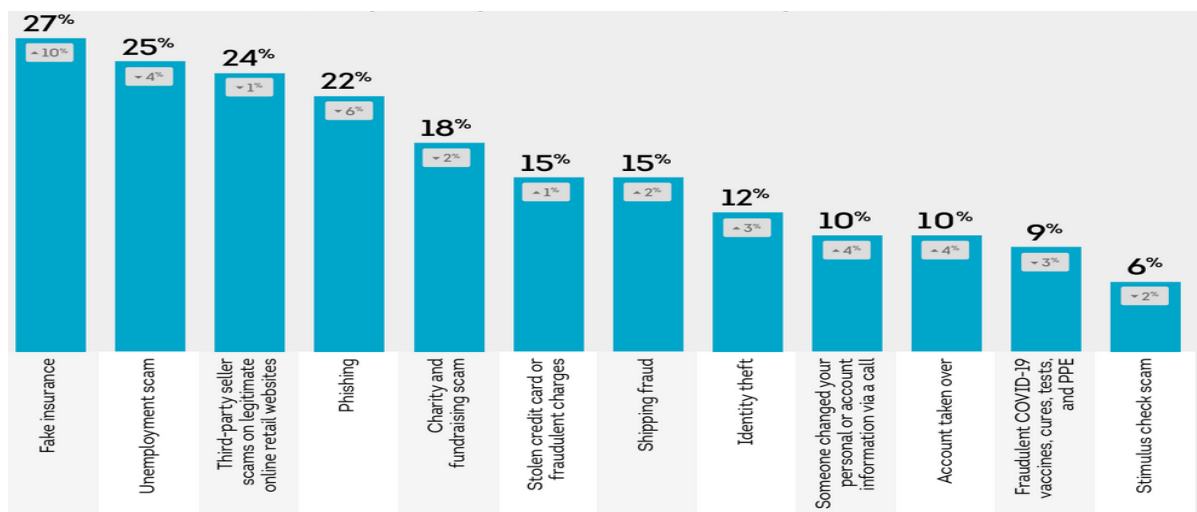


Figure 1-9: Top Covid-19 scams (Business Tech, 2020)



### 2.6.1 Financial Costs of Cyber Crimes

The high increase and impact of cybercrime in the small business sector significantly contribute to the economy. Sizwe Dlamini explained that data breaches are a threat affecting SA businesses, with an average cost of R40.2 million per breach. He further emphasised that 'In South Africa, the three root causes of data breaches identified as a malicious or criminal attack (48%), human error (26%) and system glitches (26%)' (Falcon Report online, 2020).

The following figure shows the statistics of cybercrimes in Africa.



Figure 1-10: Africa cybersecurity report (source: Serianu, 2017)

According to the Cisco Cyber Report (2018), SA is one of the most susceptible countries to cybersecurity. As cited in the survey by the DTSP (2017), various cybersecurity threats hit SA from November 2015 to December 2016.

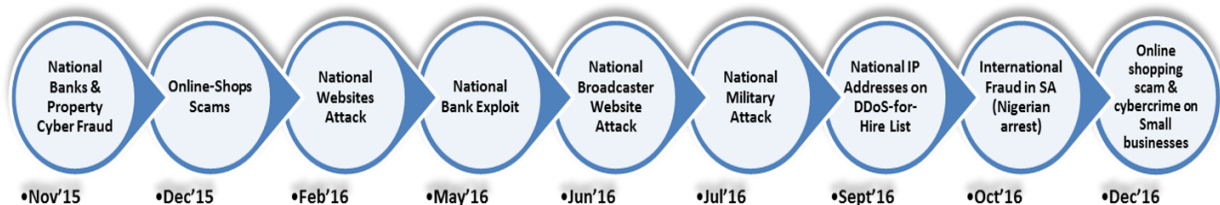


Figure 2-11: Cyber-security briefing (Source: DTSP, 2017)

A thorough breakdown of the cybersecurity incidents can be seen in Figure 2-12

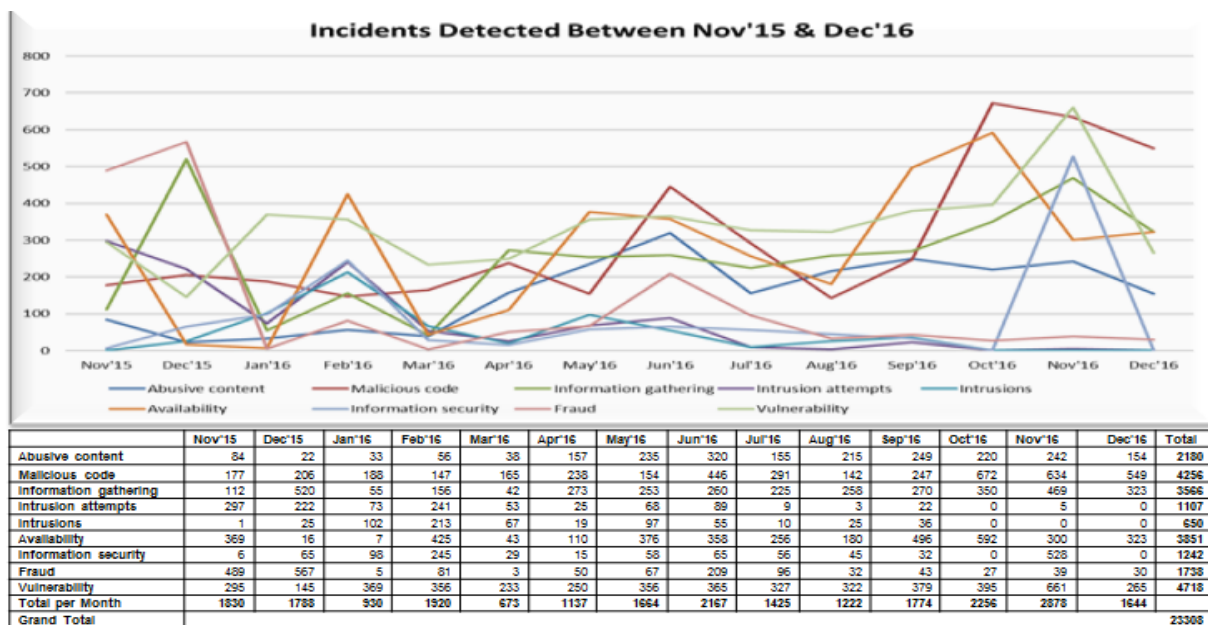


Figure 2-12: Cybersecurity incidents from November 2015 to December 2016 (adapted from DTPS, 2017)

## 2.7 CYBERRISK MANAGEMENT FACTORS IN SMES

There are several cyberrisk management factors that are essential for the improvement and maintenance of business continuity. These management factors are addressed below.

**Training and Awareness** - Awareness brings clarity and improves cybersecurity in any organisation. Ongoing training reduces the risk of employees being negligent by making decisions that undermine the security of an organisation's information (Teufel et al., 2020). Scholars have explained the necessity for continuous training, which ultimately brings awareness to employees at large. A lack of relevant support or training sometimes makes unacceptable user behaviour worse. (Ncubekezi, 2021).

**Third-Party Management** - The absence of structures, especially those focusing on the safety and security of information, becomes the challenge of various cyberattacks. Cybersecurity becomes the protection between the business and the vendors, including intruders. With proper and straightforward management of vendors, the state of cybersecurity can be improved.

**Employee and Management Attitude Toward Cybersecurity** -Even though the small business sector is highly exposed to cybercrimes, insiders also play a role. The insiders' attitudes, actions, and behaviour can be hazardous for businesses (Annarelli, Nonino & Palombi, 2020). As a result, the employees render the most significant threat (Solveve, 2021). Ncubekezi (2021) defines insiders as the weakest link of the business. The insiders presents employees who are ignorant and have a negative attitude when working on the system. Scholars argue that employee ignorance and attitude toward cybersecurity often open

doors for various cybercrimes (Sasse, Brostoff & Weirich, 2001). Management should lead and influence employees' attitudes by offering adequate awareness about cybersecurity. All organisations' cybersecurity should be controlled and managed by dedicated personnel.

The research indicates that most small businesses do not have a well-skilled person in management. For information privacy, safety and security, management involvement should be prioritised by all business sectors (Kobis, 2021). Attitude, actions and behaviour play a vital role, especially at the management level, when policies, rules and procedures can be enforced and monitored (Ncubukezi, Mwansa & Rocaries, 2020b). Consequently, employees would improve if there could be motivation from management. Certain user attitudes impact on common errors; for instance, when a user insists, 'It won't happen to me' (Richardson et al., 2020:31).

## **2.8 IMPACT OF CYBERRISKS IN THE BUSINESS SECTOR**

Cybersecurity is a remarkably ignored component of the SME business life cycle. Society interprets SMEs as independent businesses not concerned about the company's security (Howard, 2018). Cyberrisk exists with or without the business owner's knowledge as the cyberattackers initiate these attempts for various reasons. The cyberattackers do not let the transaction opportunity cease. They are always alert to any activity in cyberspace. Any activity on the system is bound to produce an outcome. Outcomes can either be positive or negative. However, a positive business outcome can result from the simple, clean system used by the business parties, such as the business personnel, the method used to process activities, and the customer. As a result, some SMEs only wake up after severe cyberattacks.

If there are no cyberattacks on the business or client, the company runs smoothly and produces the desired results. However, if an intentional cyberattacker wants to access the transactions, the outcome will only favour the attacker. That would mean the business or system is vulnerable to attackers and ultimately does not produce the desired results. The effects of adverse consequences could affect the business in many ways. For example, the outcome could affect other businesses or customers (Sen, Ahmed & Islam, 2015). In the same way, this could lead to business throughput delay and, eventually, business failure. There is no business that is immune to cyberattacks. Each business sector is directly affected by physical, digital, economic, psychological, reputational, social, and societal harm, which is explained in the following section.



Figure 2-13: Cyber harm in business sectors (Source: Agrafiotis et al., 2018)

**Economic harm** - A severe attack can result in wasted time, which does not bring profit, while businesses' primary purpose is to generate profit. As a result, South African companies contribute more to GDP to help alleviate poverty. These harms include disrupted operations and sales, reduced customers, fewer sales and investments, financial theft, extortion payments, loss of jobs, and increased scammers. Figure 2-13 summarises the categories of cyber harm in business sectors.

**Business Delays** - Cybercrimes committed by hackers could delay daily business routines. So, each day the delay happens, the production process will also be affected. For example, if an SME usually

generates thousands of rands, then these SMEs will be affected and only create tens or hundreds of rands, depending on the impact of the delay (Ajayi, 2016). The continuous business delays ultimately result in business discontinuity. Business delays can be internal or externally caused by suppliers and third-party vendors.

**Societal Impact** -Cyberattackers can harm businesses in the comfort of the communities where they have built their clientele (Gashami, Libaque-Saenz, & Chang, 2020). These societal harms could include negative changes in public perception, disruptions in daily routines and activities, a drop in the performance of the internal staff, and a change in the economy (Hertati et al., 2020). Businesses could lose their potential clients and other business prospects, significantly damaging society. Clients would leave and seek new suppliers, and the business's continuous delays could eventually lead to the small and medium businesses' complete breakdown or failure.

**Reputational Effect** - Regardless of their size, customers would invest based on the reputation of the business and the response time in the business world (Lee, 2019). Therefore, any adverse action may affect the business and benefit competitive businesses. As the SME would still strive towards ensuring that the business runs smoothly, the hacker or cyberattacker would be aiming to benefit in the process and eventually dent the business's reputation. Clients would only invest their money where the business has a good reputation, while a negative business reputation could result from the continually poor and delayed delivery of the products (Talwar et al., 2021).

**Psychological impact** - Business people suffer from worry, embarrassment, and guilt in any psychological situation, such as confusion, discomfort, frustrations, worry, anxiety, loss of confidence and satisfaction, or a change of perception (Acuti, Pizzetti, & Dolnicar, 2022). Some people become more stressed, frustrated, depressed, and anxious when specific attacks hit the business. So, any form of discomfort results in psychological harm to business owners.

**Investments and Monetary Loss** - One of the rapidly increasing crimes in cyberspace is gaining access to people, business investments, and finances. Reports state that over 60% of cybercrimes are conducted to target banking and monetary institutions (Kshetri, 2006). As technology advances, the use of online banking and transactions are growing. As a result, many people become reluctant to stand in bank queues, preferring Internet banking. Kshetri (2006) also explains that there are lucrative benefits for virus writers and hackers.

## **2.9 SECURITY MEASURES**

Cybersecurity measures have become the number one solution for every business institution (Davis, 2014). The cybersecurity measures aim to secure business information, including finances and customer information. In addition, security measures should prevent cyberrisks resulting from the different kinds

of cyberthreats such as malware, unauthorised access, phishing and network intruders, human factors, faulty devices, and lack of policies and guidelines. Cybersecurity measures can be used to protect the network, physical end devices, software, processes, and people. To protect end devices, people use antivirus software and enforce strong or complicated passwords (Totade et al., 2022). People use encryption software and firewalls to filter the traffic for network devices. It is also suggested that people should never open an email from an unknown sender and should perform a regular backup of information. Administrators should stipulate strict access rights to sensitive information (Zhang et al., 2023). Lastly, like any other business, SMEs should enforce employees' cyber-security policies, standards and rules.

## **2.10 CONCLUSION**

This chapter presented the relevant literature on small and medium-sized businesses and the impact of using cyberspace as a technological platform to perform their daily activities. A criterion used to select the SME for the study was also clearly explained. The increased usage and dependency on the platform expose businesses to cyberrisks. Cyberthreats and attacks affecting SMEs, their root sources, and their impact on their flow of information are explained. The chapter also addressed the security of information in open cyberspace. Cybercrimes, sources of security threats, and security breaches were explored.

This chapter concludes that the increased usage of cyberspace equally gave access to both legitimate users and criminals. Even though users such as SME employees use cyberspace for various business activities, cybercriminals use innovative strategies to expose SMEs to a range of cyberrisks. This requires SMEs to look closely at cybersecurity risk management strategies that will improve the safety and security of the business assets. The process of risk management requires every business institution to protect its information and other assets. The security of various business assets should be considered and improved by applying proper measures aligned with the organisations' cybersecurity framework.

The following section presents the analysis and the design of the cybersecurity risk tool for SMEs.

# SECTION B: ANALYSIS AND DESIGN

## SECTION B: ANALYSIS AND DESIGN OF THE TOOL

Research methodology

Results and discussions

Design of the risk tool



This section presents the analysis and design of the cybersecurity risk tool. This section consists of Chapters 3, 4, and 5. So, this section builds up the knowledge base for developing the cybersecurity risk tool, which uses the AgenaRisk package. The content on each chapter is presented below.

**Chapter 3:** Presents the method of inquiry used to carry out the study, the selection of the research participants, and the application of the risk management techniques.

**Chapter 4:** Presents the analysis, interpretation and presentation of the collected results from the research participants.

**Chapter 5:** Presents the relevance of the National Institute of Standards and Technology (NIST) framework and the design of the cybersecurity risk tool.

## **CHAPTER 3: RESEARCH METHODOLOGY**

### **3.1 INTRODUCTION**

The term 'research' has been used and described by scholars and other researchers in various ways. It aims to understand the underlying complexities of human knowledge, skills, and experiences (Kumar, 2019). Brown and Dowling (2001) believe that research should realise, describe and better understand a specific area, field, or practice. Saunders, Lewis, and Thornhill (2009) understand research as an inquiry to systematically discover new things and facts to increase knowledge. The current study applies the same processes in the definitions above to find new facts and evidence relating to its phenomenon. Section A of this research identified the main problem of this study, and this part accounts for the research methodology used, which is guided by the research questions.

This chapter describes the processes and stages of conducting this research and also justified the method used. The selection of the research participant selection, the process of data collection, and data analysis, introduction to risk assessment are also accounted for. The chapter ended with a discussion of data storage and management as well as ethical considerations.

### **3.2 SCOPE OF THE STUDY**

This work presents a case study research for small and medium-sized businesses in South Africa (SA). The criteria for the SMEs are that they can be from a business sector that uses ICT to run the business, have a maximum of 150 employees and make a minimum of R150 000 a year. The study aims to design, develop and evaluate a cybersecurity risk tool for small and medium-sized enterprises.

The study used the ISO 31000:2018 risk management standard that determines the qualitative cyber risks faced by SMEs across multiple business sectors to calculate the risk matrix based on the cyber risk likelihood and the risk impact. In addition, the study conducted a quantitative risk analysis to assess the severity of the consequences by using decision trees and scenario analysis; the study also performed a sensitivity analysis and determined the expected monetary value (EMV). To better understand different risks, the study also adopted NIST as the cybersecurity framework that helps to guide and manage cyber risks. Lastly, the study used the AgenaRisk package with Bayesian Network tools to examine the risk probability and impact by demonstrating the variables used and simulating the relationship between the variables.

### **3.3 RESEARCH PHILOSOPHY AND DESIGN**

The current study used a pragmatic philosophy, emphasising what works in a specific investigation rather than contentions about truth and reliability. This approach supports risk management strategies, methods, and procedures, recognises each method's differences, similarities and limitations, and promotes a combination of these elements to complement one other.



The research design is a comprehensive plan to execute the study, including answering the research questions effectively and efficiently (Babbie & Mouton, 2011; De Vos & Fouche, 1998). The research design explains the study's detailed plan, which provides an overall framework for the process of research (Leedy, 1997). It also presents a planned strategic framework to bridge the research questions, process and strategy used in research (Durrheim, 2004). The above descriptions explain that the research design answers the research question and addresses the research plan. Similarly, in this study, the processes used in the research approach, strategy and method to achieve the main aim are described and accounted for.

### **3.3.1 Research Approach**

A distinction approach is made between the inductive and deductive research approaches. The inductive approach focuses on the specific to the general application, while the deductive or reasoned approach concludes with general assumptions (Soiferman, 2010). Inductive reasoning develops a theory, while deductive reasoning tests an existing view. This study adopted the inductive method, which proposes a cyberrisk tool for small and medium-sized SMEs. The inductive approach is explorative and involves logical thinking that combines the observations from the simulations with practical information to conclude. The Bayesian network tools in the AgenaRisk package simulate the risk probability and its impact on SMEs. This study's inductive nature helped the researcher conclude with a set of specific business experiences.

### **3.3.2 Overview of the Qualitative Approach**

Qualitative research studies the nature and phenomenon of the research field by gathering data through open-ended questions. It mainly focuses on non-numerical data to understand and interpret concepts and experiences (Busetto, Wick & Gumbinger, 2020). Qualitative research answers why something is or is not and focuses on the interventions to improve situations. This study clarified the common cybersecurity risks businesses experience and the mitigation strategies used to reduce risks. The study seeks clarity on the small business experiences when using cyberspace as the platform for information exchange. The study determined cybersecurity risks, threats, cyber-attacks that dominate the small business space, and the current mitigation plans. The data-collection methods are interviews, qualitative surveys, document studies, focus groups, and participant observations. For this study, interviews were used with open-ended questions to gather relevant information about cybersecurity risks in the SME sector. The data-collection section describes the interview process and qualitative surveys.

### **3.3.3 Participants' Selection and Sampling**

A sampling process selects a specific group that will be used to collect data from and is less than the population. The population presents small and medium-sized enterprises using cyberspace to run their

businesses. While ‘population’ represents a set of interrelated organisms in a specific homogeneous area, a group of people within the same area, ‘sampling’ seeks to access a subset called a sample from the entire research population (Babbie & Mouton, 2001; Rahi, 2017). While the probability sample grants equal chances to the participants, the non-probability sampling technique does not randomly select the participants (Babbie & Mouton, 2001). Probability sampling involves random selection, allowing you to make strong statistical inferences about the whole group. Non-probability sampling is a non-random selection based on convenience or other criteria, enabling you to collect data quickly.

These research participants were selected from different provinces in SA, operating in various business sectors. The selected respondents present a good choice as they all have the same interests in contributing to the GDP. So, as shown in Table 3-3 a total of 45 respondents from the functional businesses during the Covid-19 pandemic were selected using purposive sampling. The data were collected using the designed questionnaire deployed in Google forms owing to the national lockdown, which restricted face-to-face communication. Interviews were conducted via online platforms. Purposive sampling was used to extract a lot of information out of the collected data and explain the impact of the findings. The research gathered qualitative and quantitative data about the existing cybersecurity risks, their impact, likelihood and current protection measures.

The study participants are a combination of females and males aged between 25 and 55, presenting business managers, chief information officers and Information Technology (IT) managers with similar characteristics. These were the units of analysis showing the main entities of the study. As shown in Table 3-3 the respondents were selected according to the following criteria: the number of employees per SME is not more than 150, selected per province, and the minimum annual turnover of one hundred and fifty thousand and not more than R1 million. The researcher targeted a small number of well-informed respondents from the following sectors: ICT, transport and motor trade, manufacturing, retail, electricity, gas, water, accommodation, catering, waste management, real estate, community and construction.

A summary of the sampling table is illustrated in Table 3-3.

**Table 3-3: Sample Summary**

*Notes: Western Cape (WC), Eastern Cape (EC), Northern Cape (NC), Free State (FS), KwaZulu-Natal (KZN) and Gauteng (GP)								
Research Approach	Data Collection Method	Data Source	Units of Observation	Units of Analysis	Sample per Province Interviews = I; Survey = S	Sample Criteria	Methodology	Data Analysis, Representation and Interpretation
	Read, write and analyse	Literature review	Journals, books	SME members from	<b>Sample =45</b>	SMEs in SA	<ul style="list-style-type: none"> <li>Qualitative method</li> <li>Risk management methodology</li> </ul>	<ul style="list-style-type: none"> <li>Thematic analysis</li> <li>Descriptive statistics</li> <li>Tables and graphs</li> <li>Qualitative and Quantitative risk analysis</li> <li>Sensitivity analysis with AgenaRisk package</li> <li>Decision trees</li> <li>Tornado graph</li> <li>EMV</li> </ul>
Qualitative	Online open-ended interviews	<ul style="list-style-type: none"> <li>IT and the business managers</li> <li>Employees</li> <li>Chief information officers</li> <li>Technical departmental head</li> </ul>	<ul style="list-style-type: none"> <li>IT department</li> <li>System users</li> <li>Network support division</li> <li>End-user support</li> <li>Finance department</li> </ul>	<ul style="list-style-type: none"> <li>Waste management</li> <li>Transport and motor trade</li> <li>ICT</li> <li>Electricity, gas and water</li> <li>Real estate</li> <li>Accommodation and catering</li> <li>Manufacturing and retail</li> <li>Construction</li> </ul>	<ul style="list-style-type: none"> <li>WC: I=2 &amp; S =9</li> <li>EC: S =8</li> <li>NC : S = 6</li> <li>FS : S = 6</li> <li>KZN: S=8</li> <li>GP : S = 8</li> </ul>	<ul style="list-style-type: none"> <li>SMEs should</li> <li>Have 1-150 employees</li> <li>Should be SA based on business</li> <li>Be in any business sector</li> </ul>		
Quantitative	Closed-ended questions on a survey via phone and email							

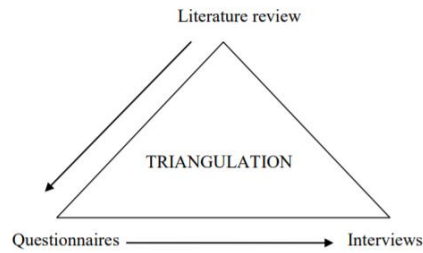
### 3.3.4 Data-Collection Process

The study participants received emails that invited them to participate in the open-ended qualitative questionnaires and interviews. The researcher chose the qualitative survey because of the global lockdown restrictions from the Covid-19 pandemic. The participants accessed the survey, which was on google forms. All the questions answered the main research question stated in the introductory

chapter. Most participants completed the survey, and most were unavailable for the interviews because of the pandemic. The combination of the two data collection methods was a success. The online survey was distributed via emails, in person, and by means of phone calls. The participants were given a link to the survey questions to click on and join in the study.

### 3.3.5 Data-collection methods

Mouton (2006:164) encourages primary and secondary data sources in research. The study triangulated the data sources: primary (interviews and questionnaires). Interviews and qualitative questionnaires were used to gather data from the selected sample of the study. Interviews were conducted with the security specialists, and the questionnaires were used for the business managers, IT managers, and chief information officers. The interviews and questionnaires provide exploratory and qualitative data. The used data sources are triangulated to achieve the study's main purpose.



**Figure 3-14: Triangulation of data sources**

At the beginning of this work, the researcher reviewed the latest relevant literature about the impact of cybersecurity crimes on SMEs in SA to develop a cybersecurity model for SMEs guided by the NIST framework. The literature came from accredited journal articles, theses, academic websites (google scholar), and databases available on the university's websites, textbooks consulted online and the university's library, and other accredited online research websites (Research Gate). The literature review determined how other researchers have addressed the research problem. The process assisted in articulating the main research aim and objectives, as stated in Section A. The related literature about SMEs, cybersecurity risks, prior indicators, cyberthreats, and attacks and protection measures are discussed in detail in Section A. The study used keywords to search the latest and related literature. After a thorough literature search, the researcher selected a research method that best-suited cybersecurity risk management, a cybersecurity framework using the AgenaRisk package with Bayesian Network tools to design, develop and evaluate the cyberrisk model for SMEs.

The following section presents the details of the data-collection methods used.

### **3.3.5.1 Interviews**

Interviews were conducted with the two selected research participants to understand what their perceptions are about cybersecurity risks, risk likelihood, impact, and protection measures. These participants were from the Eastern and Western Cape and were the only experts available for interviews. The study participants were contacted via telephone and email and their permission was granted to be part of this study. The researcher scheduled appointments a week in advance with the interested participants. The researcher asked open-ended questions to address the study's primary aim. Even though interviews may be time-consuming and impractical depending upon the numbers, this study provided an opportunity to clarify specific questions. The interviews are impractical in the sense that most people do not respond to the emails especially during the sudden global Covid19 pandemic which quantified the cybercriminals. So, for safety reasons, people are mostly not keen to respond to emails.

- **Interview Process**

The interviews required a conversation between the researcher and the participant. After introducing herself, the researcher provided a brief background about the study and how the participants fitted in. The researcher did not use abbreviations during the interview process. Appendix A outlines both the research participants who were given a research consent letter. The consent letter briefly introduced the study, followed by the research aims and consent to participate. The researcher asked permission to record the interview since the information from the interview needed to be documented. The research participants were assured that the information shared would be treated with the utmost confidentiality. In addition, the interviewees were told that data aggregation would reduce any possibility of the subjects being identified. She used a high-quality Sony digital recorder to record the interviews clearly and unobstructed. The method of recording was preferred so that the researcher could listen instead of writing during the interview session. The duration of the interviews was 25–40 minutes. After the process of data collection, the recorded interviews were transcribed.

The survey data-collection method is explained and the use of a qualitative survey is presented below.

### **3.3.5.2 Qualitative Surveys**

The study used surveys as another data-collection method to understand and gather information about cybersecurity risks, risk likelihood, impact and protection measures. The online survey was set out in Google forms and divided into four sections: the business profile, risk likelihood, risk impact and the cyber risk management plan. Table 3-3 shows that data were collected from respondents in the Northern Cape, Free State, KwaZulu-Natal, Western Cape, Gauteng and the Eastern Cape.

### **3.3.6 Data Analysis**

The researcher used thematic analysis to analyse the collected survey and interview results such as the non-quantifiable information, and interpreted it to produce meaning. The analysis determined the business background, cybersecurity risks, the likelihood of risk and risk impact. A sensitivity analysis was also done using decision trees, scenario analysis, EMV and protection measures. The information was read, interrelated concepts determined and similarities merged where necessary. The analysis determined and generated a sense of the experiences of the SMEs with regard to interactions and situations. All participants shared their current practices to maintain good cybernetic hygiene in their activities. Research questions were used to categorise survey and interview data. The interview data collected were transcribed. The completed questionnaire and transcribed interview data were interpreted and analysed using narrative analysis. ISO standard 31000:2009 was used to analyse the collected qualitative risks. This study triangulated the multiple sources of data to develop an understanding about the phenomenon.

In addition, the study used the risk management analysis techniques to analyse the collected data which is further analysed using the NIST as the cybersecurity framework. Lastly AgenaRisk package was used to illustrate the cyberrisk likelihood.

The following section presents the methodology to describe this study's adopted risk management standard.

### 3.4 RISK ASSESSMENT

This work adopted the risk management methodology comprising qualitative and quantitative risk assessments.

#### 3.4.1 ISO 31000:2018 Risk Management Standard

Figure 3-15 shows the seven phases of risk management, namely communication, and consultation, establishing the context, identifying risks, analysing risks, evaluating and treating risks, and monitoring and reviewing risks. A discussion of each phase is presented below.

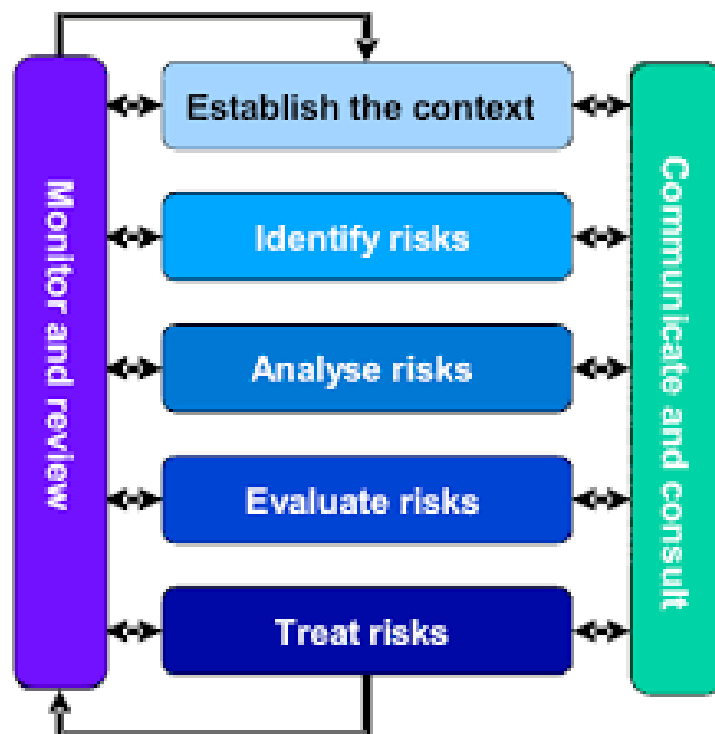


Figure 3-15: Risk management processes - ISO Standard 31000:2009

### **3.4.1.1 Communication and Consultation**

This is the first phase of the ISO 31000:2018 risk management process, which deals with regular communication and consultation with stakeholders to understand the current and emerging cyberrisks, their nature, their likelihood of occurring, evaluation, and the current treatment used to mitigate the risks. Businesses should be clear about their troubling cyberrisks to make informed decisions about risk management.

### **3.4.1.2 Establishing Cyberrisk Context**

Owing to the multiple sources of cyberrisks available, this phase gathers cyberrisk-related information and takes note of potential risks. This phase helps to establish the nature of risk, its source, the potential harm, and likelihood of risk.

### **3.4.1.3 Identify Cyberrisk**

Cyberrisks are identified according to their nature, source, cause, likelihood, and impact. In this study, the risk identification phase helps understand the possible risks that could have a positive or negative impact. This phase captures all cyberrisk events experienced and their relationships with each participating business sector's perceptions, promoting communication and feedback among the stakeholders. These risks help to identify the risk assumptions, causes, and anomalies. Cyberrisk identification informs the assessment of the risk consequences and probabilities. This study focuses on the cyberrisks experienced by small businesses from different sectors in SA.

### **3.4.1.4 Analyse Cyberrisks**

This phase focuses on assessing and analysing the risk probabilities and consequences to determine the risk matrix. The risk events are prioritised to establish risk ranking based on the importance of the risk and the mitigation thereof. The research used a likelihood scale of 1–5 as values where 1 is for rare and 5 for certain to happen. The risk impact is measured from low to high. A risk with a high probability carries a high consequence, while a risk with a low likelihood carries a low-risk result. All the identified risks are categorised and estimated to create the risk matrix and the corresponding risk response.

### **3.4.1.5 Evaluate Cyberrisks**

Evaluation of risks helps to prioritise them and allocate the resources effectively. These risks are then categorised according to their urgency and frequency. Even though each risk event is assessed to evaluate its impact cost, the risk impact is not limited to this criterion. There could be other economic and political consequences, but this study examines the monetary values and sensitivity analysis, using decision tree analysis (DTA) and scenario analysis.

#### **3.4.1.6 Risk Treatment**

This phase develops the options and required actions to proactively enhance opportunities that reduce cyberrisks (PMI, 2008). This phase also involves tracking the identified and emerging cyberrisks to effectively assess the overall cyberrisk process. Implementing the mitigation process executes proactive mitigation actions for the identified risks.

#### **3.4.1.7 Risk-Monitoring and Review**

Risk monitoring and review monitor the risks, their assessment, and mitigation strategies, according to the risk priorities. This phase focuses on systematically tracking and evaluating the risk mitigation activities' effectiveness to plan and develop appropriate mitigation strategies. These activities are measured against established metrics.

### **3.5 RELIABILITY AND VALIDITY**

This study used qualitative assessment research to analyse the likelihood and impact of cyberrisks at SMEs in SA. Therefore, it is necessary to consider the reliability and validity of the research methods and the instruments of measure used. According to Streiner and Norman (2008), the terms 'reliability and validity' describe the estimations and minimise the error associated with measurements used in specific instruments. The two concepts are mainly used to measure and evaluate the quality of research based on the method used in this study. Furthermore, the terms examine whether the technique used has measured the intended concept, whether it has fully represented what it aims to measure; the suitability of the content, and how the results correspond in a different test of the same thing.

In this study, reliability is used to measure the consistency of the technique, while validity is used to evaluate the method's accuracy. The validity concept helped align the technique's purpose with assessing its correspondence to the actual values. The study's reliability and validity rely on the cause-and-effect relationships and the independent and dependent variables. While the independent variables present the *cause*, the dependent variables present the *effect*. The 'cause' value does not depend on the other variables. The changes in the independent variables determine the 'effect.' Owing to the nature of this study, which requires the researcher to evaluate dependent and independent variables, this study looked at the cyberrisk causes and the effects caused by those risks. Reliability and validity assess the quality of the research method used to conduct this study. The collected data were stored and managed as described below for safety reasons.

### **3.6 DATA STORAGE AND MANAGEMENT**

Alase (2017) suggests that researchers prepare a sturdy safety system to protect data gathered from the research participants. This study designed a safe storage system to keep and manage the collected data.



The data management process is conducted and decided before the actual data collection. The research used passwords to protect and file the research data for this study. The collected data were organised and stored to prevent sensitive and business information leaks. The study prioritised the participants' anonymity and kept the data safe to avoid the participants' names and numbers. The transcribed data were stored and backed up systematically for interview purposes to minimise distortion. The collected data from the participants (audio) were destroyed and deleted after the transcription. The following section presents the process of data analysis and interpretation.

The following section of the study accounts for the reliability and validity of the study.

### **3.7 ETHICAL CONSIDERATIONS**

Clarke (1991) addresses the importance of ethical behaviour when conducting research with the research participants. This work obtained ethical clearance from the university's ethics committee explaining the university rules and regulations for conducting the study. The researcher copied the ethical clearance letter to the research participants and attached it to the final thesis. The researcher seriously considered the participant's rights, feelings, and well-being.

(Appendix A presents a copy of the ethical clearance certificate from the Engineering Faculty's Ethics Committee at the Cape Peninsula University of Technology).

#### **3.7.1 Informed consent and permission**

When conducting research, informed consent is the main ethical issue. Informed consent implies that a person should knowingly and voluntarily consent (Armiger, 1977). All participants received the consent letter indicating voluntary participation in this study. The signed consent letter represents a legal document for the SMEs and the researcher.

A copy of the consent letter is also attached in the appendix section.

#### **3.7.2 Confidentiality and Anonymity**

Confidentiality refers to the handling of information concerning the respondents' confidentiality. Research participants received the assurance that their details and the gathered data would remain private and confidential. Information collected is stored on a private database and kept anonymous, and the research participants are kept anonymous. The study ensures an adequate level of confidentiality of the research data. The anonymity of individuals and organisations participating in the research has to be ensured.

### **3.7.3 Privacy**

In the ethical consideration context, ‘privacy’ is the freedom an individual has to determine the time, extent, and general circumstances under which private information will be shared with or withheld from others (Levine, 1981). Among other violations, privacy mainly happens when private and sensitive information becomes available to unauthorised personnel without any knowledge or consent of the owner. The researcher must ensure that private information is not shared publicly. As a results, participants were guaranteed that their information and data collected from them would remain private, and anonymous.

### **3.7.4 Honesty and transparency**

The researcher was honest and transparent with the participants. The information gathered in this study was used for the research. There was no misleading information and representation of primary data findings. Communication relating to the research was done honestly and transparently and there was no deception about the research aim and objectives.

## **3.8 CONCLUSION**

This chapter presented the method of inquiry used to collect, present, interpret, and analyse data. This included the selection of the research participants, the data-collection method, and data analysis, and sequentially triangulated the qualitative approach to risk management. The study's methodology discussed the broader approach used to carry out the work. A qualitative method analysed the SMEs' backgrounds, common cybersecurity risks, threats, and attacks.

## **CHAPTER 4: RESULTS AND DISCUSSIONS**

### **4.1 INTRODUCTION**

This chapter presents the respondents' results and discussed the research questions in the introductory chapter, interpreting the collected data analytically and logically to answer the research questions. The chapter also analysed qualitative data and accounted for the risk assessment, relevance of the NIST framework, and the Bayesian network tools with AgenaRisk. The following section presents the sources of data used in this study, followed by the data analysis process used in the study.

### **4.2 SOURCES OF DATA**

For this study, there are three sources of data. Interviews and questionnaires present the primary sources of data and a literature review of the secondary data. The collected data from the interviews and the questionnaire were then analysed, interpreted, and presented using the thematic method and descriptive statistics. To develop the conceptual framework, the researcher studied and reviewed the latest relevant literature about the impact of cybersecurity crimes in SMEs in South Africa (SA). This secondary data was used to re-analyse the collected information so that the researcher could be clear about the underlying assumptions and theories about the data.

The current work focused on small and medium-sized enterprises in various sectors in SA. The focus is on businesses with one to 150 employees per business, generating a turnover of not more than R1 million per year.

### **4.3 DATA ANALYSIS**

The data analysis process makes sense and derives meaning from the data that constitute the study's findings. Therefore, data analysis makes it easier to manage by organising collected data into categories, interpreting them, and looking for recurring trends to determine the significance of relevant information (Marzulina et al., 2022). This work mixed the qualitative and risk management standards to answer the research questions in Chapter 1. This part of the work unpacks and presents the qualitative data analysis, and Section D presents the application of risk assessment, starting with the qualitative followed by the quantitative risk assessment and analysis. Thematic analysis was used where the researcher reviewed data collected to identify common themes such as models, topics, and ideas of meaning that recur several times. The result was analysed using thematic analysis to interpret patterns and meanings of the cybersecurity risks SMEs face in SA.

Data analysis assigns meaning and interprets either qualitative or quantitative elements of information that do not have an exact order into significant knowledge and outcomes (Neuman, 2006; Creswell, 2014). While qualitative data analysis is a scientific method of observation that gathers non-numerical data, quantitative analysis is the logical investigation of nature via statistical, mathematical or computational techniques (Creswell & Guetterman, 2018). According to Atkins and Wallace (2012),

qualitative research involves the close relationship between collecting and analysing data to build a rational clarification and interpretation. This study also used descriptive statistics to summarize the features from a collection of information.

#### **4.3.1 Qualitative Data Analysis**

For the qualitative data, the study described the design of the descriptive qualitative survey, analysing the relationships of the units and patterns of the similarities and differences in the study context. The data analysis interprets accounts, explores the experiences, and makes sense of the data collected. For the first research question, the online survey and interview analysis followed the following process:

- Identified common cyberrisks that SMEs face, especially during the Covid-19 pandemic.;
- Read and identified the codes with qualitative responses;
- Identified similar codes to collate and break them down where necessary;
- Identified the themes in the codes; and
- Identified the ideas and concepts from the list of themes.

#### **4.4 RESULTS**

In qualitative research, data collection and analysis allow for a consistent interpretation of the data. Data analysis starts by coding every incident into as many categories as possible. As the search continues, the data is moved into existing categories, or existing types are changed, and new categories are added. The data can be unfocused, repetitive, and overwhelming without continuous analysis. Analysis usually results in identifying recurring patterns that cut through the data or into the delineation of a process. Consequently, the researcher read the interviews several times to understand the data sets and facilitated the interpretation of the small data units further. Next, the researcher compared text segments to identify contextual data segments and named and categorised them.

The collected data were divided into SME background, cybersecurity risks, threats and attacks, cyberrisk likelihood and impact, monetary value, and mitigation strategies. The results are divided into sections and themes such as:

- (i) SME background,
- (ii) Cybersecurity risks, threats, and attacks,
- (iii) Cyberrisk likelihood and impact,
- (iv) Monetary value, and
- (v) Mitigation strategies

The following section describes the thematic analysis of the results and presents those using tables and graphical representations.

#### **4.4.1 SME Background**

Data were collected from the relevant research participants who were familiar with the field of study. These respondents use ICT resources for their daily activities. Results revealed respondents' experiences with common cyberthreats, attacks, and risks to running their businesses. The SMEs' experiences helped address the research questions presented in the introductory chapter. The diverse SME sector is from the Eastern Cape (EC), Free State (FS), KwaZulu-Natal (KZN), Gauteng (GP), Northern Cape (NC), and Western Cape (WC). The criteria for the participant selection is that the SMEs should have a range of one to 150 employees per business, generating a turnover of not more than R1 million per year.

##### **4.4.1.1 Demographic**

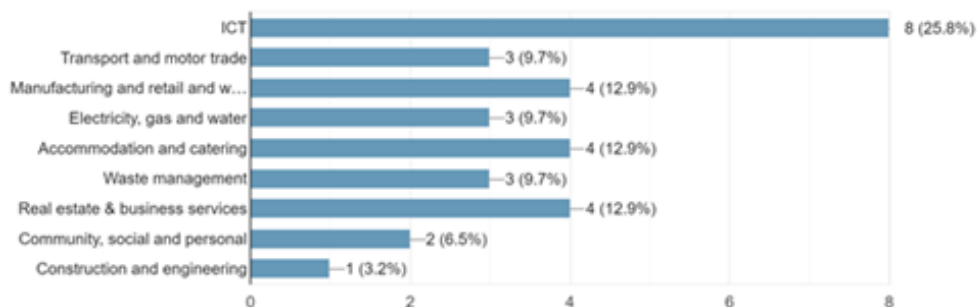
The participant demographic, which includes the province, position of the participant, gender, and age, is presented in Table 4-4 below. The participant demographic presents business owners, chief information officers, and other IT managers, both females and males between 25 to 55 years old, operating in various sectors in SA. As illustrated in Table 4-4, the participants are organised according to the provinces. Out of the 45 selected samples, 34 responded to the invitation and participated in the study, which presents a 75.5% response rate.

**Table 4-4: Participant demographic**

Province	Participant position	Gender	Age
Eastern Cape (8)	Business manager	Male	55
	IT manager	Female	33
	IT manager	Male	31
	Business manager	Male	43
	Other	Female	54
	Chief information officer	Male	50
	Other	Female	43
	Business manager	Female	41
Western Cape (8)	IT manager	Male	26
	Chief information officer	Female	33
	Business manager	Female	40
	Other	Female	55
	Other	Male	38
	Business manager	Male	25
	Business manager	Female	44
	Business manager	Male	29
Northern Cape (3)	Business manager	Male	41
	Other	Female	33
	IT manager	Male	25
KwaZulu-atal (5)	Business manager	Male	31
	Other	Male	30
	Other	Female	45
	IT manager	Female	32
	Business manager	Male	36
Free State (3)	IT manager	Male	41
	Business manager	Female	33
	IT manager	Female	39
Gauteng (7)	Business manager	Male	30
	IT manager	Female	28
	Other	Male	33
	Other	Male	31
	Business manager	Male	47
	Business manager	Female	41
	Chief information officer	Female	35

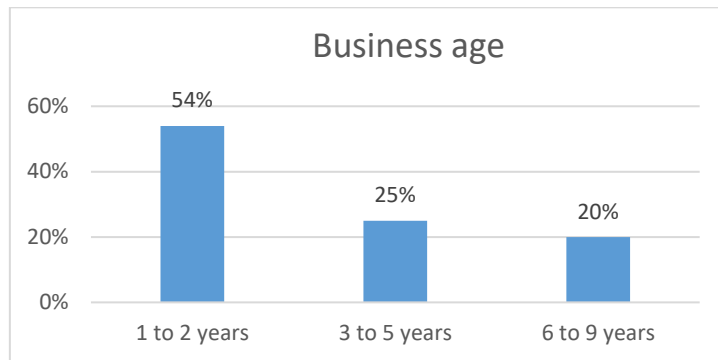
**4.4.1.2 Business Sectors**

Respondents were asked in which business sectors the SME operated. Twenty five point eight per cent (25.8%) were from ICT, 9.7% from transport and the motor trade, 12.9% from manufacturing and retail, 9.7% from electricity, gas, and water, 12.9% from accommodation and catering, 9.7% from waste management, 12.9% from real estate, 6.5% from community and society and 3.2% from construction, as shown in Figure 4-16.



**Figure 4-16: Participant SME sectors**

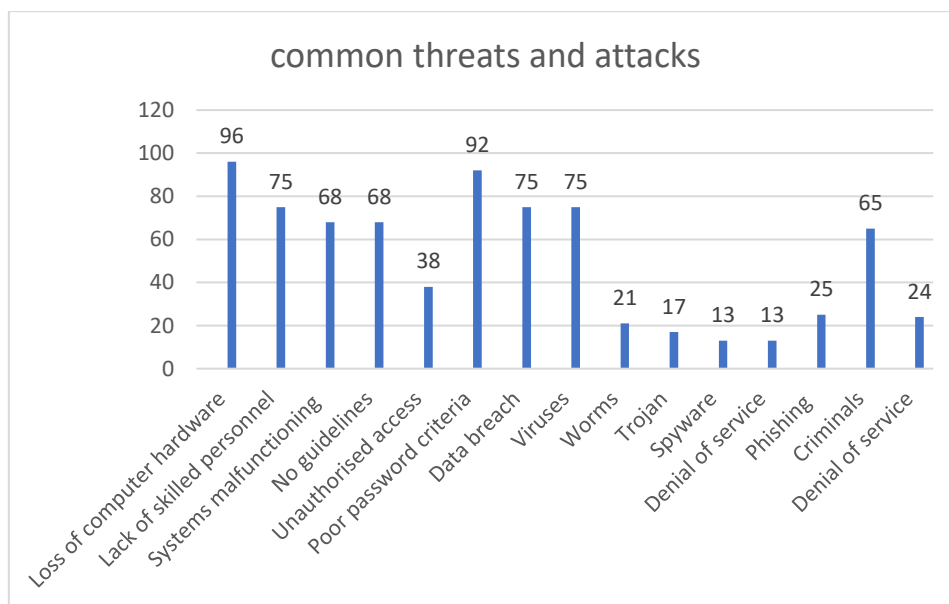
When asked about the age of the SME, 55% of the participants indicated the age as 1–2 years, 25% presented 3–5 years, and 20% 6–9 years, as shown in Figure 4-17.



**Figure 4-17: Age of SMEs**

#### 4.4.2 Identified Cyberattacks

Results showed SMEs are vulnerable and exposed to a range of cyberattacks, as shown in Figure 4-18. Businesses experience the following cyberattacks: 96% for loss of computer hardware, 75% for lack of skills, 68% for malfunctioning of the systems, 68% for lack of guidelines, 38% for unauthorised access to systems, 92% for poor password criteria, 75% for data breaches, 75% for viruses, 21% for worms, 17% for Trojan, 13% for spyware, 13% for denial of service, 25% for phishing, 65% for criminals and 24% for the user ignorance as can be seen in Figure 3-22.



**Figure 4-18: Common Cyberattacks**

Even though SMEs are victims of cyberthreats and attacks, the results show that no company is safe from cyberattacks. The shared cyberthreats and attacks expose businesses to various risks presented below.

### 4.4.3 Cyberrisks Experienced by SMEs

Results revealed SME sector experiences relating to cyberattacks, as shown in Figure 4-19. The results show that 53% of businesses have suffered from a bad business reputation, 47% from business disruption, 88% from poor economic growth and 65% from a loss of client trust, 56% from a lack of client trust, and 53% from a loss of intellectual property and 65% for poor business growth. Forty-four per cent (44%) of businesses experienced malfunctioning computers and servers, 56% unexpected system failure, 32% limited access to resources, and 71% compromised information systems.

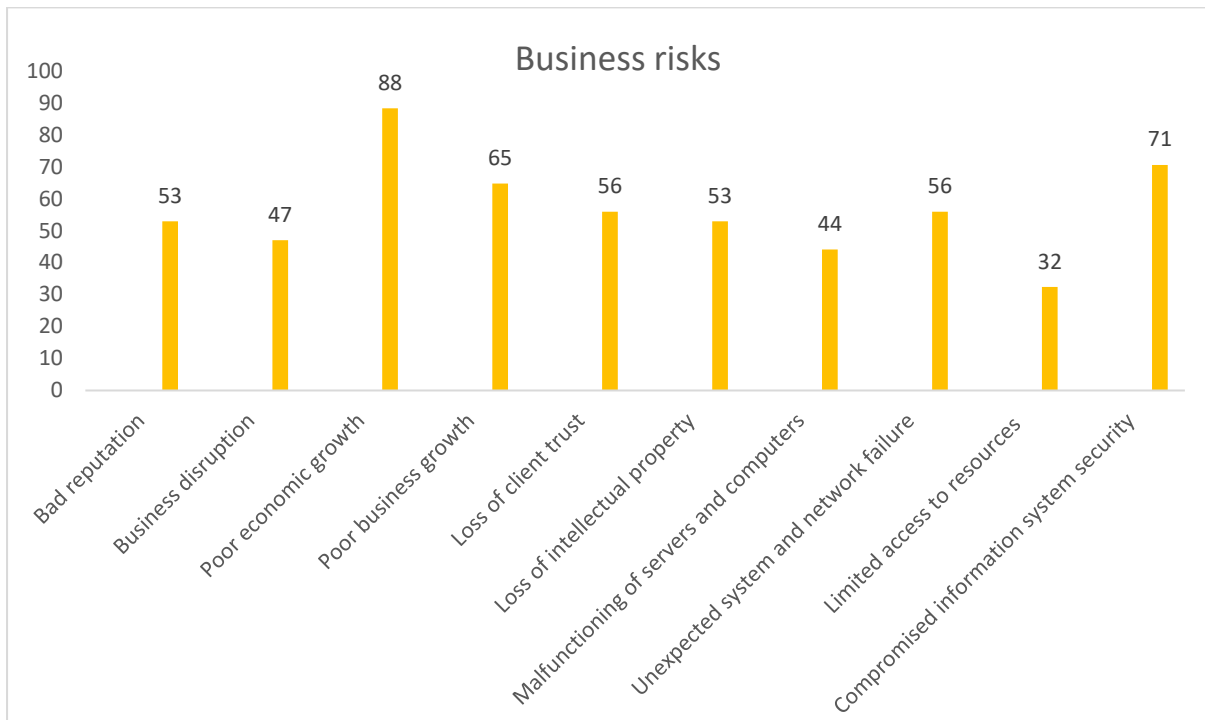
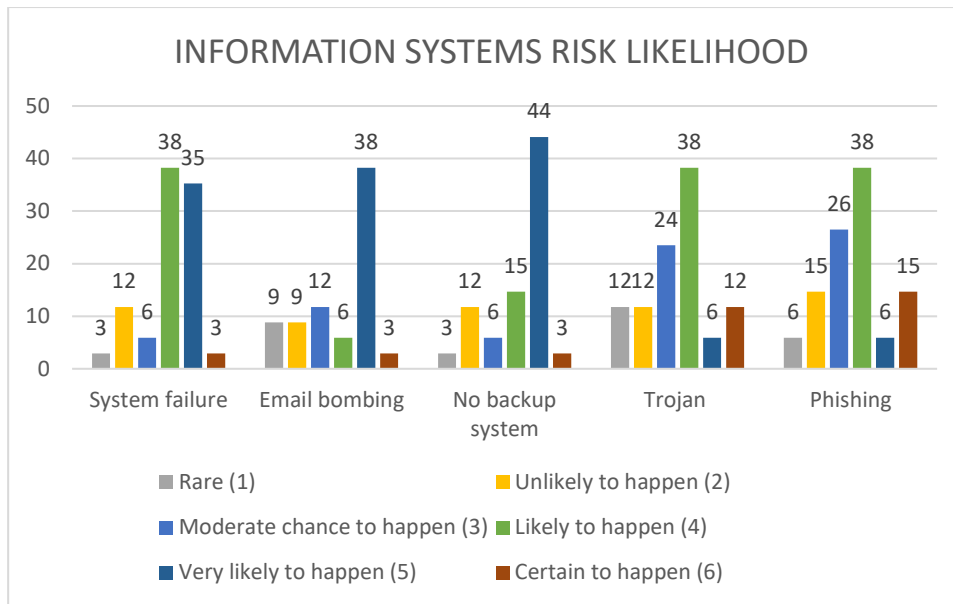


Figure 4-19 Business risks

### 4.4.4 Cyberrisk Likelihood

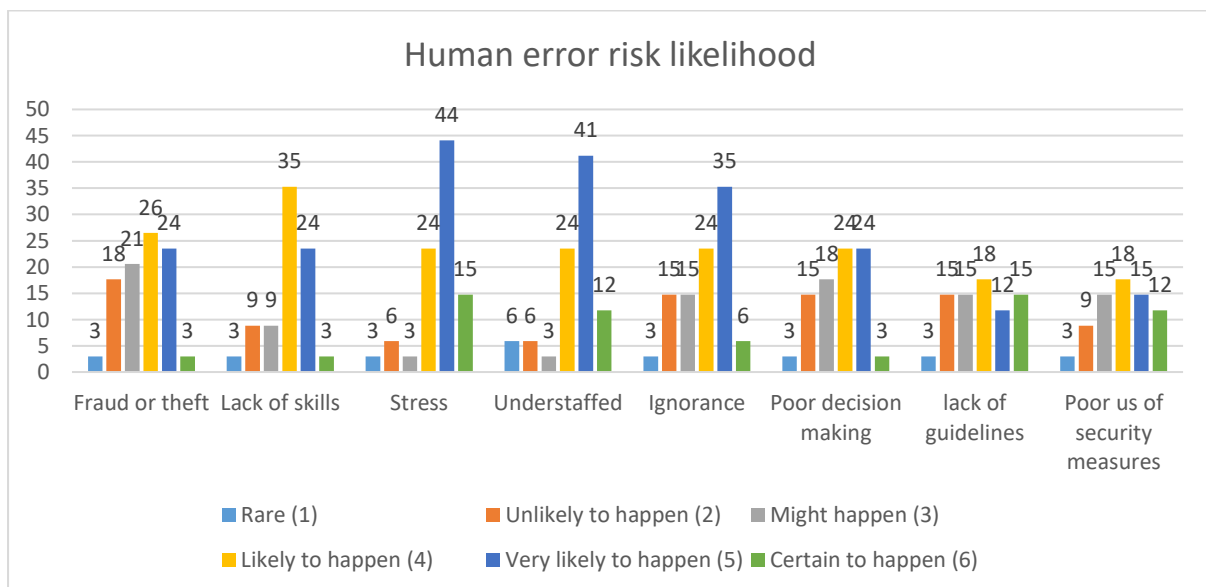
This section accounts for the cyberrisk likelihood amongst the qualitative risks. The results for the likelihood of information system risk are presented below. Even though these results will be thoroughly presented in the following part of work, this section only presents the participants' rating responses according to their sectors. Further risk assessment and discussion are presented in Section D, Part 1. The results are then translated and generated in the risk matrix to determine the severity of the risk. The respondents choose from (1) unlikely to (6) certain to happen. Figure 4-20 shows the respondents' response to system failure, email bombing, no backup system, Trojan, and phishing.





**Figure 4-20: Information system risk likelihood**

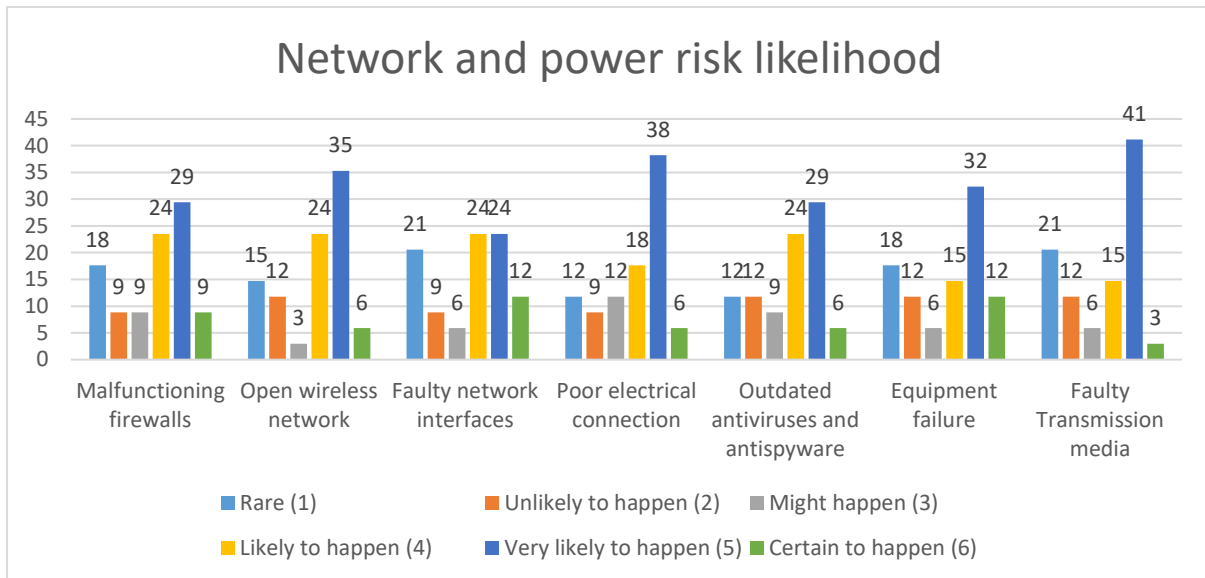
Figure 4-21 presents the risk likelihood of human error according to the likelihood ratings ranging from rare (1) to certain to happen (6). The respondents identified these risks: risk of fraud or theft, lack of skills, stress, understaffing, ignorance, poor decision-making, lack of policies and guidelines, and poor use of security measures.



**Figure 4-21: Human error risk likelihood**

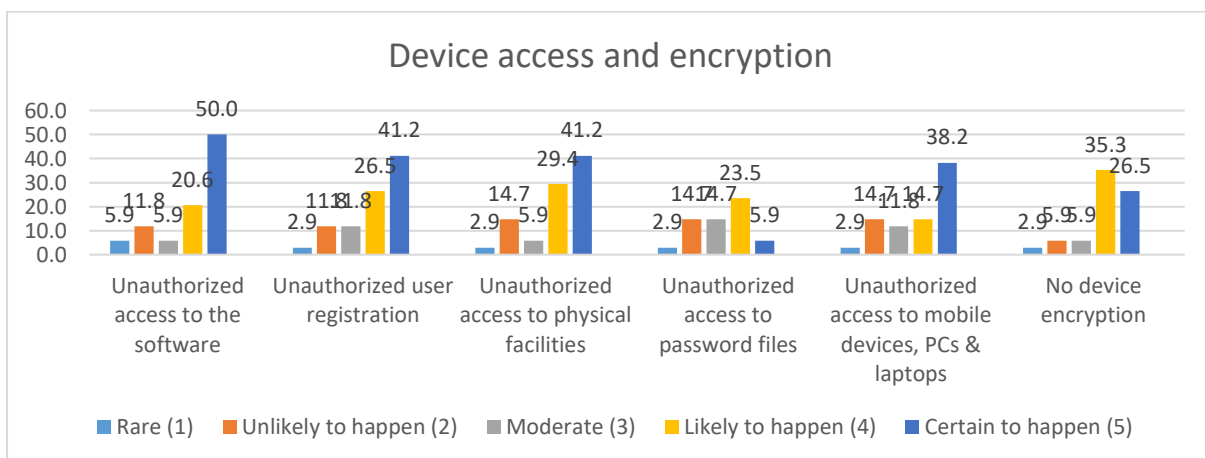
Figure 4-22 shows cyberrisks were influenced by various risk probabilities. For network and power risk likelihood, the respondents share their experiences about the risk likelihood of malfunctioning firewalls, unsecured wireless networks, faulty network interfaces, poor electrical connection, outdated antiviruses, antispyware equipment failure, and faulty transmission media. The likelihood ranges from rare (1),

unlikely to happen (2), a moderate chance to happen (3), likely to happen (4), very likely to happen (5), and certain to happen (6).



**Figure 4-22: Network and power risk likelihood**

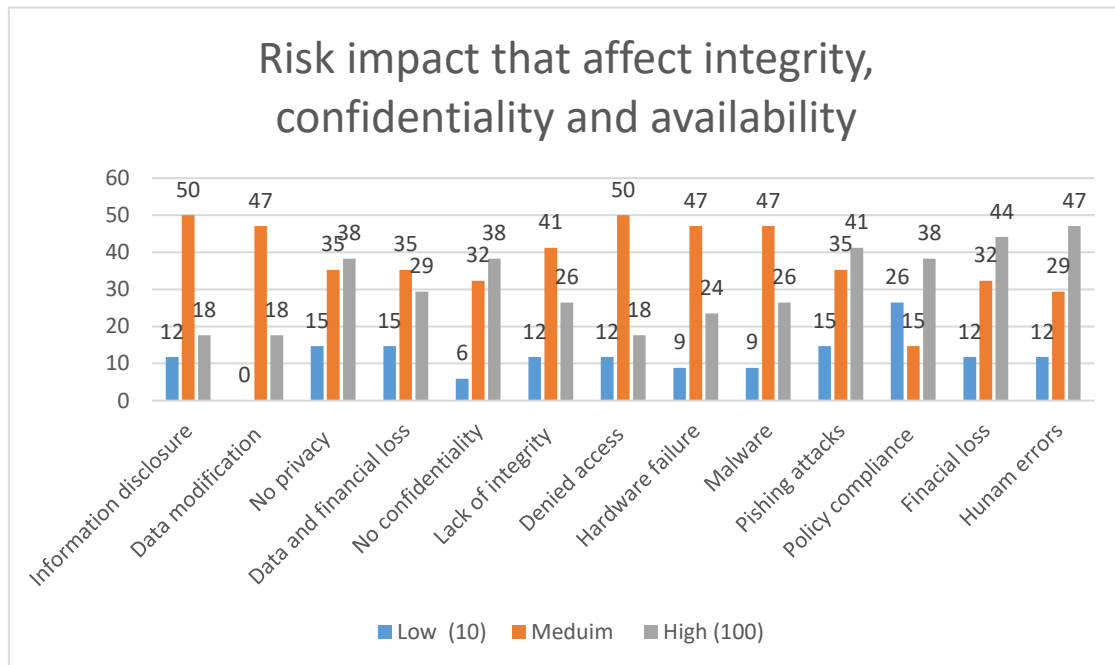
Figure 4-23 shows the device access and encryption risk likelihood. Respondents shared their experiences with the risk of unauthorised access to software, user registration, physical facilities, password files, mobile devices, and the absence of device encryption. The likelihood ranges from rare (1), unlikely to happen (2), moderate (3), likely to happen (4), and certain to happen (5). Device access and encryption risk likelihood included unauthorised access to the software, unauthorised user registration, unauthorised access to physical facilities, unauthorised access to password files, unauthorised access to mobile devices, PCs, and laptops, and no device encryption.



**Figure 4-23: Device access and encryption risk likelihood**

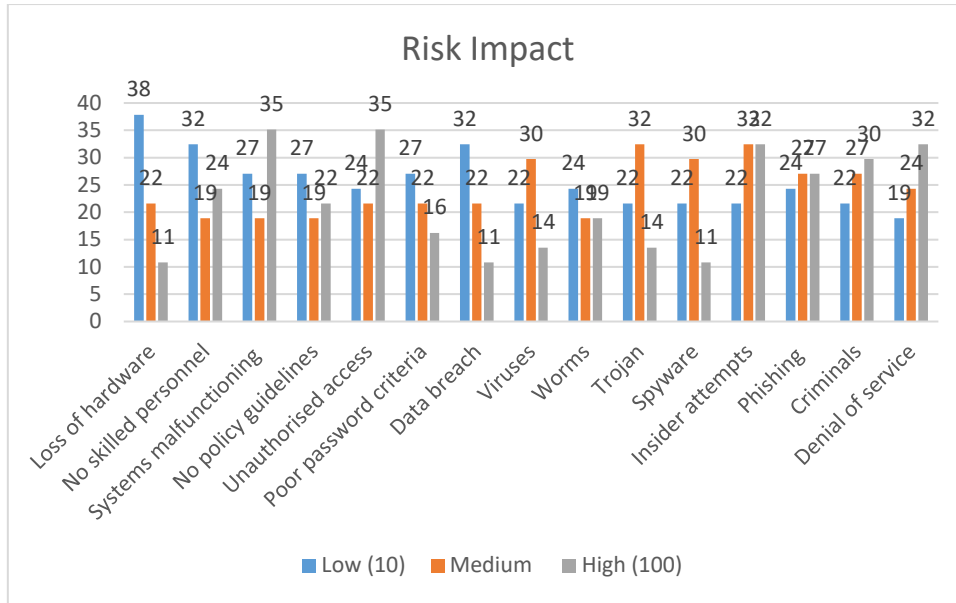
#### 4.4.5 Risk Impact

Figure 4-24 shows the results that revealed the common cyberthreats that affect integrity, confidentiality, and availability compromise businesses, and the risk impact ranges from low (10) to medium and high (100).



**Figure 4-24: Impact of cyberrisks**

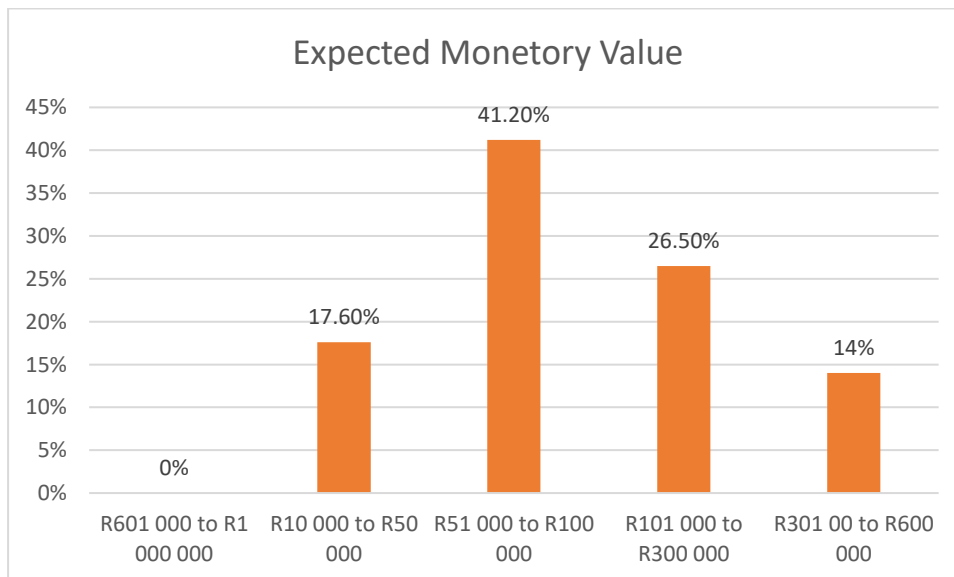
Figure 4-25 shows the risk impact of cyberrisks on hardware, network, and policies are data or financial loss, lack of confidentiality, integrity, denial of access, hardware-related attacks, malware, phishing attacks, and policy compliance. When asked about the impact of integrity, confidentiality, and availability threats, the results revealed that SMEs' experiences ranged from low to medium. Regarding disclosure of information, responses dominated with the opinion that it has a medium to a partially high impact. SMEs experienced took for granted the medium and high effects of data modification, while the lack of privacy was regarded as extremely high.



**Figure 4-25: Risk impact on hardware, network, and policies**

#### 4.4.6 Expected Monetary Value (EMV)

Figure 4-26 shows the expected monetary value. When participants were asked about the recovery amount, no respondents selected the range of R601 000 to R1 000 000. Seventeen point six per cent (17.6%) responded with a range of R10 000 to R50 000, 41.2% selected R51 000 to R100 000, 26.5% used R101 000 to R300 000, 14% selected R301 00 to R600 000.



**Figure 4-26: Expected monetary value**

#### 4.4.7 Risk Mitigation Plans

Figure 4-27 illustrates respondents' responses to the question of how small businesses manage risks as follows: 56% share, 68% transfer, 94% accept, and 76% avoid cyberrisks.

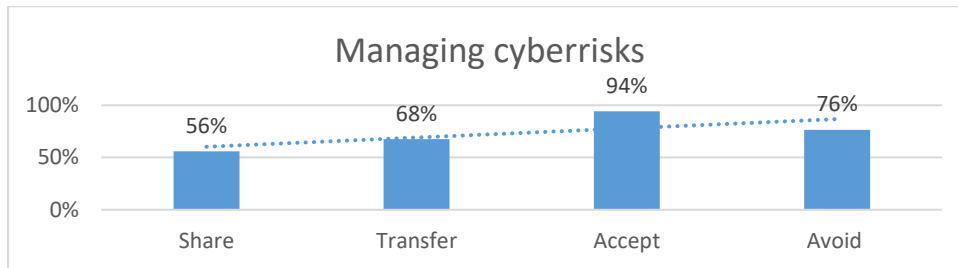


Figure 4-27: Cyberrisk management

The discussions of the results are presented below.

#### 4.5 DISCUSSION AND IMPLICATIONS

This study presented the experiences of the SME participants relating to cybercrimes, threats, and attacks. The study determined various backgrounds of SMEs, followed by the most common cyberrisks, threats, and attacks that the small business sector has experienced. The results revealed the risk likelihood further, namely the impact and monetary value of cyberattacks. This section discusses the results according to the research question in the introductory chapter.

##### 4.5.1 Nature and Background of the SMEs

The global Covid-19 pandemic became an opportunity for cybercriminals to gain unauthorised access to the South African small business sector (Ncubukezi, Mwansa, & Rocaries, 2021). The study had a reasonable number of research participants, especially during trying times and when cyberrisks are prevalent. The research participants were employees, and their selection was based on the use of ICT for business activities. Out of 45 participants that were contacted, 33 participants formed part of the study, with a response rate of 75.5%. The participants consisted of 18 males and 16 females who were selected from six provinces out of the nine provinces, representing 66.6% of the research population. The responses from the provinces are a combination of males and females from the Eastern Cape (8), Western Cape provinces (8), Gauteng (7), KwaZulu-Natal (4), Free State (3), and Northern Cape (3).

The results revealed a diverse age range demonstrating different information and computer security approaches. The results revealed further that the research participants were business managers (14), IT managers (8), chief information officers (3), and others (8). These participants possess different skills in their business setup, among the assumed responsibilities. 'Other,' as a category presents any employee who performs managerial and general work roles. These participants' responsibilities are to manage and give guidance on the use of business resources and enforce strategies to improve business

productivity. Even though there is management at these businesses, the results showed no dedicated cybersecurity personnel in all the selected businesses. Internet usage in the business sector has made businesses vulnerable to outside and inside attacks (Iguer et al., 2014). Furthermore, cybersecurity-related risks affect all institutions and require proactive measures to reduce risks. Consequently, the lack of a skilled cybersecurity team at the businesses poses a major threat, resulting in ongoing cybersecurity risks at these businesses.

The selected diverse range of SMEs has been operating and registered on the South African business database. These businesses have been running for 1–9 years. Even though the business has been operating a long time, it is still not immune to cyberrisks, threats, and attacks. Cybercrimes are common among companies, resulting in vast data leaks in all businesses regardless of size (Williams, 2020). Cybercriminals focus more on what businesses can offer than the company's size. Some large businesses have a strong and reliable infrastructure that promotes safety and security but remain cyber targets. Ngwenya (2020) and Ayandibu and Houghton (2017) share the fact that small businesses play a significant role in poverty alleviation and job creation and contribute to the gross domestic product (GDP). Anderson (2020) and Vuba (2019) state that SMEs significantly increase opportunities for employment with a relative cover of 70% to 80% of the employment population.

The criteria of the selected research participants are small and medium-sized businesses that use ICT for their daily activities which have a range of 1 to 150 employees. The sectors are ICT, transport and motor trade, manufacturing and retail, electricity, gas, water, accommodation, catering, waste management, real estate, community and society, and construction.

Their experiences with cyberrisks are explained below.

#### **4.5.2 Common Cybersecurity Risks, Threats and Attacks**

Cybersecurity is an ongoing and fundamental problem (Vakakis et al., 2019). Technology has evolved and requires businesses and people to adjust and participate in Internet adoption and usage (Ponsard, Grandclaudon, & Dallons, 2018). The increased usage of cyberspace introduces cybercrimes that necessitate the consideration of cybersecurity. Businesses and people continue to pay little attention to cybersecurity; and, as a result, most people are not computer literate. Some employees have minimal knowledge and skills to handle cyberattacks (Uma & Padmavathi, 2013). The main gap between individuals and institutions relates to minimal knowledge about the cyber trends, their characteristics, the type of cyberattacks, and the potential impact, which is a global challenge. At the same time, cybersecurity can be improved by knowing what is vulnerable, what assets are exposed, and what to protect (Abomhara, 2015). The next section presents common cybersecurity risks, threats, and attacks that businesses experience.

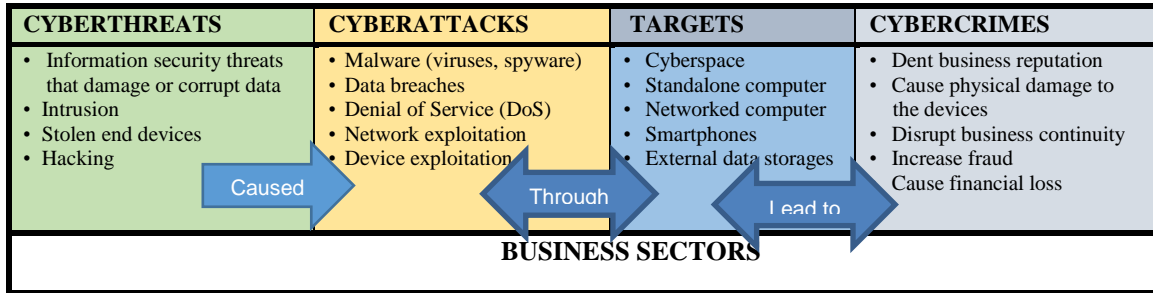
#### **4.5.2.1 Cybersecurity Risks**

Cybersecurity is necessary and should be prioritised by all institutions. It's the overall security of people, assets, and systems. However, the lack of cybersecurity poses several risks. Cybersecurity in the SME sector poses risks caused by network attacks, people (employees or criminals), malware, phishing, and minimal enforcement of any guidelines, resulting in a data breach. The results have shown that there are common and persuasive risks that compromise cybersecurity. Even though these participating businesses do not serve in the same field, their exposure to cyberthreats has a common impact. Cybersecurity risk refers to the likelihood of disclosure or loss resulting from a cyberattack or data breach. A better and broader definition is the potential loss or harm associated with an organisation's technical infrastructure, use of technology or reputation (Agrafiotis et al., 2018; Mottahedi et al., 2021).

Cyber risk is the potential harm or loss owing to unauthorised information systems. Cybercrime is a computer-generated crime, also known as an electronic crime, introducing new and innovative crimes through technology (Sarre, Lau, & Chang, 2018). Cybercrimes are committed through various cyberattacks on information systems and networks to expose, harm, and eventually cause data breaches (Sovacool & Del Rio, 2020). The thousands of pervasive cyber risks such as phishing, whaling, fishing, and pharming have become the most common types of economic fraud affecting the world and often get reported almost daily (Chang, 2013). The increased cybersecurity-related incidents are still rising to affect big and small businesses. All institutions are more vulnerable than ever to cybercrime and are hacked by organised criminals. Most small businesses become vulnerable to identity theft, theft of credentials, and other types of cybercrimes that provide financial gain. Blue Turtle Technologies (2020) explains cybercrimes as a persistent pandemic going after South African businesses, regardless of their size.

Cyberspace has quantified opportunities for cybercriminals by means of a variety of cyberthreats and attacks that ultimately become cyber risks (Sovacool & Del Rio, 2020). The results have shown business cyber risks relating to human, operational, systemic, technical and technological risks. The risks are caused by the Internet's openness, which has become the main backbone for communication and businesses (Ncubekezi, Mwansa & Rocaries, 2020b). The consequences of the openness of cyberspace to both legitimate cyberusers and cybercriminals have necessitated the assessment of cyber risks at small businesses in SA with the purpose of deploying proactive cybersecurity measures. The connection between cyberthreats, cyberattacks and cybercrimes is demonstrated in Table 4-5.

**Table 4-5: The connection between threats, attacks and cybercrimes (Ncubukezi & Mwansa, 2021a)**



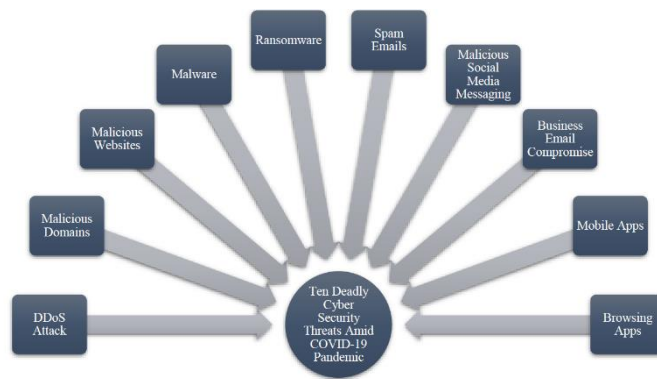
#### 4.5.2.2 Cyberthreats and Attacks

SenseOn's report (2019) states that SMEs are an attractive target in cyberspace for adversaries. SMEs in cyberspace have been the victims of cyberattacks. Businesses are exposed to diverse threats, such as malicious attempts that damage their assets (Khan, Brohi & Zaman, 2020). Often, networked devices are exposed to a range of cyberattacks, namely: human errors, malware, phishing, denial of service, data breaches, and network exploitation. These all cause cyberthreats. Some cyberattackers use external hard drives, networked or standalone end devices which mainly present an entry point for cybercrimes. All devices connected to the network become the primary cybercrime target because they get exposed to various cyberthreats. External hard drives for information-sharing sometimes expose businesses.

Cybercriminals' main focus is on the device's Internet protocol (IP) address. These devices can be stolen, intruded upon, made unavailable, or maybe lose their information. The literature indicates that SMEs have been the victims of cybercrimes. Indeed, cyberissues affect mainly the information systems, which are maliciously attacked using spyware, viruses, and social engineering, amongst others. (Iguer et al., 2014). Small businesses should implement effective and innovative cybersecurity measures to improve and protect the company's production, revenue and growth. Tackling cybercrime can bring real benefits to small businesses. As organisations of all sizes move toward driving efficiency through digitising processes, business leaders need to redefine how they think about security (Lloyd, 2020).

There are always many different types of cyberthreats. For example, Khan, Brohi and Zaman (2020:395), as shown in Figure 4-28, cited 'the distributed denial of service, ransomware, malicious domains, business email compromise, malicious websites, malware, spam emails, malicious social media messaging, mobile applications and browsing applications'. Any form of the above-mentioned cyberthreats can affect businesses at different levels.





**Figure 4-28: Common cyberthreats in the Covid pandemic (Khan, Brohi & Zaman, 2020:395)**

Cyberthreats threaten businesses, exposing SMEs to significant cyberrisks (SenseOn, 2019). All the threats harm or get access to information, business operations, the business environment and business assets (Choo, 2011; Kurpjuhn, 2015). The impact of cyberthreats leads to physical damage, financial loss, a bad business reputation and a break in business continuity. Moreover, attempted cyberthreats result in cybercrimes (Pritom et al., 2020). Most cybercrimes are committed on networked and standalone computers to damage and distribute the attack on the network (Herjavec Group, 2019). End devices act as an entry point to disrupt business activities by attacking information systems; cybercrimes affect networked computers deliberately (Uma & Padmavathi, 2013; Kurpjuhn, 2015; Balan et al., 2017). Data breaches in certain businesses are the top cyberattacks.

With technological advancement and demand, small and medium businesses (SMBs) have become the main target for various attacks. Reports in 2018 revealed that 67% of SMBs had experienced cyberattacks, while 58% of the businesses had experienced data breaches (Ponemon Institute, 2018). According to Verizon Enterprise Solutions' report (2019), 43% of attacks target small businesses, with 56% of breaches taking longer to discover. The Beazley Group report (2019) revealed the increased number of ransomware attacks which amount to 71%. The Federation of Small Businesses in the UK reports that the small business sector suffers 10,000 attacks per day (Anon, 2019). With all these quantified cyberattacks, 83% of small businesses have inadequate funds for cyberattack mitigation (Hashedout Report, 2019).

Cybercrimes can depend on the Internet or operate independently (McGuire & Dowling, 2013). At times, the quantified cybercrimes are through the Internet rather than memory sticks, which infect end devices. The Ponemon Institute's report in 2018 categorises dependent cybercrimes such as intrusion, malware, or networked computer disruption without the user's knowledge. Verizon Enterprise Solutions' report (2019) highlights the fact that SMBs have experienced many attacks. The growth of cybercrimes has become a severe and damaging economic issue for South African organisations

(Hubbard, 2019). The increased cyberattacks require proactive plans that effectively mitigate cyber risks and reduce business downtime.

#### **4.5.3 Plans for Mitigation Strategies**

The results revealed that 19% of the participating businesses share their risks, 23% transfer them, 32% accept them and 26% avoid their dangers. Transferring or sharing the risk involves shifting the risk consequences with the risks to a third party. Usually, the business has an agreement about handling transferred risks. The acceptance of risks is carried out according to the response plan, which accepts the outcome of the risk. Avoiding cyber risks involves proactively revising the business plan to avoid potential risks. As part of the response planning, the task team should document all the risk incidents and plan their response mitigation actions linked to the responsible personnel. The response plan should also contain the results of qualitative and quantitative analysis, the budget and the timeframe allocated to each risk response.

This study adopted the NIST framework to help guide and manage cybersecurity risks in the business sector. The NIST framework has tested phases that focus on the improvement of safety and security of the hardware, software, people, governance, network, vendors and processes in the business sector. The framework is thoroughly discussed and adopted in Section C, Part 1 of this study, while its relevance is presented in the section below.

#### **4.6 NIST FRAMEWORK RELEVANCE IN MANAGING CYBERSECURITY RISKS**

The results showed the SME sector's different strategies to mitigate and reduce risks. Ncubekezi, Mwansa, and Rocaries (2020a) state that mitigation strategies are the key elements of maintaining the cybersecurity hygiene of the business. The security measures are designed to promote small business continuity and enhance production to increase profit, contributing to the main aim of SMEs in the country. Likewise, the NIST framework describes the incorporation of its phases into different businesses to manage cybersecurity risks and improve business operations. A smoothly run and improved business helps to contribute to the GDP and alleviate poverty (Doktoralina & Apollo, 2019).

Risk mitigation is the process of preventative action to reduce the probability of risk occurrence or impact on the project. The results revealed a need to adopt a cybersecurity framework (CSF) guideline for SMEs to improve management and reduce cybersecurity risks. The chosen framework explores the use of rules, tools, and controls that form an essential part of a successful business. The NIST CSF has a detailed set of processes to help the SME sector assess and measure cybersecurity and risk management by determining the necessary stages to strengthen them (NIST, 2014). The adoption of the NIST in the context of cybersecurity for SMEs is described in Section D.

## **4.7 APPLICATION OF RISK MANAGEMENT STANDARD**

The study adopted ISO 31000:2018 as the risk management standard for all its processes. It becomes essential to perform risk analysis and assessment to evaluate and estimate risk occurrence or losses influencing decision-making (Zhang, 2013). Risk results from interactions between risk factors and risky objects in a system (Grandell, 1991). Although qualitative risk assessment is based on expert knowledge, quantitative risk assessment uses mostly mathematical methods (Li, Hong & Zhang, 2018).

Risk management analysis helps analyse the operational tasks and critical business assets (Shad et al., 2019). The collected data and the analysis of the results contributed significantly to the alignment of the cybersecurity risk framework as well as to the overall risk assessment that evaluated the risk likelihood and impact. The results were analysed and presented. The section above accounted for the qualitative analysis, while this section gives an overview of the risk management analysis. This process is essential for every business. The risk analysis is performed to prioritise the risks in preparation for further risk assessment. The top priorities will be assigned to the cyberrisks with high impact and high probability.

### **4.7.1 Qualitative Risk Assessment to Determine the Risk Matrix**

The global Covid-19 pandemic has exposed and increased technological risks at different institutions. The technological risk is often interpreted as the likelihood multiplied by its impact. Cyberrisk probability is determined by exploitation and vulnerability (Paté-Cornell et al., 2018). Cyberrisk is the probability of the disruption and vulnerability of private and sensitive business data, finances, and their actions in cyberspace, ultimately causing a data breach. Cybersecurity risk is the probability that cyberthreats can exploit small businesses and result in vulnerability (Kure, Islam & Razzaque, 2018). The results of this study showed different cyberrisks and SME experiences regarding cybersecurity risk likelihood and impact. The quantitative risk assessment was performed to determine the sensitivity analysis and the EMV. The detailed cybersecurity risk analysis is presented in Section B.

### **4.7.2 Quantitative Risk Assessment Techniques**

The study analysed the monetary impact caused by business cyberrisks. The study revealed experiences with the funds of businesses to improve and maintain continuity. The economic value is paid to repair the business asset or improve a business service. The assets could be tangible and intangible properties that are priced at their monetary value. When asked about the financial impact caused by cybercrimes in the SME sector, the businesses indicated that they used between R100 000 to R300 000 to restore the business to its state. The results showed that companies experienced unexpected device failure, disrupted services, phishing attacks, human errors, and poor adherence to cybersecurity guidelines

resulting in data breach. These results are analysed further using the quantitative risk analysis in section D.

The collected data built the knowledge base for the AgenaRisk package that performs well-defined tasks requiring human intelligence, which relies on mathematical, statistical, and decision theories (Boukherouaa et al., 2021). Chapter 7 uses quantitative risk management techniques to analyse the sensitivity of cyberrisks. The results of the sensitivity analysis and the Tornado graphs are produced using the AgenaRisk package. The study also used the decision table analysis and scenario analysis.

The literature shows increased use of AI tools in the financial sector, while the expectation of protection plays a role in the instant rise of cyber criminals (BoE, 2019). The unexpected Covid-19 pandemic necessitated and increased the appetite for businesses to incorporate AI into their services. Supervision with AI collects structured and unstructured data, detects early warning, and performs risk profiling. Unstructured data analytics identifies potential violations and predicts the cyberrisk in real-time (Boukherouaa et al., 2021). For further risk mitigation, the study incorporated AI. More information about the choice of AI used in the study is described below and applied and explained further in Section C.

#### **4.8 ADOPTION OF AGENARISK PACKAGE**

Based on the study results, businesses must plan cybersecurity risk management thoroughly. An effective way to mitigate risks during the Covid-19 pandemic required intelligent systems which proactively detected early warning signs and reduced cyberrisks. Ncubekezi, Mwansa, and Rocaries (2020a) suggest using AI tools to proactively mitigate cybersecurity risks and reduce their impact on the business sector. Under the AI umbrella, this study adopted the Bayesian network tools, which gained popularity in advanced technologies and focused on the probabilistic graphical modeling (PGM) techniques for calculating the risk uncertainties using the likelihood of cyberrisk. The BN shapes complex scenarios with fewer resources and information. In the cybersecurity context, the AgenaRisk package uses the BN tools to determine the probabilistic models about the uncertain situation based on random variables assigned to the prior indicators to produce conditional probabilities for the corresponding random variables.

This work aimed to design, develop and evaluate the cybersecurity risk tool for SMEs in SA. The results presented revealed the participants' experiences relating to the business's cybersecurity, which informs the design and development of the cybersecurity risk model. This study used the AgenaRisk package with BN tools to illustrate the relationships between the variables which came up from the analysis of the collected data. BN is a probabilistic graphical model representing a set of dependent and independent variables with conditional dependencies on a directed acyclic graph (Yang, 2019). BN

presents the probabilistic conditions, which are yielded by selected prior indicators (Liu et al., 2019). Section C describes the adoption of the BN tools with an AgenaRisk package and uses the simulated case scenarios to illustrate the relationships with the analysed data variables. These variables demonstrate the prior indicators, dependent and independent associations, and posterity indicators.

#### **4.9 CONCLUSION**

In conclusion, this chapter presented and reported the collected qualitative research findings and discussed them further. The study used thematic analysis to analyse and interpret data from the research participants. The results were presented according to the themes. The study accounted for the relevance of the cybersecurity framework, risk management standards, and the adoption of the Bayesian Network tools with AgenaRisk. The NIST cybersecurity framework, risk management standards and the use of the AgenaRisk package was accounted.

## **CHAPTER 5: DESIGN OF THE CYBERSECURITY RISK TOOL**

### **5.1 INTRODUCTION**

The advanced skills deployed by cybercriminals have, in one way or another, threatened all business sectors leaving no business immune to cyberrisks. Even though the SMEs find their way into the convenient platform that supports information exchange faster, the criminals also find ways to gain lucrative benefits, exposing business sectors to various cyberrisks. Consequently, the global Covid-19 pandemic granted people, businesses and other institutions an equal chance to rely on cyberspace to connect (Ncubukezi, Mwansa & Rocaries, 2020a). With the increased presence of cyberusers, criminals also gain unauthorised access to various business assets. As a result, cybercrimes have become the second-largest risk and constantly attack small business enterprises (Soomro & Hussain, 2019). The continued vulnerability of small businesses compromises information and computer privacy, safety, and security (Sulistiyowati et al., 2020). The exposure to various cyberthreats and attacks poses several challenges which threaten diverse areas of business.

The increased cyberrisks at businesses and other institutions require proactive measures to manage, reduce and protect businesses against intruding cyberthreats (Ncubukezi, Mwansa & Rocaries, 2020b). The study designed, developed and evaluated a cybersecurity risk tool for small enterprises. This work proposed the CSF to manage, control and reduce cyberrisks, especially during the Covid-19 pandemic. The structure of the chapter starts with cybersecurity and the role of cybersecurity frameworks in small businesses; the NIST framework is described and the proposed framework is also presented and concludes with the chapter summary.

### **5.2 CYBERSECURITY**

Cybersecurity plays a significant role in this digital era with a society that uses cyberspace to connect the personal and business arenas (Torres & Thompson, 2020). The exposure to cybercrimes and attacks has increased, especially in the SME sector. Small businesses are the main target for potential cybercrimes that affect their economic growth and eventually cause reputational damage (Li et al., 2018; Armenia et al., 2021). Hackers use cyberspace to lure and violate security owing to poor adherence to the policies and sometimes the absence of security guidelines. Cybersecurity presents a combination of risk management approaches, tools, policies, security concepts, and safeguards (Armenia et al., 2021). It also presents procedures, actions, training, and best practices (Fernandez de Arroyabe, & Fernandez de Arroyabe, 2021) as well as assurance and technologies that share an interest in protecting the business environment, people and assets (Van Haastreht et al., 2021).

Research indicates a low motivation for improving cybersecurity for SMEs (Van Haastreht et al., 2021). However, the cyberrisk management process is essential for all businesses. There is a significant need to adopt a cybersecurity survival strategy to improve business continuity (Armenia et al., 2021).

### **5.2.1 SMEs and Cybersecurity**

Cyberspace has gained more attention in modern days. That means since the Covid-19 pandemic, all institutions, including SMEs, rely on the Internet to grow and attract clients (Ncubekezi & Mwansa, 2021). For SMEs, the use of cyberspace brings more flexibility in the sense that the SME sector can grow their businesses through the Internet (Li et al., 2018). Staff can multitask to increase productivity and innovation (Osborn, 2015) as well as attract new business prospects and increases their competitiveness. Considering these benefits of the Internet for SMEs, the literature shows a high presence of intruders, which threatens the cybersecurity of SMEs. The sector is vulnerable to various crimes owing to a lack of finances and resources to handle cyberrisks and attacks (Gregoriades & Karakostas, 2004). In addition, the lack of cybersecurity awareness and knowledge of SME employees reduces their appetite to improve attitudes toward cybersecurity (Ncubekezi, 2021).

The debate has been going on about the connection between cybersecurity and the SME sector (Ponsard, Grandclaudon & Dallons, 2018). Various scholars have highlighted the fact that the industry does not consider security an essential part of the business. The evidence is that the minimal or no budget caters to cybersecurity (Armenia et al., 2021). Ncubekezi, Mwansa, and Rocaries (2020a) explain that cybercriminals do not look at the business's size; instead, they focus on the lucrative benefits. As a result, during the global Covid-19 pandemic, the rise of cyber criminals was due to their innovative skills to compete with cyberusers. The SME managers have a misleading sense of security which opens doors for cybercriminals because the risk evaluation is compared with other big businesses rather than their loss. Consequently, the SME sectors mostly lack clear cybersecurity guidelines, which could be used as a blueprint to enhance security measures and provide good cyber hygiene. Likewise, the sector pays little attention to the cybersecurity policies and processes which could be adhered to (Osborn, 2015).

Ponsard, Grandclaudon and Dallons (2018) attest to the poor adherence to cybersecurity policies, rules, standards and procedures resulting in a negative outcome. Osborn (2015) highlights the fact that the SME sectors have experienced a shockingly high securityrisk that denotes high vulnerability. Malware has been one of the main strategies to lure the industry. The SMEs' online presence exposes them to a range of cybercriminals, such as phishing emails which falsely raise hope for better opportunities to grow the businesses. In addition, the SMEs' ignorance of the implementation of cybersecurity

procedures and lack of awareness increases the chances of exploiting their systems. Consequently, the SME sector has become the target for cybercriminals (Ncubukezi, 2021).

### **5.2.2 Principles and Guidelines for Cybersecurity Risk Management**

The ISO 27000 standard comprises over 130 security controls in 11 key areas. However, not all rules can be applied because the controls and key areas can be chosen according to a professional risk assessment. As a result, the SME should verify which standard has too many controls that are not relevant to its circumstances. Risk management (RM) is not about running away from uncertainty. Instead, the primary focus is on applying appropriate measures to avoid risks. ISO 31000:2018 is one of the risk management guidelines or principles that is not specific to a sector. Instead, it works for all industries, including public or private, teams or individuals. Organisations use ISO 31000:2018 for decision-making, business operations, performing processes or functions, implementing projects, producing products, rendering services, and asset management. ISO also works well with any risks, regardless of the nature of the risk and the possible consequences they may carry.

ISO 31000:2018 offers standard rules and procedures for all organisations to encourage consistency and standardisation. Risk management plans and frameworks involve designing and implementing them at every organisation based on needs, which include its objectives, background, arrangements, processes, procedures, tasks, plans, products, services, assets, and specific practices. ISO 31000:2018 complements risk management processes in the existing and future standards. It also offers methods for supporting and handling particular risks per sector. It, however, does not replace the existing ones and does not intend to provide certification.

### **5.2.3 Cybersecurity Risk Management in SMEs**

It is always essential to manage cyber risks in the business sector. Generally, thorough and real risk management and control can bring several positive benefits to business sectors. Organisations ranging from big to small enterprises could be in private or public industries and enjoy the same benefits. All organisations need risk handling to prepare for unexpected downtime or sudden shocks to the businesses. The business's available resources may reduce unnecessary waste and unexpected cyberfraud. As all businesses aim to deliver services, cyber risk management should increase the production and delivery of services in a reasonable turnaround time. Also, proper cyber risk management helps improve the contingency plan, minimise downtime, promote healthy systems, and maintain maintenance activities, ultimately lowering costs. Lastly, robust, firm, innovative risk management strategies could improve the business and promote a balanced cybersecurity system.

During the Covid-19 pandemic, SMEs were advised to adopt new technologies such as the Internet and related services. However, with the Internet's convenient benefits, most SMEs grabbed the opportunity



without clearly understanding the risks which come with it. Nonetheless, the possible risks of exposure to cyber risks relating to a range of cyber threats and their vulnerabilities were underestimated by SMEs. Unfortunately, the situation has led to real challenges for SMEs, and there is a need for transparent management of cyber risks (Alahmari & Duncan, 2020).

The main aim of cybercrimes is to harm or damage, disturb, interrupt or dent the business's daily operations, which ultimately grows the sector (Van Niekerk, 2017). Cybercriminals use different attack strategies to gain a lucrative portion of the company, which exposes businesses to various risks (Almeida, Carvalho & Cruz, 2018). Risk is one of the challenging elements at SMEs and requires business owners to manage it differently. Therefore, risk and management become a warning signal for every company, particularly SMEs, which are most vulnerable to business risks (Smit & Watkins, 2012). The risks are the results of the effect of cyber threats. Every business should have a cybersecurity strategy that improves and enhances the privacy of information and the safety of people and assets.

#### **5.2.4 Cybersecurity Strategy**

A cybersecurity strategy aligns organisational efforts with an improved attitude toward security (Almuhammadi & Alsaleh, 2017). It balances acceptable norms and opportunities presented by the Internet. Bell (2017) states that SMEs are uniquely positioned for the usage of cybersecurity techniques. SMEs are challenged owing to a shortage of staff and may not designate somebody to execute the procedure without an organisational structure. However, owing to the increased cybersecurity vulnerabilities, all institutions must have a well-defined and executed cybersecurity procedure. Indeed, in spite of the fact that a cybersecurity procedure may not dispense with dangers, it can provide a better chance for arranging and assessing the introduction of institutions to security measures (Mierzwa & Scott, 2017).

### **5.3 ROLES OF CYBERSECURITY FRAMEWORKS**

Generally, frameworks present clear, detailed guidelines, procedures, standards, and rules to protect businesses and their systems. The framework addresses the preparedness of the companies, the mitigation strategies, and the post-attack strategies to work together in managing, controlling, and reducing cybersecurity risks. A framework to mitigate risks should contain activities and a set of compliance controls. The literature indicates that the SME sector does not have a budget assigned to cyber risk management, unlike large businesses. Even though most SMEs do not have a structure for cybersecurity risk management, it becomes essential for them to have a consolidated transparent system and guidelines translated into a framework to manage cybersecurity strategies. The frameworks identify what already exists and how they fit in or are adapted for use. For this study, the framework will form the core foundation of a cybersecurity standard and strategy at the SME.

The frameworks are essential for the small business sector to manage cyber risks regardless of employee awareness and understanding to control and manage cyber threats. All the frameworks focus on reducing and mitigating cyber risks, human-related activities and shaping people's behaviour when handling adversaries and malicious individuals. However, institutions have still not yet adopted the frameworks owing to several hindrances that ultimately expose them to a diverse range of cyber risks that are difficult to manage. The framework also helps to conduct a thorough risk assessment for organisations. It complements existing commercial administration and cybersecurity measures and gives the administration something with which to make informed choices. It is technology-neutral and employs pre-existing rules, guidelines and procedures.

### **5.3.1 Barriers to Adopting Cybersecurity Risk Frameworks**

The literature identifies the lack of risk management, governance, and awareness as the main potential barriers which could hinder the adoption of cybersecurity frameworks in different institutions (Armenia et al., 2021). The governance in cybersecurity frameworks promotes continuous risk assessment to prepare adequate protection strategies. However, poor governance implementation leads to a flawed risk management plan and poor attitudes and awareness, which could be an entry point for emerging cyber threats. Therefore, SMEs need to integrate a culture of good cybersecurity with good cyber hygiene.

In addition, organisations have revealed several other barriers to adopting the cybersecurity frameworks: lack of budget, limited computer literacy, little attention to cybersecurity, lack of management support, and outdated software and hardware (Nicho & Muamaar, 2016; Bali, 2018, Loonam et al., 2020). Even though situations may not be the same for business sectors, the main barriers relate to the poor use of technological tools. Other barriers are misalignment of the appropriate tools, lack of automotive controls such as a firewall, automatic updates of the antivirus and anti-spyware, poor monitoring, few compliance tools and no dedicated cybersecurity officers (Abdullah et al., 2018; Parikh, 2019; Kahle et al., 2020).

### **5.3.2 NIST Benefits for SMEs**

Adopting NIST for organisational needs has several benefits that leverage the implementation of the cybersecurity framework. The NIST cybersecurity framework can integrate seamlessly with existing organisational cybersecurity policies or procedures and align cybersecurity with acquisition processes. For example, businesses can incorporate the framework in their cybersecurity risk management, organisational cybersecurity evaluation, incident-reporting of the cybersecurity risks, maintaining and managing cybersecurity requirements, cyber risk detection computer programs, and understanding cybersecurity risks.

### 5.3.3 Related Studies

The NIST framework can be effectively used in various settings. Benz and Chatterjee (2020) used the NIST framework to develop the methodology for the least mature and most vulnerable SMEs. Their study proposed a cybersecurity evaluation tool (CET) with 35 survey questions aimed at IT leaders.

## 5.4 NIST CYBERSECURITY FRAMEWORK

The NIST framework originated in the United States (US) as the policy that provides computer security guidance for best practices or standard practices that help businesses to evaluate and improve the capacity to detect, prevent and respond to all cyberattacks (NIST, 2014). It also aims to improve critical infrastructure security. The framework also reduces cyberrisk levels and defines the standard methodology for managing cyberrisks. Even though most institutions have defined policies or procedures that address cybersecurity, it becomes essential for institutions with more complex cybercrimes to adopt the NIST framework to develop and maintain these policies. The NIST provides a broader, more balanced form of cybersecurity that suits all business sectors (Cockcroft, 2020).

This study adopted the NIST framework to develop a cybersecurity tool that offers a solid foundation for a useful evaluation of and a list of recommendations for cybersecurity at SMEs. The framework has a set of five continuous and concurrent functions that address the different steps for processing cyberthreats: Identity, Protect, Detect, Respond and Recover as shown in Figure 5-29 (NIST, 2018: online).

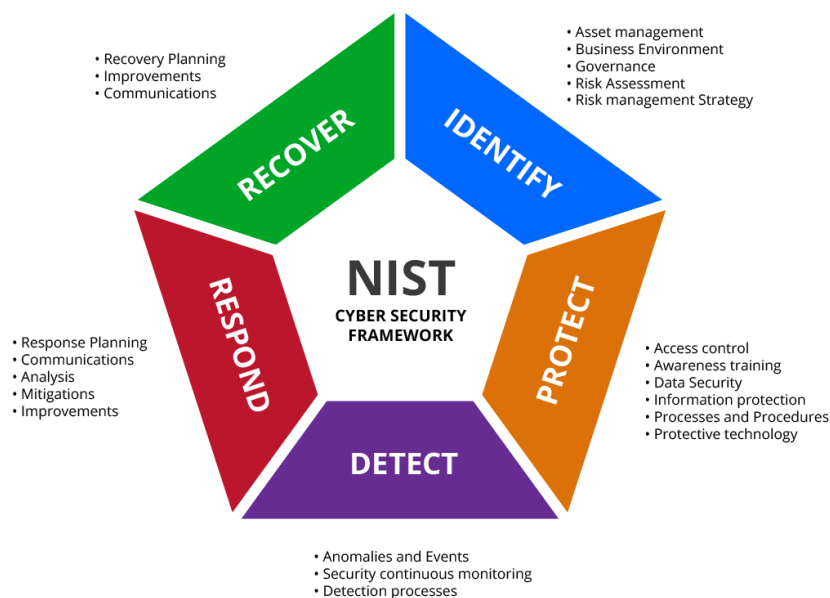


Figure 5-29: NIST Cyber-security Framework 1.1 (NIST, 2018: online)

Even though the framework cannot help all sectors as a ‘blanket approach,’ the framework’s intention is not to follow a certain route as it represents the dynamic experiences of cybersecurity risks at most institutions. The framework promotes the integration of business with the management of cybersecurity. It also evaluates, manages, maintains, and aligns cybersecurity risks (Cockcroft, 2020). In this study, the framework provides businesses with ways to describe the state of cybersecurity as well as the ideal state of cybersecurity, prioritising security loopholes, improving security, and bringing awareness to the system users.

#### **5.4.1 Relevance of AgenaRisk Package variables to NIST CSF components**

The increased presence of cybercrimes in cyberspace highlights the demand to assess and calculate cybersecurity risks to plan effective protection measures. It becomes essential for the SME sector to take steps that manage and assess cybersecurity risks (Van Haastrecht et al., 2021). A CSF is necessary for any imminent security work (McGraw, 2005). Considering the cybersecurity role in SMEs that significantly contributes to the country’s economy, it becomes essential to design and develop the framework for SMEs using the NIST framework. As documented, NIST is an internationally recognised cybersecurity framework (Armenia et al., 2021). As a result, the framework is widely and increasingly adopted to strengthen and improve the safety of businesses (Cockcroft, 2020).

The international framework provides rules, guidelines, procedures, best practices and standards for risk management, which has an unchanging point of view for the business setting (Armenia et al., 2021). The interest of the study is on the SMEs in SA, which have been faced with an increased number of cybercrimes and require guidelines for managing cybersecurity. This necessitates a practical and effective model to define the cybersecurity risk profile during these critical times. The current work recommends aligning the NIST core functions with the Bayesian network model for risk assessment to determine the risk probability and impact. The use of the Bayesian network tools incorporated in AgenaRisk package is thoroughly discussed in Section 3, where variables are clearly explained. In this chapter, the NIST core components are aligned with the variables used in the conceptual model created using AgenaRisk package. The study further developed five simulated case scenarios to assess the risk likelihood and impact. The study can benefit small businesses interested in managing their cybersecurity risks.

This work proposes an actionable CSF for small enterprises with guidelines for maintaining minimal impact on SMEs. The NIST cybersecurity framework guides the design and development of the framework for SMEs in SA. The five core functions of the NIST CSF are used to:

- Identify business assets, systems, data, people, and capabilities.
- Protect the business elements to promote the safe delivery of the services.

- Detect risk activities to identify the rate of a cybersecurity incident.
- Respond to acts against the identified cybersecurity event.
- Recover by identifying actions to reduce the impact of a cybersecurity incident.

The design of the cybersecurity tool for businesses is shaped by the ideas and experiences of the SME sectors. All these framework functions are broken down and categorised into actionable practices relating to SMEs. Data were collected from the sample research participants to inform the framework's design and development in order to implement the insights gleaned from real-life cybersecurity risks.

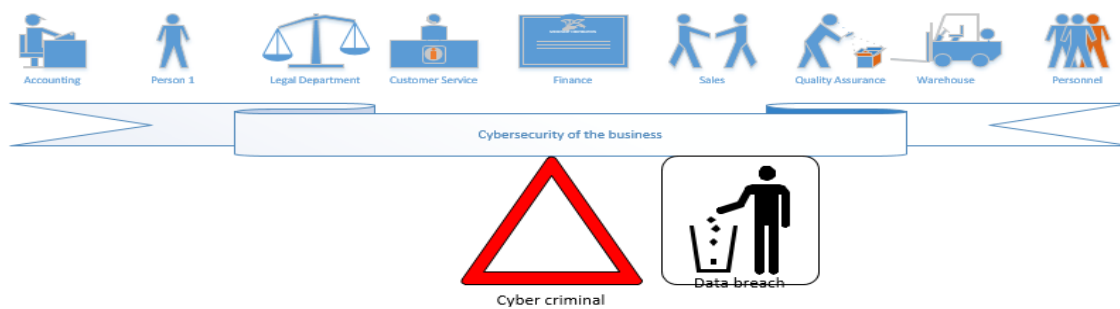
**Table 5-6: Alignment to the NIST Cyber Security Framework 1.1 Core components. (Data source: survey, 2021; NIST, 2018)**

Function	Category unique	Category	Description of the adopted NIST Phase	Survey items	Variable on the model
<b>Identify</b>	ID.AM	Asset Management	Identify assets such as employees, devices, data, and systems.	Hardware, software, email and application system within the business systems should be protected regularly.	End devices Protection level
	ID.BE	Business environment	Clarify employee responsibilities, cybersecurity guidelines, risk strategies and management to achieve business goals	The critical infrastructure, as third-party service, should only work according to the security guidelines in the emails.	Physical security software
	ID.GV	Governance	Availability of cybersecurity procedures, policies and guidelines to monitor and manage all risks and cybersecurity-related risks.	Define cybersecurity policies, procedures, guidelines, and rules for adequate security.	Policies, guidelines & cybersecurity
	ID.RA	Risk assessment	Business managers promote business continuity through cybersecurity risk management of all business functions.	Management should identify internal and external cyberthreats, attacks and asset vulnerabilities.	Third-party planned or unplanned attacks
	ID.RM.	Risk management	Make decisions based on cyberrisk, third-party constraints, vulnerability, and tolerance.	Identification of the risk management strategy	Protection measures, malware, guidelines
<b>Protect</b>	PR.AC	Identity management & access control	Identify, manage, restrict and monitor physical, logical device system processes and facility access to guard against unauthorised access.	Use passwords and authentication methods on end devices, systems, and emails.	End devices, policies, management, guidelines and protection measures
	PR.AT	Awareness and training	Offer cybersecurity awareness training, guidelines, and education to carry out cybersecurity-related tasks and responsibilities effectively.	Experienced personnel must bear responsibility for the initial setup of all systems and devices and deactivating old accounts	Management, policies, guidelines, and protection measures
	PR.DS	Data security	Use the risk strategy to promote integrity, confidentiality, and availability of information.	Awareness of employees to understand cybersecurity risks and best practices needed to operate the business's IT systems safely.	End device, employees, policies, and guidelines
	PR.IP	Information protection & procedures	Cybersecurity guidelines or procedures promote the safety and security of information, assets, and processes.	Only legitimate users should access information about systems needed and about their jobs.	End device, employees, policies, and guidelines
	PR.MA	Maintainance	Monitoring performance of maintenance systems through policies and procedures that promote safety and security.	Management to take responsibility for regularly enforcing the change of passwords, system and device setup.	End device, employees, policies and guidelines
	PR.PT	Protective technology	Policies clearly outline procedures that promote all business assets' safety, security and resilience.	Regular backup of the critical information, systems and data which is periodically reviewed.	Policies, guidelines, and protection measures
<b>Detect</b>	DE.AE	Anomalies and events	Detect anomalies and potential attacks through technologies that generate an early warning on the system.	Protection software (antivirus, anti-malware, etc.)	Policies, guidelines, and protection measures
	DE.CM	Security continuous monitoring	Identify vulnerabilities relating to cybersecurity and their source to take proactive protection measures.	Frequently updates the software, hardware, physical security and device encryption.	Policies, guidelines, and protection measures
	DE.DP	Detection processes	Run penetration tests and deploy proactive systems that will send early warning signs.	Deployment of the proactive detection systems will send alerts when the system is attacked.	Protection measures, end devices, policies
<b>Respond</b>	RS.RP	Response planning	Have a clear guide describing the plan for incident response and deploy proactive detection systems that will protect the system	Use of firewalls against unauthorised access on systems, wired or wireless networks.	End devices, policies, guidelines, and protection measures
	RS.CO	Communications	The incident management system connects the internal and external stakeholders.	Communicate with all business structures and third parties.	Management, employees, systems & guidelines
	RS.AN	Analysis	Clear guidelines about the process of analysis to effectively respond to incidents.	The dedicated IT and cybersecurity personnel can analyse the system's security from criminal attacks and malware or strengthen its security.	Management, policies, guidelines, and protection measures
	RS.MI	Mitigation	A structured plan to prevent and reduce risks and resolve incidents.	Continuously update hardware and software.	Policies, guidelines, and protection measures
	RS.IM	Improvements	Activities and efforts to improve risks, incident management and removing obsolete software or devices.	Obsolete software or devices should be thrown away or disposed of.	Policies, guidelines, and protection measures

<b>Recover</b>	RC.RP RC.IM	Recovery plan	A clear recovery plan and implementation are communicated to improve the privacy and safety of the business systems and assets	Regularly review the system – to back up information and processes	Policies, guidelines, and protection measures
----------------	----------------	---------------	--	--	---

## 5.5 CYBERSECURITY AND CRIMINALS

Cybersecurity is an ongoing and worrying issue that has become more popular in academia. Its main focus is on the overall protection of networked connected systems made up of software, hardware, people, and data. Owing to the openness of internetworked systems, cyberattacks have become a significant inconvenience that requires safety and security measures. Similarly, human factors relating to employee behaviour, attitudes, values, understanding, awareness, and actions can compromise the business system (Kabanda, 2018). The growing demand and business exposure to cybersecurity require risk analysis to become an essential and integral part that supports businesses in controlling and managing cybersecurity risks. Cybersecurity becomes the mediating factor between the business and its cyberattackers or criminals. Consequently, for information security, privacy and safety, cybersecurity stands between the actions and decisions made by the organisation and the criminal's actions. Figure 5-30 demonstrates the cybersecurity between the business and intruding cybercriminals.



**Figure 5-30: Cybersecurity as the mediating factor between business and criminals**

Cybersecurity protects and secures cyber-related assets in light of its role in the business. Cybersecurity protects legitimate people and criminals with conflicting interests in business information and resources. As the study aimed to design, develop and evaluate a cyberrisk model for SMEs in SA, the introductory chapter discussed the research objectives, which mainly focused on determining the cyberrisks in the small business sectors. After a thorough analysis of cybercrimes, the study proposed the adoption of artificial intelligence (AI), which will help to present various risk scenarios faced by the SME sector graphically and their likelihood of risk. The study proposed using the Bayesian Network with artificial intelligence (AI), which is discussed below. Yermalovich and Mejri (2020) suggest the usefulness and relevance of predicting the different cyberthreats and attacks to identify the risk levels.

## 5.6 BAYESIAN NETWORK BACKGROUND

The Bayesian networks (BNs) are sometimes called Bayes networks, Belief Networks, Bayesian Belief Networks, or Probabilistic Networks (Sevinc, Kucuk & Goltas, 2020; Verzobio et al., 2021). The BN



with AI defines the conditional independencies in the BN and allows class-dependent independencies to be determined between subsets of variables (Cai et al., 2018). AI is the art of finding methods for solving complex, complicated problems requiring the same intelligence level. Bayes' theorem predicts, evaluates the risk, and updates the predicted probabilities of the risk event by incorporating new information (Serrano et al., 2018), thus helping to make the right decision based on complex dependent or independent data. Thomas Bayes' Model predicts how to determine the probability of the cyberrisk and its conditions. The model uses mathematical formulae to calculate the conditional probability of the possible cyberrisk cause for a given observed outcome (Aguessy, 2016). The conditional probability is computed from knowledge of each cyberrisk, the chance of it occurring and the likelihood of each cause's outcome (Gupta, 2017). This study used AgenaRisk package which can produce a graphic model illustrating relationships of the variables where learning is performed as well as the classification of the variables.

According to Fenton and Neil (2018), the Bayesian Network uses data to build and influence diagrams to illustrate the risk probabilities in the cybersecurity field. The BN assesses the risks by performing risk probabilities based on the data and value of information. The use of the BN and its effectiveness in cybersecurity is evident when analysing risk uncertainties (Xie et al., 2010). Four types of the Bayesian Network are commonly used, so the Bayesian selection from the four types is presented below.

### **5.6.1 Bayesian Selection**

There are three entities that make up the multi-entity Bayesian network (MEBN), namely Bayesian network (BN), Dynamic Bayesian network (DBN), and the attack-based Bayesian network (De Wilde, 2016). This study adopted the MEBN, which uses elements to present security threats, indicators, and measures, and the DBN. The MEBN and DBN are an extension of the BN even though they take less time to generate the BN. The MEDN is relevant because the current research analysed cybercrimes in the business sector and also designed and developed the security tool for cyberrisk mitigation that requires different influencing variables connected to the effect of risk. Even though risks can be positive and negative, the study demonstrated the possible options that yield the outcome. In addition, this study used the DBN because the cases presented in Section C, Part 2 are unique for each case and illustrate the possible stages in which the risk outcome can be achieved. So the tool required all the risk variables with different values connected to produce a cyberrisk. The relevance of the Bayes Network in this study is presented below.

### **5.6.2 Relevance of the Bayes Network in the study**

AgenaRisk was used with Bayesian Network tools to predict the risk probability for cyberrisks in the SME sector. AI also simulates human intelligence processes like computer systems. Human intelligence

processes include learning and reasoning (Russell & Norvig, 2010). Learning is seeking and acquiring information, including the rules and instructions for using data (Fenton & Neil, 2018). Reasoning uses the rules to reach estimated decisions and self-correction. AI represents an area in the computer sciences that focuses on the creation of intelligent machines which work and react like humans (Russell & Norvig, 2003). The study focuses on the second definition, making the right decisions and finding solutions for complex problems.

This interest in AI will involve how machines simulate intelligent human behaviour, including thinking, learning, reasoning, and planning. AI with the Bayesian approach will help determine the complex risk scenarios, including the dependent, independent, and exclusive cyberrisk causes, which results in decision trees (Fenton & Neil, 2014). The decision trees are the models which presents a tree of decisions and the related consequences such as the outcomes of an event and the relationships of the variables based on the conditional statements. Also, the model will provide some truth to the meaning of the more diverse cyberrisk situations. The Bayesian Model will also determine the cyberrisk caused by mutually exclusive and exhaustive events. A new trend is applying the BN theory to risk assessment. Theoretically, there is minimal research on Bayesian networks' cybersecurity and data privacy. Consequently, it is unclear how the Bayesian network can be effectively implemented in cybersecurity. It becomes essential for businesses to predict and determine the likelihood of risk in data breaches. For example, businesses could experience data breaches when insiders (employees) perform actions based on their attitudes, ignorance and poor decision-making. Similarly, cybercriminals could use the loophole caused by poor employee decision-making to access unauthorised data.

This study has adopted the BNs to determine cyberrisk independent and dependent variables, which result in significant data breaches. With the use of this technique, it becomes possible to assess the likelihood of data breaches. Even though there are minimal studies on the use of BNs in cybersecurity and privacy, this study adopted the BN technique to develop a model that could be used to determine risk probability. The adoption of the BN in this study contributes to new knowledge by designing, developing, and evaluating a model in which a group's data breach was observed by means of prior indicators, with the business protection measures predicting the likelihood of a data breach at the SMEs. As described in the previous section, this model combines accidental employee threats and intentional malicious threats. The study presents scenarios that demonstrate different observations based on the prior indicators and the best combination of measures that are most likely to minimise the probability of data breaches.

This part of the chapter develops the cybersecurity risk tool for small and medium-sized businesses. The work addresses the steps and elements used to design the risk tool to reduce and combat cyberrisks. The study performed a qualitative risk analysis by identifying the common risks to SMEs. The

quantitative risk analysis addresses the likelihood of cyberrisk and probability of avoiding, reducing, transferring, accepting and responding to risks. Designing the model by using the probabilistic graphical technique requires a set of variables that could sometimes be interdependent (Jensen, 1996).

The Bayesian Model defines the Bayesian rule that states that the prior probabilities should be used to compute the posterior probabilities. In an equation, Baye's theorem says the posterior probability is  $P(A|B)$ , which can be computed based on  $P(A)$ , or it can be presented as the conditional probability  $P(B|A)$  (Mo, Beling & Crowther, 2009). The technique can be used with any available data to make a framework. The Bayesian tool uses the nodes as variables and the arcs present the links that connect the variables and the dependencies.

$$\text{Equation 1: } P(A|B) = P(BxA) \times P(A)/P(B)$$

The Bayesian theorem treats the group of prior probabilities to the posterior probability in a hierarchical network, yielding the second equation. The second equation means that the posterior probability presented as  $P(A)$  is made of a group of prior probabilities presented as  $P(A|B1)$ , which continues until  $P(A|Bn)$ , which can be related to  $P(Bi)$  values:

$$\text{Equation: } P(A|B) = P(B \times A) \times P(A)/P(B)$$

The researcher has used the quantitative research approach to generate numerically developed facts. The approach quantified the ideas, behaviour and other defined variables from a more significant population. The approach formed the knowledge base for AI in combating cyberrisk. The Bayesian approach with AI calculates the risk probability using different variables for the dependent and independent cyberrisks (Ghasemi et al., 2018). The BN uses the directed acyclic graphs for various analyses to demonstrate the risk probabilities and to handle various data sets. (Kabanda, 2020).

## 5.7 RELATED WORK

Even though the prediction of risks and sensitivity analysis using the Bayesian Network is beneficial for all sectors, minimal research has been conducted on using the Bayesian Network in predicting information and computer-related risks in small businesses. However, some studies have used the Bayesian Network in different sectors. Sevinc, Kucuk and Goltas (2020) researched a Bayesian network to predict and analyse the most likely causes of forest fires in Southwest Turkey. Their study revealed that the month and temperature were the leading influential factors for fire ignitions. Another author, Dlamini (2011), used the Bayesian network to estimate the risks of fires in Swaziland. He used the geographic information system (GIS) and remote sensing data. His study selected 13 explanatory variables processed to generate fire risk maps and analysed them using the BN and the GIS. The results of the probabilistic outputs were used to manage and mitigate risks.

Cai, Huang, and Xie (2017) present the approaches for diagnosing faults using the BN and provide a series of classification schemes. The diagnosis aims to help technicians in Engineering to isolate, detect and pick up faults and troubleshoot them. The study used the BN as the probabilistic graphical model dealing with uncertainty scenarios. Their paper contributed to the field of fault diagnosis methodology with BN and the BN classification schemes in fault diagnosis. Consequently, this study applied the Bayesian network to a small business setting to predict cybersecurity risks by enabling uncertain scenarios. The Bayesian network graphically presents the identified components and interactions of the variables measured in conditional probabilities. The technique is used to illustrate simulated case scenarios relating to the cybersecurity risks at the SMEs in SA. The contribution of this work demonstrates the importance and brings awareness of cybersecurity risk probabilities and their impact on SMEs.

## **5.8 AGENARISK WITH BAYESIAN ARTIFICIAL INTELLIGENCE TOOLS**

This study used the AgenaRisk Desktop package on a Windows operating system to design and develop cybersecurity risk models and simulated scenario for risk probabilities. The method was founded more than two decades ago. Fenton and Neil (2014) explain that the Bayesian network uses decision-support software to assess risk probability. AgenaRisk package is in Bayesian Artificial Intelligence (AI), specialising in modelling and determining probabilities of complex and risky scenarios to improve decision-making (AgenaRisk, 2021). The technique predicts and makes decisions by combining data, dependent variables, and general knowledge about simulated scenario cases. Even though the AgenaRisk package can be used on various platforms to model risks, this study uses the method to model cybersecurity risks at SMEs in SA.

This study used the BNs in cybersecurity and privacy of business information, demonstrating the intentional malicious and employee-generated threats through end devices such as computers or smartphones. Malicious threats could gain access to unauthorised business information through the business device. This could result from the employee's ignorance in adhering to and applying security measures (Ncubekezi, Mwansa & Rocaries, 2021). In the same context, the insiders could ignorantly become the weakest link in the business system owing to work overload, stress, inappropriate behaviour, poor adherence to security measures or decision-making, lack of awareness or skills and lack of policy enforcement (Ncubekezi, 2022a). So, in this work, the BN predicts risk likelihood at SMEs in SA. This study has designed the first model based on common sense and relevant literature. The researcher grouped the protection measures as a variable for clarity and simplicity and developed the risk assessment tool further.

The BN is used to design and develop cybersecurity models to understand better and to analyse the risk impact and uncertainty in various sectors, including financial, and project management (Richardson et al., 2019). AgenaRisk is used to visualise the potential outcomes and give a better illustration and interpretation of the security risk. The models demonstrate different experiments with nodes, with their assigned values, to produce an outcome based on the likelihood of each outcome and the impact. Most variables used in the models are dependent. The illustrations demonstrate the probability distribution of the variables, which can be iterated at many different times with random inputs using random number generators. Outputs of the models determine the probability of each outcome owing to specific uncertainties. The aims of the different outputs can inform the planning of a mitigation response.

### **5.8.1 Using Collected Data to Plan for Bayesian Network**

This part of the work used data from prior chapters to design the conceptual models. This data has been used to inform the database for Bayesian Network simulation, which analyses the likelihood and impact of cybersecurity risks at SMEs. Risk likelihood and impact assumptions should occur with existing qualitative data. The empirical data for making assumptions will be from past SME cyber risk experiences or historical data. The technique uses random values to simulate the risk likelihood from different variables. The model calculates the results by repeating the action multiple times based on any other random values and comparing the results of each value. The technique also determines the sensitivity analysis using Tornado graphs and decision trees based on the high sensitivity.

## **5.9 APPLICATION OF THE AGENARISK IN THE SME SECTOR**

This part of the study used the Bayesian network with AgenaRisk to predict the probability of cybersecurity risks caused by planned and unplanned attacks in business systems. This study focused on employees' and criminals' cyber threats and actions. Employee-generated attacks are also known as inside or human errors that ultimately result in deletion, loss and data modification (Elmrabit et al., 2020). Criminals' intentionality compromises the system through planned attacks, while human factors are accidental actions influenced by employee ignorance and poor decision-making.

At the same time, criminals look for a loophole in the unsecured system and deploy malware attacks, phishing attacks and other cyber-attacks. A study by Kjærulff and Madsen (2006) suggests considering the use of variables when designing the model structure. So these variables are used on the generic Bayesian, secondary, Beta, and Alpha models. The ultimate variables selected for the models are the primary node, prior indicators, and the measures. So, the problem-related variable information and mediating variables were selected with the correct type and are discussed below.

### **5.9.1 Problem-related variable**

The variables produce observations related to the predictions, decisions, and diagnoses. The variables pose an interest in the problems to determine the cyberrisk probability that results in the ultimate data breach owing to planned and unplanned actions. The variable cannot be observed in isolation or directly; therefore, the variable is a problem variable.

### **5.9.2 Information variable**

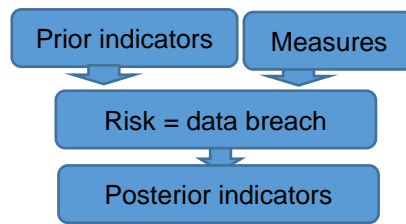
The information variable mainly carries vital information which determines the solution. This variable is made up of the symptoms and background information. The symptom information represents the results when a problem has occurred. So, in this case, the consequence of the occurrence of the problem results in posterior indicators. These consequences are illustrated and discussed clearly in Section C, Part 2, using different simulated risk cases.

The background information presents the prior indicators available before the risk consequence. Different risk scenarios are presented in Section C, Part 2, illustrating the background information before the ultimate risk takes place. The availability of the background information influences the risk probability and consequence in the BN model. The background information and the symptoms can connect and influence the risk consequence of a scenario. The last variable used in this study is the mediating variable presented below.

### **5.9.3 Mediating variable**

These variables are the offspring of the information and problem variables while being the parents of the symptom variables. These variables are usually essential for the appropriateness of the model. For example, in the BN model, these variables would include the level of protection which covers different measures used to protect the entire organisation or business. This variable is also used on the different models designed below.

These different levels of the variables can be connected dependently and independently to form the BN model structures. The use of these variables illustrates the different nodes which can be linked together even though not all BN models may have the same variables, some having only three variables than those shown in Figure 5-31. These variables are also applied in the following sections. As explained in the sections above, the prior indicators and the measure variables can influence the probability of the risk in the BN model. The effect of probability of the risk results in the posterior indicators showing symptoms of the affected nodes and risks posed by a certain case scenario. The models presented below demonstrate the use of the different dependent and independent nodes and their ultimate impact. This part of the work presents the generic, secondary, Beta, and Alpha models.

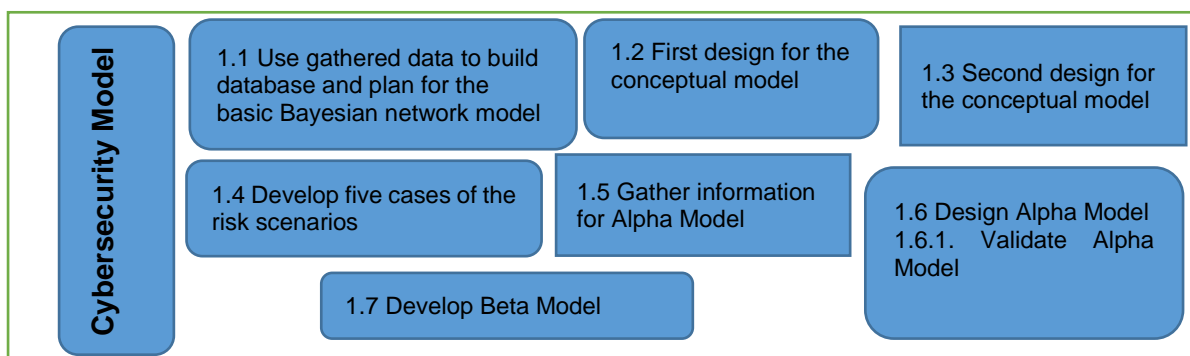


**Figure 5-31: Variables used on the Bayesian network**

### 5.10 AGENARISK PACKAGE FOR CYBERSECURITY TOOL DESIGN

After the risk management processes, the study further used the Bayesian Network tools in the AgenaRisk package to determine cybersecurity risk probabilities, using uncertain variables to answer the last research question. The study explored the ultimate and common risks, prior indicators and security measures. The researcher also used relevant literature to review the prior indicators of the threats and the measures used to mitigate cyber risks. The key terms used to search for the literature are human errors, cybercriminals, threat indicators, cyberattacks and prediction. Section 1 of the study presented the literature review with data breaches as the ultimate goal for accidental and planned threats. This phase presents the processes used to design and develop the cybersecurity framework for SMEs in SA. The cybersecurity framework design steps are from 1.1 to 1.7, as shown in Figure 5-32.

- **Phase 1.1** Use gathered data to build a database and plan the basic model;
- **Phase 1.2** First, design the generic conceptual model;
- **Phase 1.3** Second, design the secondary conceptual model;
- **Phase 1.4** Develop a risk case scenario;
- **Phase 1.5** Gather information for the Alpha Model;
- **Phase 1.6** Design the Alpha Model; and
- **Phase 1.7** Develop a Beta Model.



**Figure 5-32: Use of the Bayesian network**

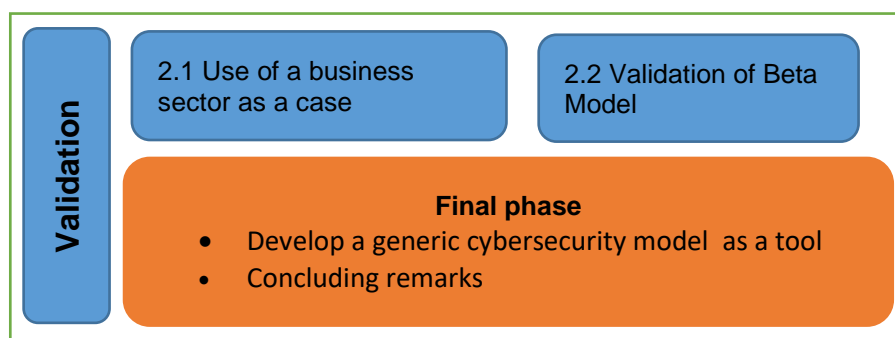
This phase answers Research Question 3 by designing the cybersecurity framework which uses the BN tools for SMEs. A first standard structure was created, followed by two conceptual models. The first model illustrates the direct and indirect relationships between the measures, prior indicators, and the essential variables. The second model was designed in detail, describing the roles of measures and prior indicators in information loss. Five different threat scenario cases were used to evaluate the model's effectiveness. The two models demonstrate clear and detailed connections between the variables, with the second model being more precise than the first model. After completing the two models, the study designed the Alpha structure focusing on human errors and criminal threats leading to data loss. At this stage, scenario-based cases were developed, demonstrating the simulated threat situation in the SMEs, which is the study's primary purpose.

The data gathered from qualitative risk assessment during the preparation stage and the two conceptual models to inform various cases using the Alpha Model. The Alpha Model indicated the risk likelihood of the relationships of the nodes between the set variables. The model also showed sensitivity analysis that links to the level of influence and absolute degrees of the variables. The likelihood of cyberrisk can be adjusted at any time to demonstrate the possible outcomes. The researcher then conducted interviews with the information security officers based on their expertise in privacy and security. The idea is to understand their view on cybersecurity, including threats (breaches). Suggestions from an interview with a security expert informed any revision and review of the Alpha Model and the validation. The following phase validated the tool using the Beta Model.

### 5.10.1 VALIDATION OF THE MODEL

This last phase shows that the study has three steps that lead to the final step.

- **Phase 2.1** Use of a business sector as a case;
- **Phase 2.2** Validation of Beta Model;
- **Final stage**



**Figure 5-33: Validation of the model**



In this phase, the researcher validates the usefulness of the Beta Model in the SMEs in SA, which addresses the last research question. Moreover, the study performed the final stage by developing the generic conceptual cybersecurity model in Figure 5-33. Two information security officials were selected and interviewed to validate the usefulness of the Beta Model and discuss the practical implications further.

**Final phase:** An Alpha and a Beta Model were used to develop a general model that could be adjusted for multiple threats.

After performing risk management, the study adopted the NIST cybersecurity framework. The selected framework explored the rules, tools, and controls essential to a successful business. For the success of this work, SMEs need to adopt a framework to improve management and reduce cyberrisks based on the recognised standards and guidelines.

## **5.11 CONCLUSION**

Cybersecurity in the business sector has been an ongoing debate. Even though many scholars have been engaging with the topic, minimal attention is paid to the security aspect of the small business sector. The evidence is in the inadequate finances reserved to save businesses from cybercriminals. This chapter looked at the state of cybersecurity, NIST as an internationally recognised cybersecurity framework, and how the NIST framework is applied in this study and SME context. It is recommended that the application and implementation of the NIST framework in the small business sectors to align with the existing controls. Its adoption would improve the state of cybersecurity, employee awareness, and training, thereby aiding the extensive implementation of cybersecurity as well as improving business security by proactively mitigating various cyberattacks.

In addition, the chapter accounted for the use and adoption of the AgenaRisk package with Bayesian Network tools that proactively reduce, and mitigate the increasing cyberrisks. The chapter further presented the adoption of the AI application through the use of AgenaRisk package specialising in modelling and determining cybersecurity probabilities of complex and risky scenarios to improve decision-making. The history and the relevance of the Bayesian network are discussed, including the related studies which successfully used the technique in their context.

## **SECTION C: TOOL DEVELOPMENT AND SIMULATION OF CASE SCENARIOS**

### **SECTION C: USE OF AGENARISK FOR THE DEVELOPMENT OF RISK TOOL**

Cybersecurity risk tool development and simulation of real-life case scenarios



This section consists of Chapter 6 which presents the tool development and simulation of the real-life case scenarios using the AgenaRisk package with Bayesian Network (BN) tools. Cybersecurity tools developed are presented as models, namely: Generic, Secondary, Beta, and Alpha models. Each model illustrates the nodes, prior indicators, elements, and discussion. In addition, the section evaluates the risks by simulating different real-life scenarios such the end devices, human errors, malware, phishing, and adherence to the policies and guidelines. Each case scenario showed the different nodes used, relationships, and the ultimate results.

## CHAPTER 6: DEVELOPMENT OF CYBERSECURITY RISK TOOL

### 6.1 INTRODUCTION

This chapter focuses on the development of the cybersecurity risk tool for SMEs. This chapter addresses the last objective that proposed the design, development and evaluation of the cybersecurity risk tool for SMEs in South Africa (SA) using the probabilistic technique. The illustration of the dependent and independent cyberrisks, their potential influences or prior indicators and the measures to be implemented are accounted for. This work identified the variables used to determine the risk probability using the Bayesian Network with the AgenaRisk. The study designed and developed different models to illustrate the risk probability for other cases. The study evaluated the models further by consulting security professionals for further guidance to improve the generic models.

A generic model, secondary model, Beta model and the Alpha models are presented with the model structure, effective nodes, prior indicators and the measures. All these models are used further discussed.

### 6.2 GENERIC MODEL

This study used graphical models to illustrate the design and development of cybersecurity risk in the SME sector. These visual models illustrate the relationships between the identified dependent and independent variables among cybersecurity threats, attacks, vulnerabilities, and exploits that have become the key players in determining the cyberrisk likelihood and risk impact. The researcher created a generic model structure with different variables and dependencies that can be customised to predict risks, as illustrated in Figure 6-35. Figure 6-34 illustrates prior indicators, measures, and the possible risk of an ultimate data breach as the main variables used to design the model in Figure 6-35.

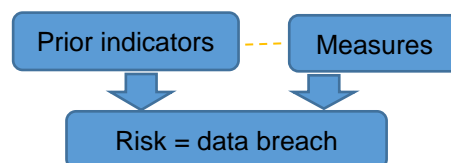


Figure 6-34: Variables for the BN structures

#### 6.2.1 Generic Model Structure

Figure 6-35 shows the complete generic model with essential connected nodes, prior indicators, and the measures demonstrating the generic Bayesian Model used by any sector that experiences cyberthreats and attacks. The model shows different nodes connected to produce a probabilistic outcome. The discussion of the generic model is presented below.

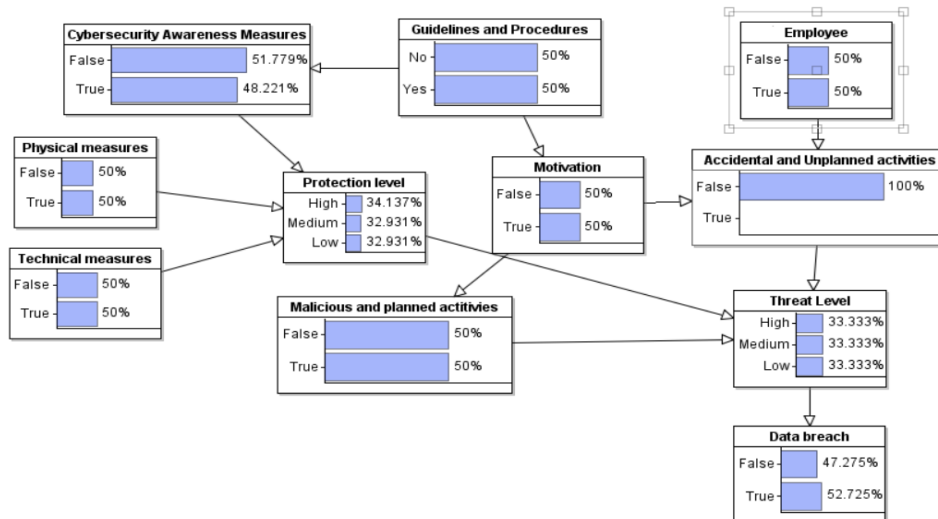


Figure 6-35: Generic Bayesian model

### 6.2.2 Different nodes

As shown in the model in Figure 6-35, the three identified nodes (data breach, planned activities, and unplanned activities) illustrated in Table 6-7 inform the model's ultimate goal. The variables use Boolean values (true and false). The primary problematic variable is the data breach which results from the planned (criminal) and unexpected (accidental) activities which trigger the threat level. The impact of these activities is described and shown in the simulated human error case study in the following part of the work.

Table 6-7: Main node and values

Main nodes	Node	Selected type	Values
	Information loss or data breach	Boolean	[True, False]
	Accidental or planned activities	Boolean	[True, False]
	Criminal or unplanned activities	Boolean	[True, False]

### 6.2.3 Prior indicators

The prior indicators represent the actions taken by the criminals and employees to breach the system. Likewise, prior indicators are opportunities resulting from the system security loopholes. Table 6-8 shows that prior indicators are the motivation or opportunity to compromise the system and increases the threat level. The threat level determines the extent of the exploitation of the system. These variables are ranked with values high, medium to low.

Table 6-8: Prior indicator nodes and values

Prior indicators	Prior indicators	Selected type	Values
	Motivation	Ranked	[High, Medium, Low]
	Threat level	Ranked	[High, Medium, Low]

## 6.2.4 Measures

Table 6-9 shows the five measures that need to be considered: protection level measures, technical measures, cybersecurity awareness measures, physical measures, and instructional measures. The protection level is ranked high, medium, and low, while other measures use the Boolean values of true and false. The protection level is the overall security of the business at all levels. Technical measures strengthen the hardware, software, and encryption. This measure uses multifactor authentication or encryption techniques to protect and secure systems. Cybersecurity awareness measures require regular awareness training and training programmes that constantly remind and equip system users. Physical measures cover the environment's safety and security where the computers and other business assets are stored. Lastly, instructional measures are the ability to use the available policies, procedures, rules, standards, and guidelines when using business assets.

**Table 6-9: Measure nodes and values**

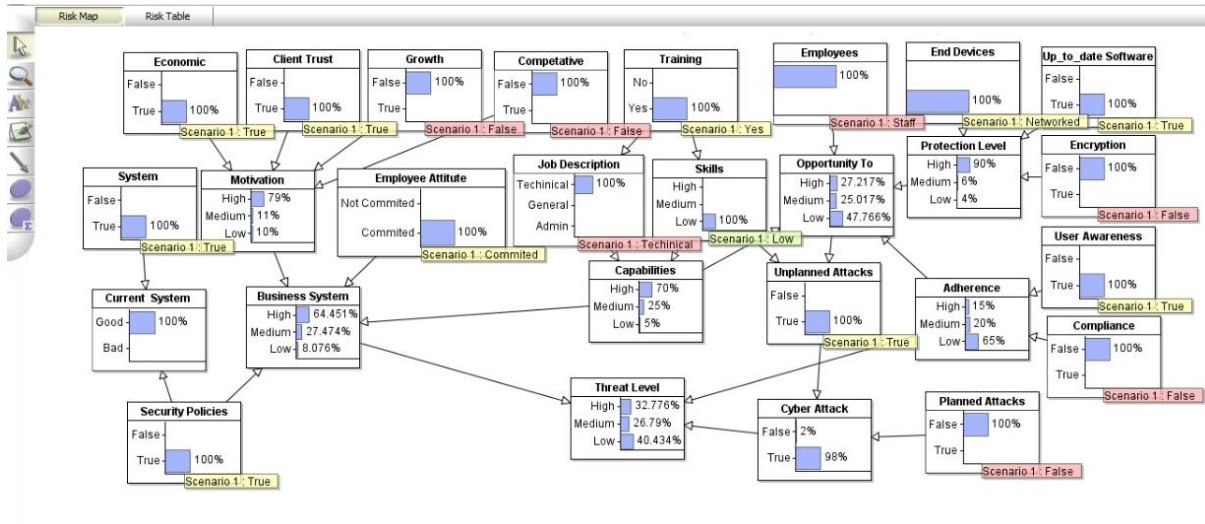
Measures	Nodes	Selected type	Values
	Protection level	Ranked	[High, Medium, Low]
	Technical measures	Boolean	[True, False]
	Cybersecurity awareness measures	Boolean	[True, False]
	Physical measures	Boolean	[True, False]
	Instructional measures (guidelines and procedures)	Boolean	[True, False]

## 6.2.5 Discussion of the Generic Conceptual Model

This section presented the generic conceptual model any business sector could use in different cyberthreat cases. Each cybersecurity risk can have multiple measure nodes and prior indicators. For each case scenario, it becomes essential to use related information, which will be on the conditional probabilities table (CPTs). As shown in Figure 6-35, the top nodes on the model do not directly influence the risk outcome. The directly connected node is more effective in determining the overall risk likelihood and impact. So, for the use of the generic model, the business sectors must use the nodes appropriately when creating the model structures. The model in Figure 6-35 should effectively assess the sensitivity analysis.

## 6.3 SECONDARY MODEL

In the previous section, the study presented the basic or generic model. This section presents the second model, which is an extension of the generic model. The complete generic model with connected elements is shown in Figure 6-36. The model has dependent and independent variables that illustrate the risk likelihood in the business systems.



**Figure 6-36: Second conceptual model or Secondary Model**

### 6.3.1 Elements of the Secondary Model

This model extends the basic model illustrating the risk likelihood based on the varying inputs to generate and output goals. There are dependent and independent variables that make up the secondary model. Each variable or node carries a randomised value. The various elements of the second model are discussed below.

#### 6.3.1.1 Secondary Model nodes

The basic nodes for the second model are the planned or unplanned attacks and the successful cyberattack shown in Figure 6-36 and Figure 6-38 and illustrated in Table 4-10 and Table 6-7. The variables use the Boolean values (true and false) and the ranking (high, medium, and low). A successful cyberattack results from planned or unplanned attacks on the system. The attacks are caused mainly by outsiders, the criminals, and insiders, the employees.

**Table 4-10: Secondary Model basic nodes and values**

Main nodes	Node	Selected type	Values
	Planned attacks	Boolean	[True, False]
	Accidental attacks	Boolean	[True, False]
	Cyberattack	Ranked	[High, Medium, Low]

#### 6.3.1.2 Secondary Model prior indicators

A list of the prior indicators is shown in Table 6-11 with the selected type and their values. The indicators represent the influences that enable criminals to perform both planned and unplanned activities in the business system. These prior indicators are the opportunities that expose businesses to threats and compromise security vulnerabilities. The prior indicators are the motivation and opportunity to compromise the system. This systemic compromise can expose the level of the employee, skills and job

description, the availability of cybersecurity training, and employee capability. It becomes a threat that determines the exploitation of the system and exposes employee attitude. The indicator variables are ranked with values high, medium and low, yes or no, technical, general and administrative, committed and not committed.

**Table 6-11: Secondary prior indicator nodes and values**

<b>Prior indicators</b>	<b>Prior indicators</b>	<b>Selected type</b>	<b>Values</b>
	Motivation	Ranked	[High, Medium, Low]
	Employee skills	Boolean	[True, False]
	Training availability	Boolean	[True, False]
	Capabilities	Ranked	[High, Medium, Low]
	Job description	Labelled	[Technical, General, Admin]
	Employee attitude	Ranked	[Not committed, committed]
	Economical	Boolean	[True, False]
	Client trust	Boolean	[True, False]
	Growth	Boolean	[True, False]
	System	Boolean	[True, False]
	Business System	Ranked	[High, Medium, Low]
	Current system	Labelled	[Good, Bad]
	Competitive	Boolean	[True, False]
	Opportunity	Ranked	[High, Medium, Low]
	Threat level	Ranked	[High, Medium, Low]

### 6.3.1.3 Secondary Model measures

Table 6-12 shows the Secondary Model measures: adherence, compliance, up-to-date software, protection level, physical measures, encryption, and instructional measures (policies). Adherence and the protection level are ranked high, medium, and low, while the rest of the measures have Boolean values, true and false. Adherence and compliance focus on applying the given guidelines thoroughly, standards, rules, policies and procedures that govern the protection and use of business resources. The protection level is the business's overall security at all levels, while the physical measures present the safety of the hardware resources. Physical measures cover the environment's safety and security, where the computers and the business assets are hardware-related. Encryption protects and secures business systems by encoding digital data using the password as a key and mathematical techniques to decrypt information. Lastly, instructional measures present the policies, procedures, rules, standards, and guidelines that guide and govern the use of business resources.

**Table 6-12: Secondary measure nodes and values**

Measures	Nodes	Selected type	Values
	Adherence	Ranked	[High, Medium, Low]
	Compliance	Boolean	[True, False]
	Up-to-date software	Boolean	[True, False]
	Physical measures (End devices)	Boolean	[True, False]
	Protection level	Ranked	[High, Medium, Low]
	Encryption	Boolean	[True, False]
	Instructional measures (policies)	Boolean	[True, False]

### 6.3.1.4 Discussion of the Secondary Model

Owing to the growing demand for the Internet for business growth and visibility, the small business sector faces various threats and attacks that compromise information safety and security. According to Figure 6-36, some attacks result from insiders and outsiders. The Secondary Model in Figure 6-36 extends the Generic Model presented in Figure 6-35. The Secondary Model has added more variables, illustrating the ultimate loss of information from the business systems. Even though there are dependent variables, prior indicator variables are influenced by the actions in the business system. For example, the motivation variable is influenced by economic growth, client trust, business growth, and competitive factors, which motivate the decreased safety and security of the business.

Even though there are other factors, such as employee attitudes, the business system state, or employee skills, the model reveals the importance of awareness and training as essential elements that help to improve the business system (Ncubukezi, Mwansa & Rocaries, 2020b). Employee attitudes could result from human errors owing mostly to ignorance and lack of skills, which determines the level of skill and awareness. The insiders are the employees from various departments in the business sector. The outsiders are cybercriminals who perform the planned attacks, which increase the threat levels based on the opportunities from the insecure systems. Systems can be less secure owing to poor adherence, lack of compliance, and user awareness of programmes and awareness training.

The ultimate cyberattack increases the threat level, which exposes the business systems owing to the lack of or minimal implementation of security policies. This means a lack of detailed documents with security guidelines, procedures, rules, and standards has an effect on the systems' safety, privacy, and security. For every business, there should be involvement of the management team that will enforce the use of regularly reviewed guidelines. The threat level increases when the protection level gets compromised, when there is no device or physical protection, the software is outdated, and encrypted digital data are not used.



The following section presents the Beta Model, which results from the designed Generic and Secondary Models.

## 6.4 BETA MODEL AND ITS STRUCTURE

The Beta Model is the development and extension of the Generic and the Secondary Models based on the security expected from the industry. The interviewed cybersecurity experts suggest the variables used in the model. These variables are connected to produce the ultimate results. The elements of the model illustrated in Figure 6-37 are clearly described in the following section.

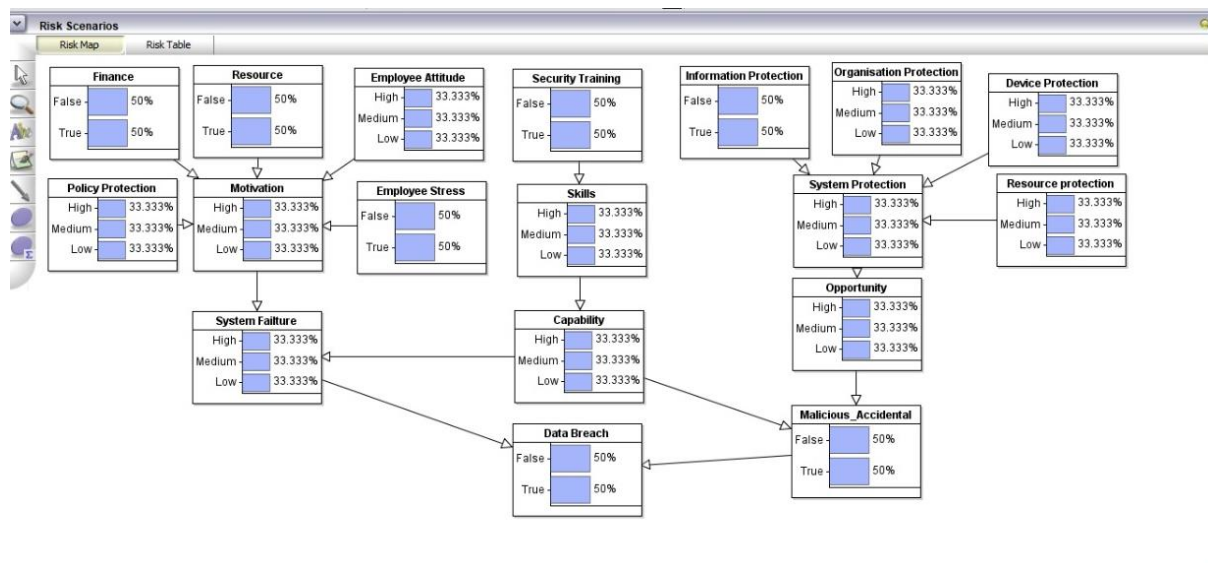


Figure 6-37: Beta Model

### 6.4.1 Elements of the Beta model

The variables used in the Beta model are divided into the basic nodes, prior indicators, and the measures discussed below.

#### 6.4.1.1 Beta Model different nodes

The Beta Model's basic nodes are the data breach, malicious attacks, system failure, and capability failure, as shown in Figure 6-38 and illustrated in Table 6-13. The nodes have different variables that use Boolean values (true and false) and ranking (high, medium, and low). The primary problematic variable is the data breach resulting from the system failure (because of the minimal implementation of the organisation's security measures for its assets) and the malicious attacks, which are unplanned attacks from employees and criminals.

**Table 6-13: Beta Model basic nodes and their values**

Main nodes	Node	Selected type	Values
	Data breach	Boolean	[True, False]
	Malicious attacks	Boolean	[True, False]
	System failure	Ranked	[High, Medium, Low]

**6.4.1.2 Beta model prior indicators**

Table 6-14 shows the prior indicators of the Beta Model with their selected types and values. These measures include employee skills, risk opportunity, capability, attitude, motivation, finance, employee stress, and available resources. Employee attitude and motivation are ranked high, medium, and low, while the rest of the measures are valued as the Boolean variables, true and false. The skills present the computer literate, cybersecurity skills, and user awareness when on the business system. An opportunity for a threat or a risk is based on implementing safety measures to secure and strengthen the system. If a business system is not secured, then the system will be vulnerable to threats. The capability variable is influenced by the employee's skills and security awareness level. Employees with minimal knowledge could expose the business to various threats through ignorance, human errors, lack of technical skills, and employee-related stress.

Furthermore, some knowledgeable employees could risk the system as they can intentionally exploit it for personal gain. At the time, the employees become the weakest link in the system (Ncubukezi, 2022a). Employee attitude can be determined by the level of stress employees have and the individual employee's behaviour. Employee stress could be related to understaffing and lack of skills resulting in negligence when working on the system. The motivation variable in the model is influenced by the availability of resources, finance, and employee attitude. Both insiders and outsiders have equal means to expose the business system, which violates the system's privacy, integrity, and confidentiality. Most criminals are after lucrative benefits such as financial gain, information, and resource availability. Business resources become exposed to cyberrisks when they are not properly secured.

**Table 6-14: Beta model priority indicators**

Prior Indicators	Node	Selected type	Values
	Opportunity	Ranked	[High, Medium, Low]
	Capability	Ranked	[High, Medium, Low]
	Skills	Boolean	[True, False]
	Employee attitude	Ranked	[High, Medium, Low]
	Motivation	Ranked	[High, Medium, Low]
	Finance	Boolean	[True, False]
	Employee stress	Boolean	[True, False]
	Resource	Boolean	[True, False]

### 6.4.1.3 Beta Model measures

According to Table 6-15, the Beta Model measures the variables that influence and promote security in the business sector. These measures are information security, organisational security, device security, system, and resource protection. Every business should protect its data and information from unauthorised access, modification, deletion, and data loss. When information security is compromised, it affects the security principles such as confidentiality, integrity, and authentication (Ncubukezi, 2022b). Organisational security includes all the safety and security aspects that strengthen the business, people, and resources. So this factor requires strong management that will strengthen, enforce and review the organisational standards, including the rules, procedures, and policies that guide the use of every resource in the business system (Ncubukezi, Mwansa & Rocaries, 2020b). In addition, management should always educate its employees about the safety and security of the business assets, which includes the employees themselves. The increased demand for the Internet in the business space has quantified the crimes and requires proactive measures to reduce risks.

With the increased demand to use gadgets, it becomes essential for businesses to strengthen their level of security of the devices, both portable and standalone. The devices present the primary need and recipient for businesses which should use all possible measures protecting them against unauthorised access and loss of the device. Similarly, the entire system should be protected, including the network, folders, and files to which employees have access. Equally, the same applies to access to the network resources, which requires protection, blocking incoming and outgoing traffic.

**Table 6-15: Beta Model measures**

Measures	Node	Selected type	Values
	Information security	Boolean	[True, False]
	Organisational security	Ranked	[High, Medium, Low]
	Device security	Ranked	[High, Medium, Low]
	System protection	Ranked	[High, Medium, Low]
	Resource protection	Boolean	[High, Medium, Low]

### 6.4.1.4 Discussion of the Beta Model

The Beta Model extends the Secondary Model, which illustrates the risks and motivating factors initiated by insiders and outsiders in the business system. The model showed the basic nodes, prior indicators, and the connected measures to achieve an outcome. Even though the risk can be positive and negative, the model demonstrated the likelihood of the positive and negative risks as well as the risk likelihood resulting from the mediating factors in the business system.

## **6.5 ALPHA MODEL**

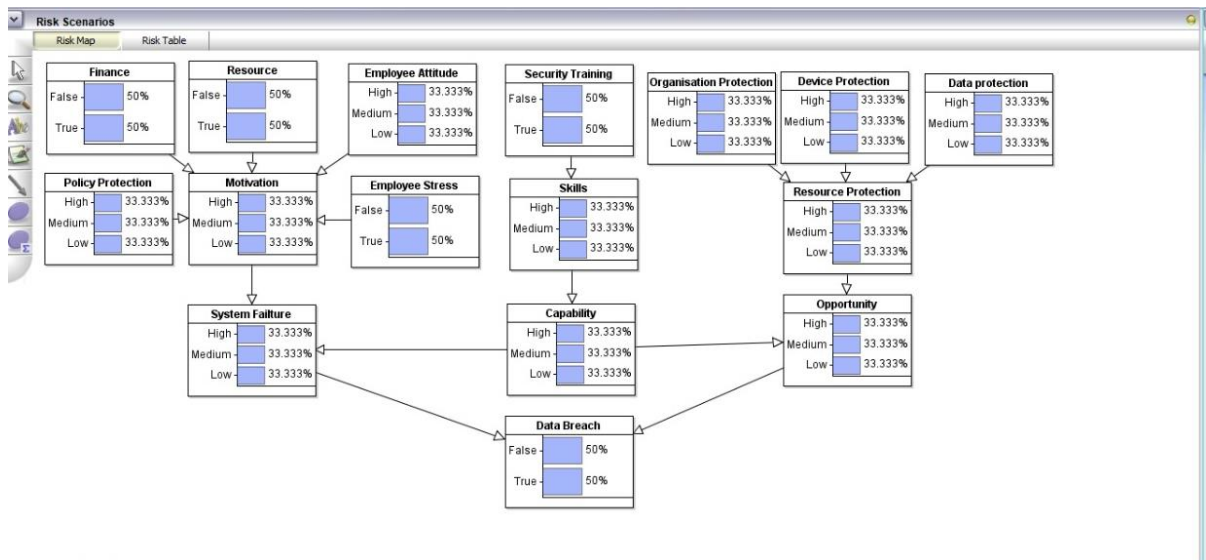
SMEs have become the main target for common data breaches (Richardson et al., 2019). The Alpha Model is the extension of the conceptual models, which consists of different nodes, prior indicators, and measures. This model has the Conditional Probability Table (CPT) of the nodes linked to form a Bayesian Network. These nodes are connected to demonstrate cyberrisk probability in the SME sector.

Some of these nodes are based on the information presented in the basic and secondary models. The first leg of the model contains finance, resources, and employees. These business departments have been selected as the business's most critical and vulnerable departments. These departments motivate the actions performed on the system based on clear business policies, rules, and guidelines that govern and guide the usage of the business resources. Negative actions carried out on the system result in the entire system's failure. In addition, human errors in the systems can be caused by the level of employee stress when working on the system. However, the model has been simplified to three states which are rated low, medium, and high, which will help perform the calculations.

The second leg focuses on the availability of cybersecurity training and awareness in the business sector. Security training and awareness improve the security of the business assets, including employees. The increased level of understanding reduces the risk probabilities. In contrast, the minimum efforts or absence of security training in the SME sector increases the probability of risks, resulting in data breaches. Similarly, the number of employee skills determines the employee capability for the activities that can be performed on the system. Consequently, the employee capability can either lead to the system failure or to the opportunity that motivates a data breach. The opportunity presents the amount of vulnerability based on the presence or absence of organisational security, device security or data protection, which all protect the business resources and reduce opportunities for risk.

### **6.5.1.1 Alpha structure**

This structure comprises various nodes, prior indicators, and the measures presenting the dependent and independent variables, which connect to illustrate risk probability resulting in data loss. The Alpha Model in Figure 6-38 presents three legs that ultimately connect to form a successful data breach. These different legs are explained below and divided according to the nodes, prior indicators, and measures.



**Figure 6-38: Alpha Model**

The different nodes used in the model are presented below.

### 6.5.1.2 Alpha-model different nodes

The basic nodes for this model are system failure, opportunities, capability, and data breach, as shown in Table 6-16 to inform the model's ultimate goal. The variables use the Boolean values (true and false) and the ranking (high, medium, and low). The primary problematic variable is the data breach resulting from the opportunities (because of the minimal security of the organisation and its assets), employee capability, and system failure.

**Table 6-16: Alpha basic nodes and their values**

	Node	Selected type	Values
<b>Main nodes</b>	Data breach	Boolean	[True, False]
	Opportunity	Ranked	[High, Medium, Low]
	Capability	Ranked	[High, Medium, Low]
	System failure	Ranked	[High, Medium, Low]

### 6.5.1.3 Alpha Model prior indicators

The prior indicators represent the actions taken by criminals and employees to breach the system, while prior indicators are the opportunities resulting from the system security loopholes. Table 6-17 shows that initial indicators are the motivation or opportunity to compromise the system, which creates the threat level. The threat level determines the amount of exploitation of the system. These variables are motivation, security training, system failure, skills, finance, resources, employee attitude, and employee stress. These variables are ranked with values from high, medium to low. Some of these variables are Boolean values, true and false.

**Table 6-17: Alpha Model prior indicator nodes and values**

<b>Prior indicators</b>	<b>Prior indicators</b>	<b>Selected type</b>	<b>Values</b>
	Motivation	Ranked	[High, Medium, Low]
	Security training	Ranked	[High, Medium, Low]
	System failure	Ranked	[High, Medium, Low]
	Skills	Ranked	[High, Medium, Low]
	Employee attitude	Boolean	[True, False]
	Employee stress	Boolean	[True, False]
	Resources	Boolean	[True, False]
	Finance	Boolean	[True, False]
	Threat level	Ranked	[High, Medium, Low]

#### **6.5.1.4 Alpha Model measures**

As shown in Table 4-18, the Alpha Model measures are organisational such as the device, data, policies, and resource protection. All these variables are ranked high, medium, and low.

**Table 4-18: Alpha-model measures**

<b>Measures</b>	<b>Prior indicators</b>	<b>Selected type</b>	<b>Values</b>
	Organisational protection	Ranked	[High, Medium, Low]
	Device protection	Ranked	[High, Medium, Low]
	Policy protection	Ranked	[High, Medium, Low]
	Resource protection	Ranked	[High, Medium, Low]
	Data protection	Ranked	[High, Medium, Low]

#### **6.5.1.5 Discussion of the Alpha Model**

The quantification of cyberattacks owing to the rapid use of the Internet requires the intervention of AI (Artificial Intelligence) that performs beyond what the human mind can do. The final Alpha Model illustrates the different variables, basic nodes, and the measures connected to show the risk probability of the ultimate data breach. The model illustrates the importance of security measures in businesses. Organisations should have a detailed living document like a policy that guides the use of the business resources and protects the employees. The absence of these business guides leads to a failing business and quantified risks. Likewise, the organisation should have a person responsible for implementing, enforcing, and reviewing to constantly improve the business security of the assets, resources, and personnel.

Businesses should also pay serious attention to device protection to avoid risks. The end devices present the primary assets used to store and retrieve information. Therefore, every device needs to be captured on the asset register with a unique code and have some form of security that will guard and protect against unauthorised access, usage and theft. The safety of the devices should also protect valuable data and stored information. Some devices may be standalone, while other devices may be networked. In the cases where devices are standalone, they might be vulnerable to cyberrisks through the use of

external devices for information exchange and sharing. In addition, when a device with inadequate security measures is stolen, the perpetrators can have full access to the sensitive and private information stored on the devices, resulting in a major data breach.

On the other hand, networked devices are likely to be exposed to a range of cyberrisks owing to the inadequate implementation of security measures at the device level. For example, the device can be exposed and become vulnerable to viruses, spyware, and other security breaches. A resource presents the networking device that enables the business system's service. A failure to secure a resource exposes the resources and other devices connected to that resource. So it becomes essential for every business resource to be protected to ensure the safety of the transactions, information, and services.

## **6.6 DEVELOPMENT OF THE SIMULATED RISK CASES**

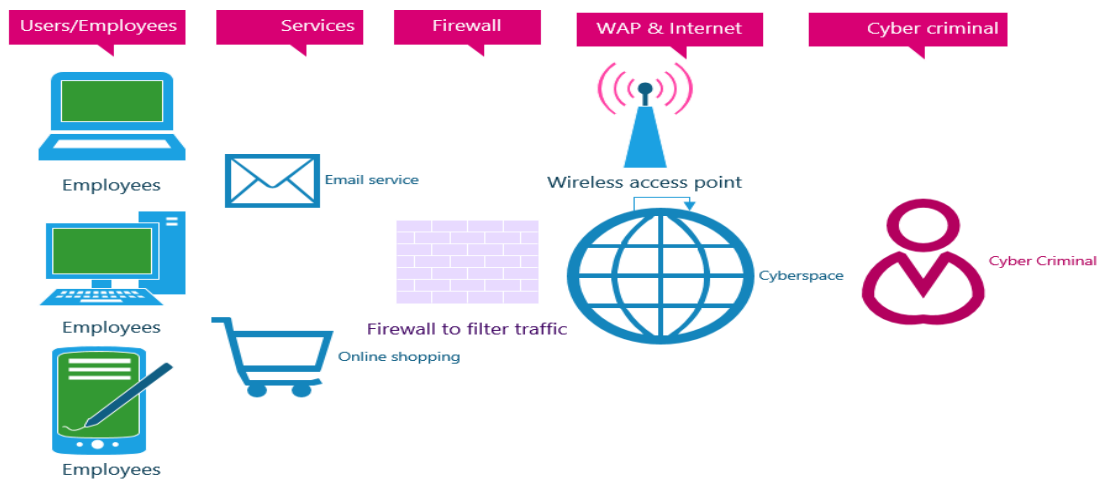
The simulated risk scenarios are based on the collected data for five common cyberrisks. The data used was collected from the participants and analysed using the scenario analysis. The analysis method focuses on predicting the probability of the risk occurring or the risk consequences (Kishita et al., 2016). It also helped to explore future trends in a specific period. One of the key stages when using scenario analysis is to identify the future trends, uncertainties, and the key factors that disturb the main plan. The last objective of this study focuses on the use AgenaRisk package to determine the risk likelihood of various cyberrisks to which the SMEs are exposed. The collected data was used to develop the knowledge base for five common cyber-attacks.

Using the Bayesian network technique, these simulated scenarios are presented in a graphical form, analysed, and connected on the AgenaRisk package. Each cyberrisk case provides a background scenario of the risk likelihood and its impact. Each case illustrates the variables used, connections of the variables, and prior and posterior indicators (risk likelihood and effect). The simulated risk scenarios used in this study are based on real-life cases of SMEs facing uncertainties in their future business operations, especially after the Covid-19 Pandemic. This technique is applied to guide risk mitigation for any possible risks and bring insights to future cases.

### **6.6.1 CYBERSPACE AND ITS SECURITY**

Owing to the global lockdown as a result of the Covid-19 pandemic, people and institutions working at home under the 'new normal' and businesses used cyberspace to perform their daily activities. Ideally, cyberspace offers benefits to all its users. The openness of the convenient use of cyberspace grants equal access to intrusion of persistent cybercriminals. Therefore, the effective use of cyberspace requires proper cybersecurity for all transactions. Cybersecurity is a multidimensional aspect of the business involving cyberspace, information security, personnel, and cybersecurity, which forces organisations to

protect all the aspects that promote and protect assets. The protection of cyberspace necessitates businesses to identify and protect it.



**Figure 6-39: User processes during information processing (Source: Ncubekezi, 2021b)**

Even though businesses perform different activities, they all use the same technological platform (cyberspace), making it an integral part of the business. Figure 6-39 illustrates how users interact with systems interacting on the business system connected to cyberspace for information flow. These users access the service. The system can sometimes have an active or inactive firewall to filter incoming and outgoing traffic accessed by means of a connection to the Internet, while the perpetrator could be any cybercriminal awaiting a lucrative benefit. Depending on the safety of the business network, at times, employees receive error-free services when there are proactive safety measures coupled with active firewalls. The proactive implementation of the firewall and security measures increases the safety and privacy of the system to prevent the perpetrator from gaining unauthorised access to the system.

Cybercriminals always use every opportunity to sneak in and gain unauthorised access to private information when there is a loophole in the system or minimal security measures. The Internet and its openness sometimes result in major damage to the business system. Therefore, unsecured access to timely, convenient, and open cyberspace exposes and quantifies cyberattacks through user actions.

## 6.7 SIMULATED SCENARIOS ANALYSIS

Simulated scenarios describe the phenomena, create normative statements, and explore particular contexts through different lenses to reveal multiple facets (Rashid et al., 2019). In addition, these scenarios are appropriate when there is little or no control over events of the phenomenon, which has some real-life context. A research strategy is a detailed plan to answer the research questions and involves the objectives, existing knowledge of the phenomenon, available time and resources, and the underlying philosophical considerations (Wedawatta, Ingirige & Amaratunga, 2011). Remenyi et al. (2003) believe that a research strategy gives an overall direction of how the study will be done, including



its processes. So, to answer the research questions, each system works well in a particular type of research and involves various data-collection tools. This study used the qualitative simulated scenario as a strategy to answer the research questions and addresses the main objectives.

Simulated scenarios are an investigation of a particular phenomenon within its real-life context using different sources of evidence' (Robson, 1993: 146). The research purpose, objectives and questions are the primary influencers in selecting this strategy. In addition, this research strategy can be classified as exploratory, explanatory and descriptive. It also becomes possible for the research strategy to combine two categories. For example, one can use the exploratory and explanatory methods. While an illustrative purpose of the research analyses and the link between dependent and independent variables can be used to explain the relationships, the descriptive purpose analyses how the subject behaves. The research purpose, objectives, and questions of this study are exploratory and descriptive. For example, research objectives 1 and 2 are exploratory, while objective three is descriptive.

This section focuses on developing scenario cases about common cyberrisks. In this research, scenario analysis helps to separate and identify the main trends (certainties or uncertainties) by looking at the trends that may not or may be significant or may not change. The action is essential because it avoids frustration and improves efficiency while saving time. This work presents scenarios of events, roles and relationships in small and medium-sized businesses in South Africa (SA), focusing on the cyber events that contribute to cyberincidents involving cyberattackers (cybercriminals and employee errors) and demonstrating their relationships.

### **6.7.1 Scenario analysis Setting**

These simulated scenarios are based on small and medium-sized businesses. Businesses use mainly technology to render services to clients. These businesses are from diverse business sectors, varying in years. The businesses have been selected in different provinces and are categorised as theoretical and empirical. The simulated scenarios examine how activities take place. A simulated scenario interprets and understands the context of cyberrisks to which the small business sector is exposed. Furthermore, the strategy describes, explores, and explains the main elements, features, meaning, and consequences in the scenario.

A practical simulated scenario allows the exploration of issues to understand natural settings and their complexities. This work presents simulated scenarios of small businesses that experience common cyberrisks. The study further evaluates the cause of cyberrisk, the likelihood of cyberrisk occurring, and its impact on businesses. Moreover, the Bayesian model with AgenaRisk was used to analyse various cyberrisks and their impact to recommend risk mitigation strategies. Five simulated scenarios are the sources of data breaches that pose a threat to small businesses. These cases concern end devices,

human errors, malware attacks, phishing attacks, and poor adherence to security policies, guidelines, or rules. Each case describes, explores, and explains various elements that result in risks that ultimately compromise information security. They demonstrate the relationships between dependent and independent elements, the likelihood of risk, protective measures taken, and the consequence of the risk. These simulated scenarios used qualitative interviews and surveys for data gathering.

### **6.7.2 Adoption of the AgenaRisk Package with Bayesian Network Tools**

Among other available and existing risk management tools, this study used the AgenaRisk because of its potential to create a user interface for the model (AgenaRisk, 2021). Therefore, this study used the AgenaRisk tool to design and develop a model for businesses. The tool demonstrates, analyses, and predicts cybersecurity risks in the business sector. In addition, the tool allowed predictive reasoning about unclear Bayesian networks and supported diagnostic analysis. Lastly, the validation phase used a business-simulated scenario to demonstrate risk indicators and security measures that inform the Beta model.

The Bayesian network predicts the probability of cyberrisks, resulting in loss of money and data breaches. The employees and criminals initiate these cyberrisks in the small business sector. The Bayesian network developed and demonstrated the structures using the AgenaRisk tool. A total of five scenarios are created to determine the risk likelihood that the small business sector can be exposed to base on the activities performed by legal or illegal users. Each case does not show the exact numbers precisely; instead, it shows the relative probabilities based on cyberrisk scenarios. Each case scenario illustrates the relationships between the variables and their influence on the level of the risk likelihood, which is equivalent to the risk impact.

The Bayesian Network (BN) technique determines the probability of risks based on the prior indicators, protection levels, risk likelihood, and the consequences of the risks. The conceptual model mainly guides the use of the BN in Section A in Chapter 1. The tool clearly illustrates the case study's important features: the prior indicators, protection measures, and the post indicators of the cyberrisk. Even though these case study models show some level of analysis, the models do not conduct any sensitivity analysis. Instead, the various demonstrations of the models for each case study is shown with different probabilities. Each case study has different risks, ultimately contributing to the risk impact. Creating the various case study models has been guided by the information received from the data collection and analysed using a thematic and qualitative risk assessment. The following sections present the case studies concerning end devices, human errors, malware attacks, phishing attacks, and poor adherence to the policies, rules, and guidelines.

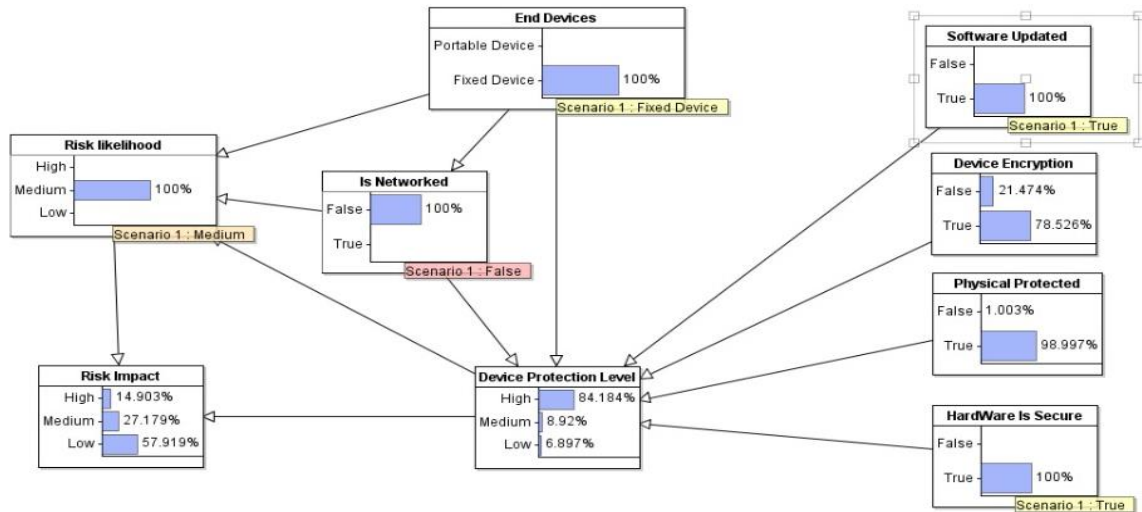
## **6.8 SIMULATED SCENARIO 1: OBSERVATION OF END DEVICES**

End devices are one of the main resources that promote activities by both legitimate users and criminals in the business space. With the increased demand to connect to cyberspace, most people and businesses use various end devices: smartphones, mobile devices, tablets, laptops, and computers (Imgraben, Engelbrecht, & Choo, 2014). The increased use of end devices introduces ways that compromise privacy, safety, and security in all organisations, requiring mitigation strategies and increased awareness. The literature shows that there is minimal understanding of users' safety practices on end devices in homes and business sectors (Tabassum, Kosinski & Lipford 2019). Employees ignorantly want to use their home devices at work that, establish unsecured connections, posing a risk, and compromising computer and information security.

Cyberattackers understand and pay close attention to the end devices as they become their primary targets for deploying malware attacks (Rusi & Lehto, 2017). Criminals can steal information of good value and money through infiltrating end devices. Likewise, these devices may not be connected to the business network but serve as standalone computers where employees share and exchange information using memory sticks. Regardless of the connection to the network, the end devices generally pose a risk because some end devices do not use proper security measures owing to the access of Bring Your Own Device (BYOD) (Ncubekezi, Mwansa & Rocaries, 2020b). Some end devices could experience a single point of failure where a device can crash or malfunction. Some could even display error messages that could freeze the device or automatically shut it down owing to corrupt software or faulty hardware.

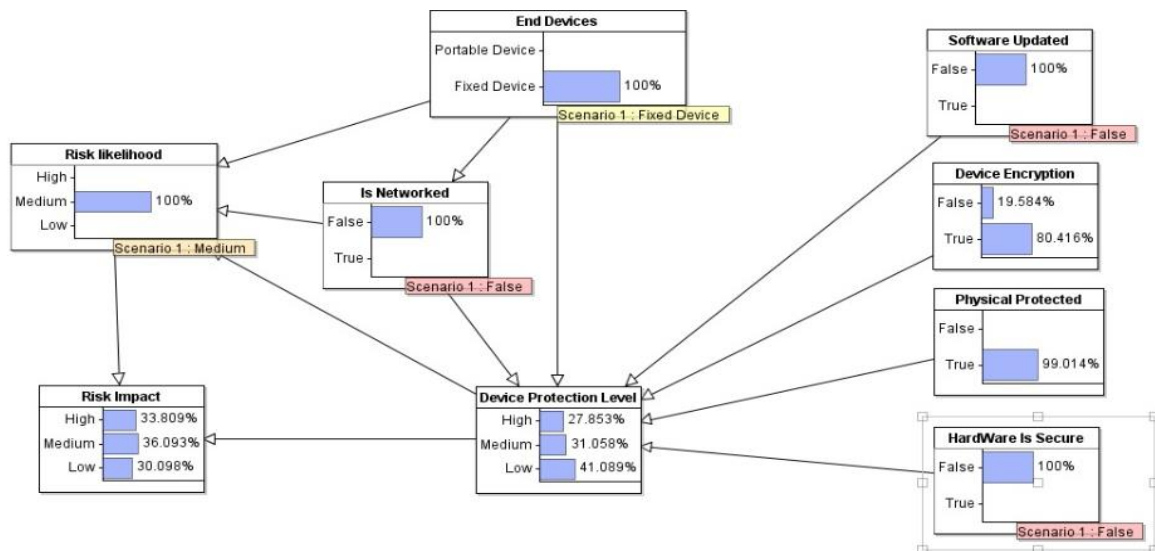
### **6.8.1 Analysis**

This case study focused on end devices. As explained in the section above, the case study is guided by the conceptual model in Section 1.5. The main variables of this case study are the prior indicators of the receiving end devices, protection level, and the posterior indicators, which influence the risk probability and consequence. As illustrated in Figure 6-40, the prior indicators are the end devices that could be either portable or fixed and connected to the network or act as standalone devices. The device's protection level is influenced by implementing the current security measures such as updated software (application and operating systems), device encryption, physical protection, and hardware security. In addition, complete device protection is also influenced by the nature of a device (networked or standalone). The level of device protection affects the posterior indicators to determine the risk likelihood as well as the impact. The higher the device protection, the lower the impact, even though the risk likelihood would be influenced by the device protection, portable or fixed device, which could be networked or standalone.



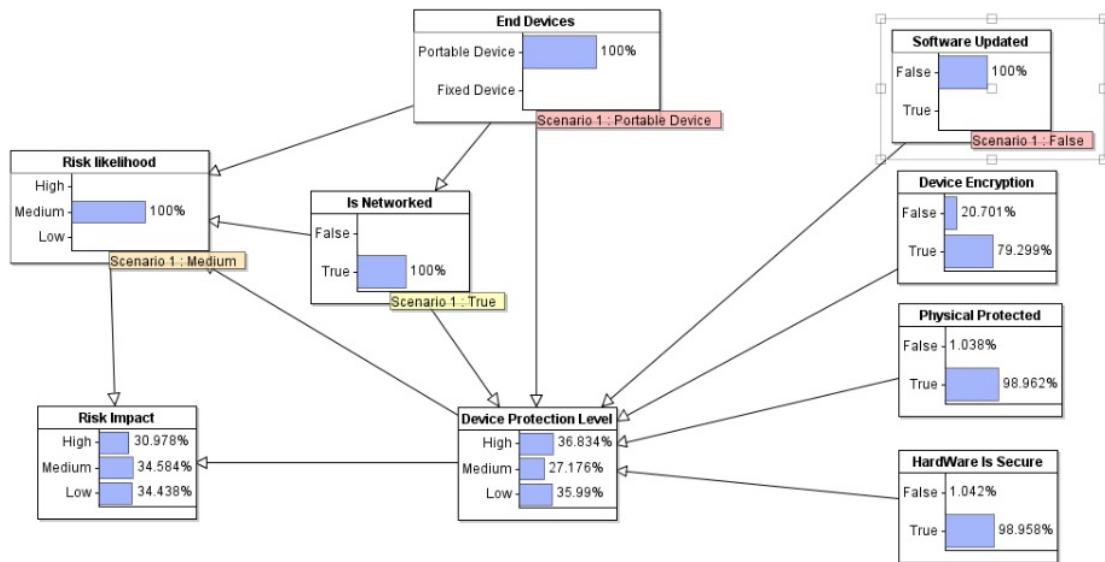
**Figure 6-40: Fixed standalone end devices with high protection level**

Figure 6-40 illustrates fixed and standalone devices with 84% high device-protection level based on 100% outdated software updates and 100% lack of hardware security. The device is in a secured physical environment with a 78% high level of encryption. Based on the overall device protection, this scenario had a medium-risk likelihood with 57% of the risk impact.



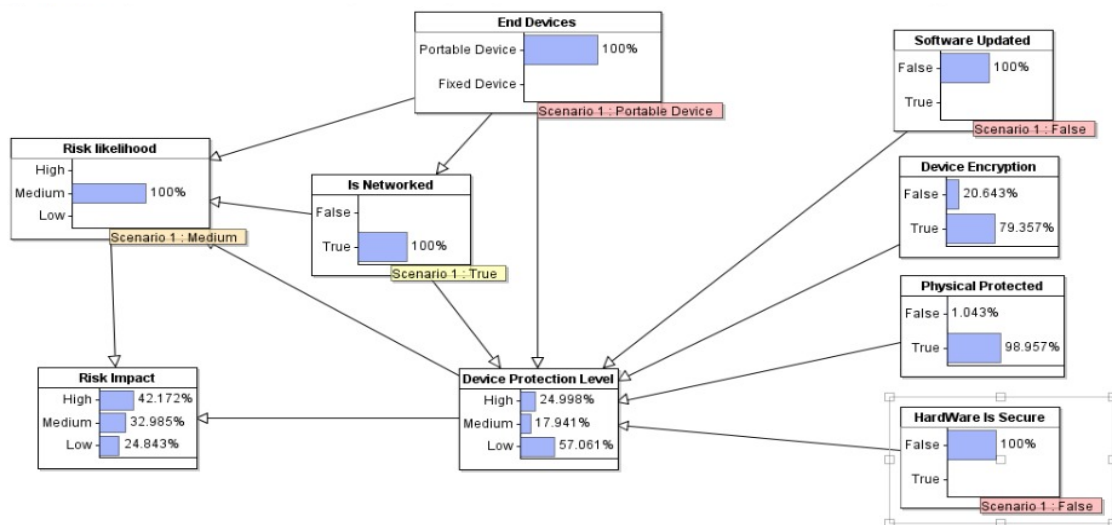
**Figure 6-41: Fixed standalone end devices with low H/W and S/W protection**

Figure 6-41 illustrates networked fixed-end devices with a 41% low device-protection level. This scenario has no software updates, 80% high device encryption, 99% physical safety, and 100% hardware security. Inconsistent device protection influences medium risk likelihood and 36% medium risk impact.



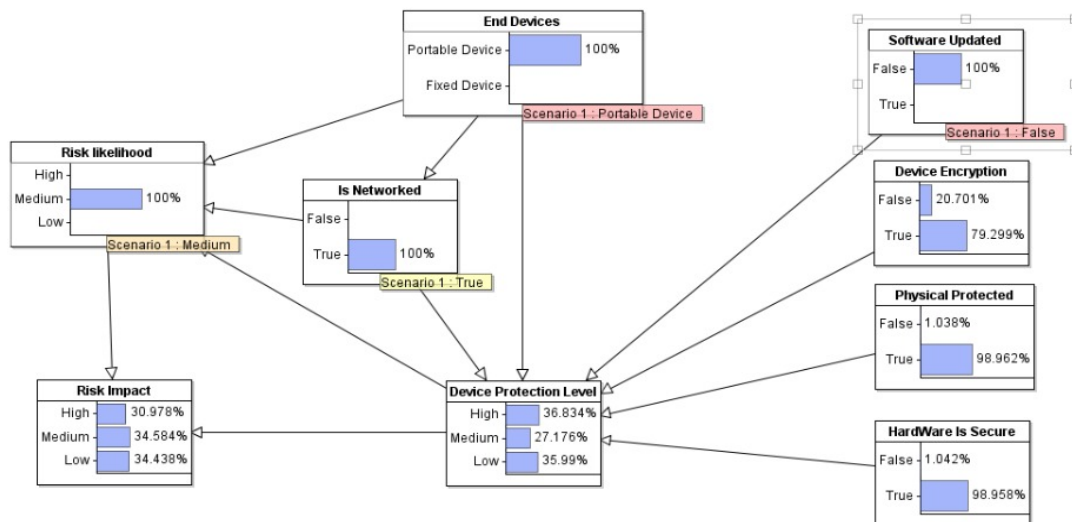
**Figure 6-42: Portable networked end devices with high device protection**

Figure 6-42 shows the portable networked end devices with high device protection levels owing to the physical space, hardware, and device encryption. The software becomes the only low influential factor for risk level. The range of the high mediating factors influences the device security's overall level, determining the risk likelihood and impact.



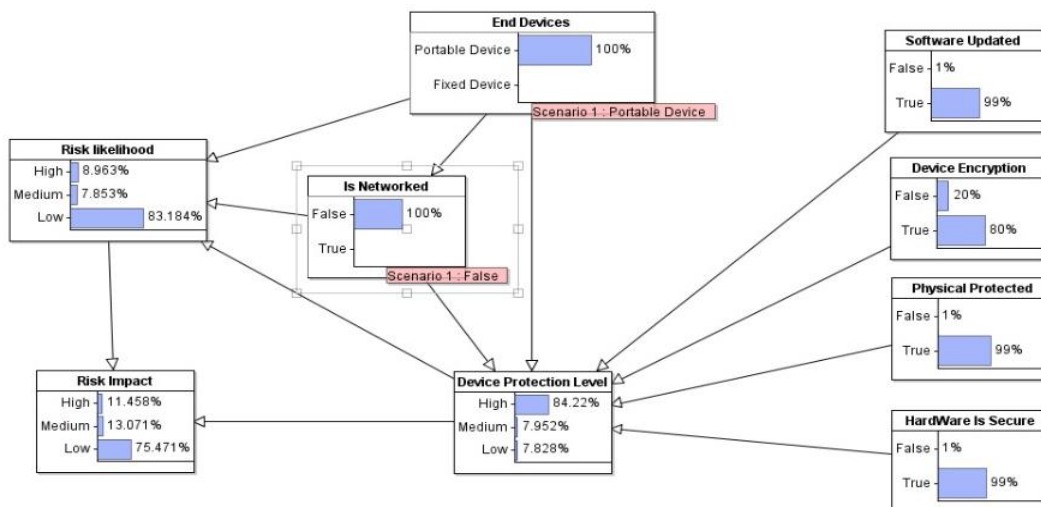
**Figure 6-43: Portable networked end devices with low hardware and software security**

Figure 6-43 demonstrates a networked portable end device with a 57% low protection level owing to no hardware and software updates, 98% dominating physical protection, and 79% device encryption. The dominating 57% low device protection level has a medium-risk probability and 42% high-risk impact.



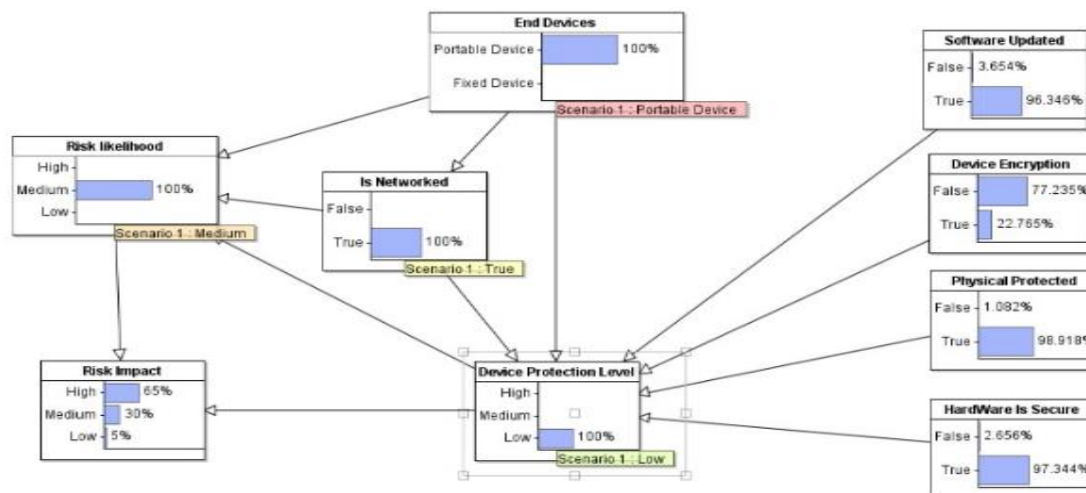
**Figure 6-44: Portable networked end devices with low software protection**

Figure 6-44 presents a networked portable end device scenario with medium-risk likelihood and 34% medium-risk impact. The 36% of device protection has influenced the results. In this scenario, the software is not regularly updated, only 79% of device encryption, 98% of physical safety of the buildings, and 98% of hardware security.



**Figure 6-45: Portable standalone end devices with high device protection**

In Figure 6-45, the portable standalone end devices with an 84% protection level resulted in an 83% low-risk likelihood and a 75% low-risk impact. Safety measures are 99% software updates, 99% hardware, and 80% physical security, resulting in 84% device protection.



**Figure 6-46: Portable networked end devices with low device protection level**

Figure 6-46 shows a 100% low device protection level due to 96% software updates, 22% device encryption, 98% physical protection, and 97% hardware protection. All the variables, in this case, contribute to the overall cyberrisk likelihood and impact medium-risk likelihood results and 5% low-risk impact for a portable networked device.

### 6.8.2 Discussions and Recommendations

Risk is determined by the risk likelihood and impact. This study used the BN's technique to illustrate the probability of the risk relating to the end devices. The study referred to various end devices with different capabilities. The end device simulated case scenario revealed different outcomes of the risk probability and impact, informed by enabling and mediating factors. The diverse contributing factors showed the varying probability of the risk related to the end devices. The minimal implementation of security measures exposes the receiving end devices to a range of cyberthreats (Ncubekezi, Mwansa & Rocaries, 2020b).

Even though some end devices may be fixed and not connected to the network, the device's protection level continues to influence the risk level and its impact. The physical security of the devices may not reduce the risk probability of the device if the hardware, software, and encryption are ignored. The guarantee of the end devices should be applied at all levels (hardware, physical, software, and encryption) (Ncubekezi & Mwansa, 2021a). If the device's security is prioritised for the hardware, software, physical, and encryption level, the level of risk to the device will be low, resulting in a low-risk impact. There is a wide range of security remedies and measures; using and implementing firewalls, and intrusion detection systems (IDS) would be beneficial to securing and protecting the business's assets.

Adequate security measures promote good cyber hygiene. With the high rate of risk uncertainties, it would be beneficial for the small business sector to deploy protective measures at all levels of end devices.

## 6.9 SIMULATED SCENARIO 2: OBSERVATIONS OF THE HUMAN ERRORS

Among the increased cybercrimes at SMEs, human errors are influenced by different attitudes and behaviours. Human errors could be unplanned but result from poor decision-making, employee ignorance, lack of skills, and poor compliance with the active cybersecurity guidelines. Employee mistakes put businesses at risk, while the SME sector pays little attention (Ergen, Ünal & Saygili, 2021). Often, criminals gain unauthorised access owing to employee work overload and other related factors. The challenge is the diverse range of human errors, which open doors to unauthorised access to people who steal sensitive information and other valuable assets. This action results in a significant data and security breach (Richardson et al., 2020). For example, criminals take advantage of the unsure network sessions by violating safe surfing and privacy (Wallace et al., 2020).

Figure 6-47 illustrates employees who are interacting with the system. However, their actions toward the system create opportunities for cybercriminals to gain access by hijacking unprotected sessions (Ncubukezi & Mwansa, 2021b). Unfortunately, the openness of the Internet and ignorant actions expose private, sensitive, confidential, and valuable business information and resources. Several threats are the result of human errors. Some threats are harmful malware such as viruses, phishing, Trojan, adware, spyware, and worms (Karaci, Akyüz, & Bilgici, 2017). The software automatically gets installed without the user's knowledge when a victim ignorantly clicks on harmful links or uses automatic pop-up messages. The promoters of human errors are ignorant users, which cause poor decision-making, and show a lack of skills, and minimal knowledge about information and computer security, leading to poor implementation and not adhering to security guidelines.

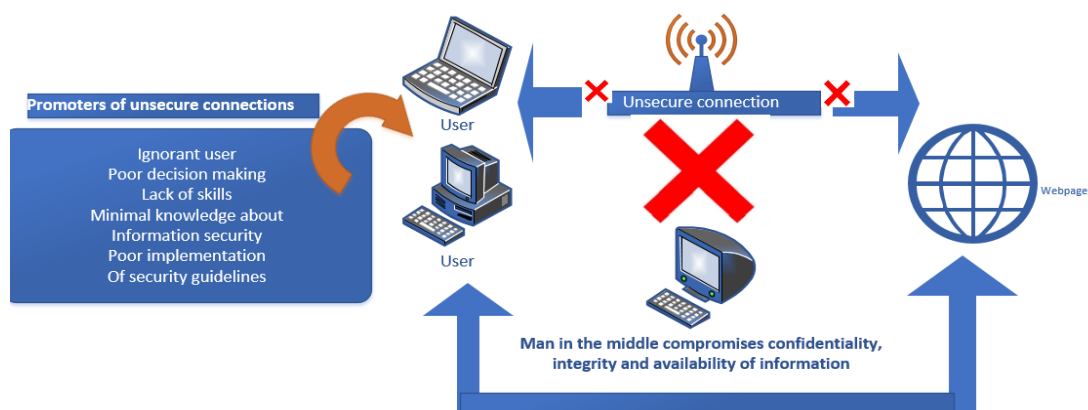


Figure 6-47: Human errors in the business system (Source: Ncubukezi and Mwansa, 2021b)



As shown in Figure 6-47, a data breach becomes the ultimate result because, in the process, information gets modified, deleted, or eventually lost. The simulation of the human error scenario results based on the planned and unplanned events is presented.

### 6.9.1 Results

This section illustrates the simulated scenario for human errors. The human error scenario presented two system users: a normal user and an experienced IT user. As used in this study, the normal user presents as an employee who is not well trained and informed to use the system, while an IT user is skilled and well-orientated towards cybersecurity best practices. However, both users can experience planned or unplanned attacks based on their actions, attitudes, and behaviours on the system. A planned attack presents a criminal looking for opportunities to gain unauthorised access to unsecured systems. AgenaRisk is used to determine the risk likelihood of human errors based on different scenarios influenced by human activities and the state of security (system's protection level). The risk probability influences the risk impact. This scenario is presented owing to the high demand for Internet use and working off-site during the global pandemic, where data became the leading lucrative benefit in all organisations. Criminals always have the intention of gaining unauthorised access. Employees are sometimes the link for data breaches by committing unplanned actions compromising the security of the systems. In contrast, employee ignorance and poor decision-making influenced by work overload or lack of skills and awareness results in unplanned attacks. Employees could be general system users or skilled Information Technology (IT) users who interact with the system. Different scenario cases are presented below, demonstrating the risk probability of human errors. The graphical representation will indicate some detection levels from planned or unplanned events.

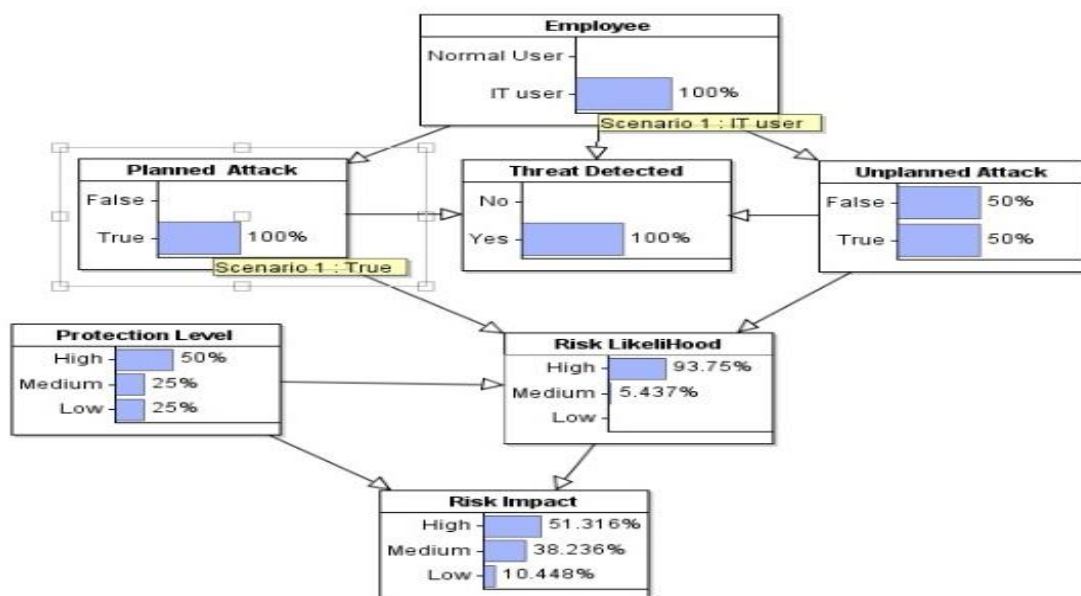


Figure 6-48: IT user experiences a partially unplanned and planned attack at a 50% protection level

Figure 6-48 shows a normal user who experienced partially planned and unplanned attacks, with 50% of the unplanned and 100% of the planned events, which means there is a 100% threat detected. Owing to the 50% of low protection, the risk probability is 93%, with 51% of risk impact.

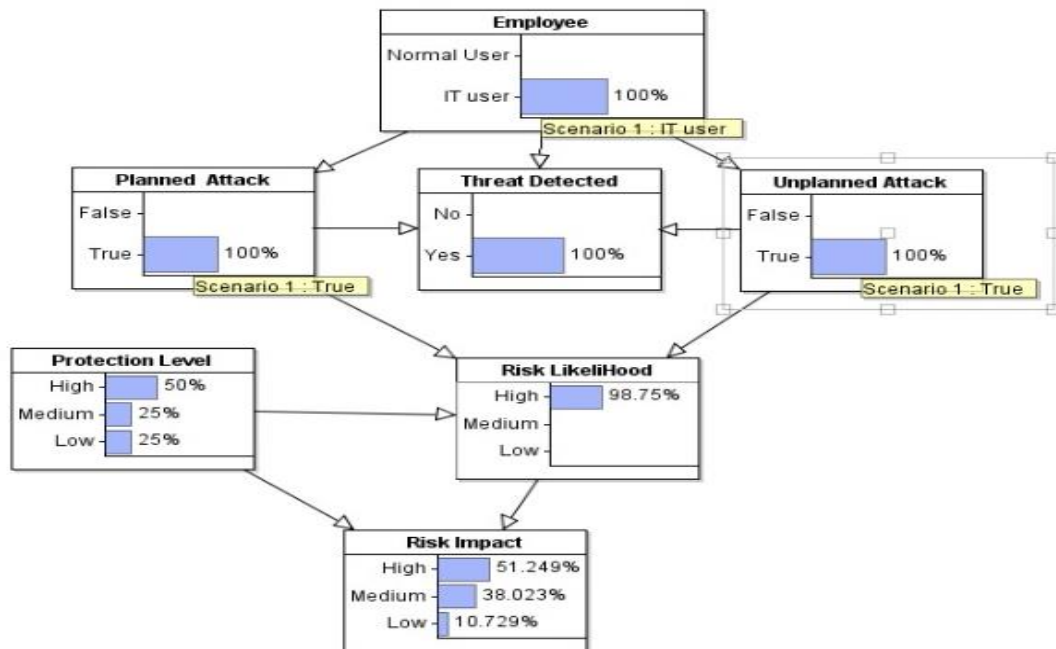


Figure 6-49: IT user experiences an unplanned attack at the 50% protection level

Figure 6-49 shows an average user who experienced a 100% unplanned attack with a planned attack at 100%, which means 100% of the threat. With a protection level of 50%, the scenario has a 98% risk likelihood, resulting in a 51% risk impact.

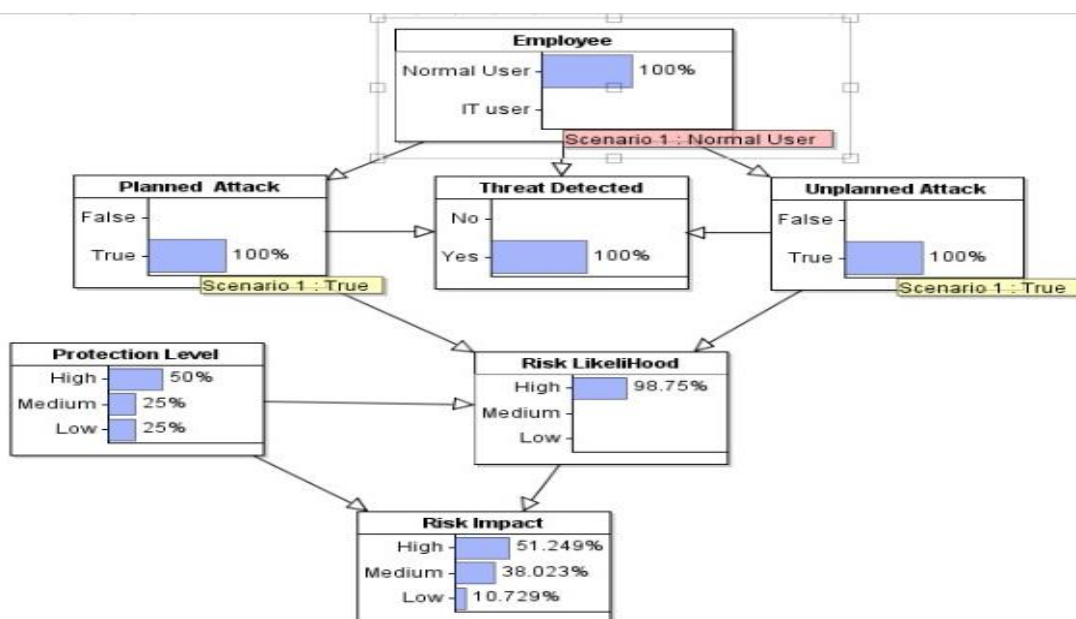


Figure 6-50: Normal user with planned and unplanned attacks as high risk likelihood

Figure 6-50 shows a normal user who experienced both planned and unplanned attacks. Those attacks happened at the 50% protection level, resulting in 98% risk likelihood and 51% risk impact.

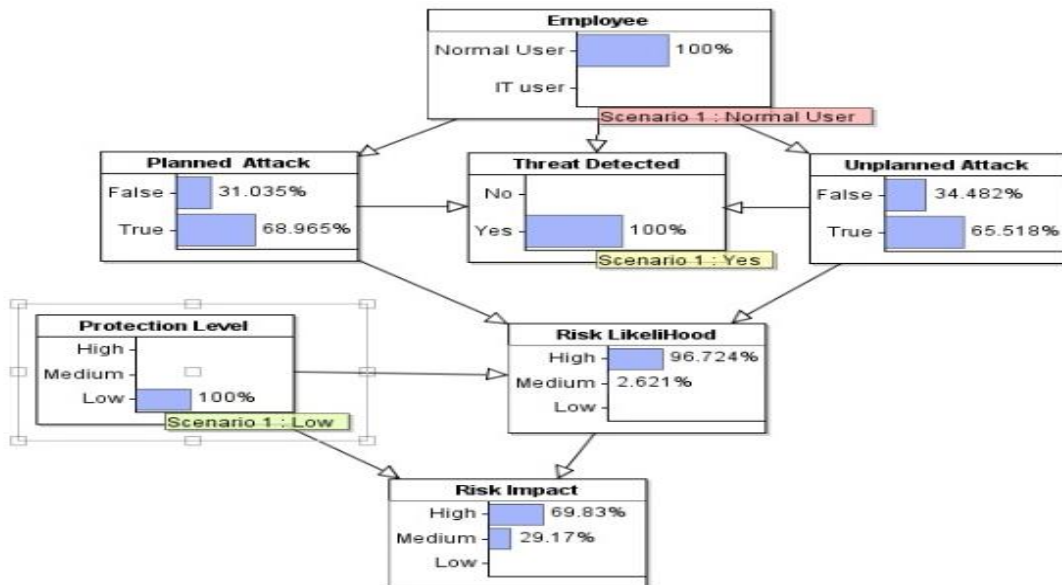


Figure 6-51: Normal users experience high and low attacks at a high protection level

Figure 6-51 shows a normal user with 68% planned and 65% unplanned attacks. The scenario shows a 100% low protection level, resulting in 96% of the risk likelihood and 69% of the risk impact.

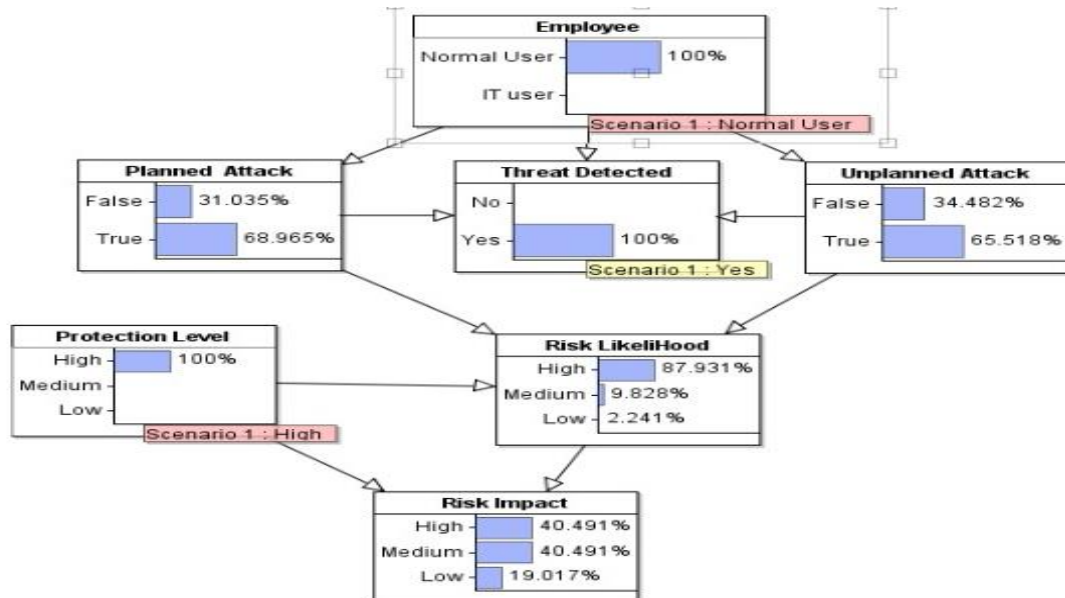


Figure 6-52: Combination of planned and unplanned attacks on normal user

Figure 6-52 shows a normal user with a threat detected in 68% of the planned attack and 65% of the unplanned attack at a high protected level, resulting in 87% of the risk likelihood and 40% of the medium and high-risk impact. The discussion and recommendations for the human error simulated case scenario are presented below.

## **6.9.2 Discussions and Recommendations**

Unfortunately, businesses can never grow without human intervention. The literature indicates that human errors are one of the attacks that are underestimated and ignored (Hadlington, 2017). The case scenario demonstrated that human factors could be the source of attacks compromising the system in one way or another. Some harmful human actions are caused by insiders, while intentional errors compromise the systems. Sometimes, human mistakes expose businesses to risks that significantly affect information and computer security (Anwar et al., 2016). Criminals take advantage of gaining unauthorised access to the system owing to insider action. Criminals usually take time to plan for their activities, while insiders react based on their attitudes, behaviour, and opportunities. The ignorant, pressured actions reveal valuable, sensitive information and other business resources to opportunistic cybercriminals.

Criminals hijack unsure sessions to violate privacy and security (Wallace et al., 2020). Minimal use of safety measures increases the chances of data breaches. Sometimes, human errors are caused by inadequate staff members, fatigue owing to work overload, and operating under pressure (Turk, 2013). Similarly, insiders create a loophole in the system when they have bad intentions. Understaffing in businesses creates human errors because some employees may be highly ignorant of their actions in the system. Some employees do not have adequate skills to help them make informed decisions. In this scenario, the risk probability is influenced by the presence and adherence to the available security policies, rules, procedures, and guidelines. The amount of risk likelihood influences the risk impact in the system.

The higher the risk probability, the greater the impact. As stated in the previous section, cybersecurity risk results in reduced profit, poor performance, loss of clientele, and a bad reputation, affecting overall business continuity (Ncubekezi, Mwansa & Rocaries, 2021). Turk (2013) states that employees can be the weakest link of the chain and a channel for criminal activities, as the criminals use every opportunity they have. A malware attack simulated scenario is presented below.

## **6.10 SIMULATED SCENARIO 3: OBSERVATIONS OF THE MALWARE ATTACK**

Malware attacks are severe and replicate threats that all institutions face. The rise of Internet usage exposes organisations to malware attacks (Ncubekezi, 2021). Malware is a severe attack that compromises the cyberhygiene of the devices, information, and network intentionally. The perpetrator often sends a message or email falsely presenting a legitimate source. An ignorant user would be deceived and click the email link, automatically installing the harmful malware. Sometimes, the victims would curiously and ignorantly open emails which automatically install the malware software when they are opened. Users sometimes open external websites with the installation package, which traps users with no knowledge of the tricks (Kobis, 2021). Malware attacks have become one of the most

common threats in all sectors. These attacks often find their way into systems where poor or inadequate security measures are implemented. The results of the malware attacks are presented below.

### 6.10.1 Results

This case concerns the range of malware attacks deployed on networked or standalone devices. Malware attacks take over the victim's control of the systems. Standalone devices could be infected by external devices connecting and transferring data from one device to another. In contrast, networked devices get infected through external links, access to less secure websites, or fraudulent emails. This section presents the simulated results of the possible malware attacks and their relationships as variables, the risk impact, and likelihood. The researcher presents four simulations that demonstrate different cases with different risk impacts and risk probability. The risk impact is influenced by the protection level and the risk likelihood, while the risk probability is influenced by the state of security of the computer and the protection level. The computer presents a standalone or networked tool to receive and send information on the business network. Any external hardware can expose a standalone device to various harmful malware.

In contrast, networked devices could be exposed to viruses, spyware, ransomware, Rootkits, and Trojans. As a result, security or protection should be applied to the hardware, network, and software to promote information safety. When the safety precaution is thoroughly applied and enforced at all levels of the business, the risk likelihood would be low, resulting in a low-risk impact. The different graphical representations of the malware attacks demonstrate different scenarios with different results.

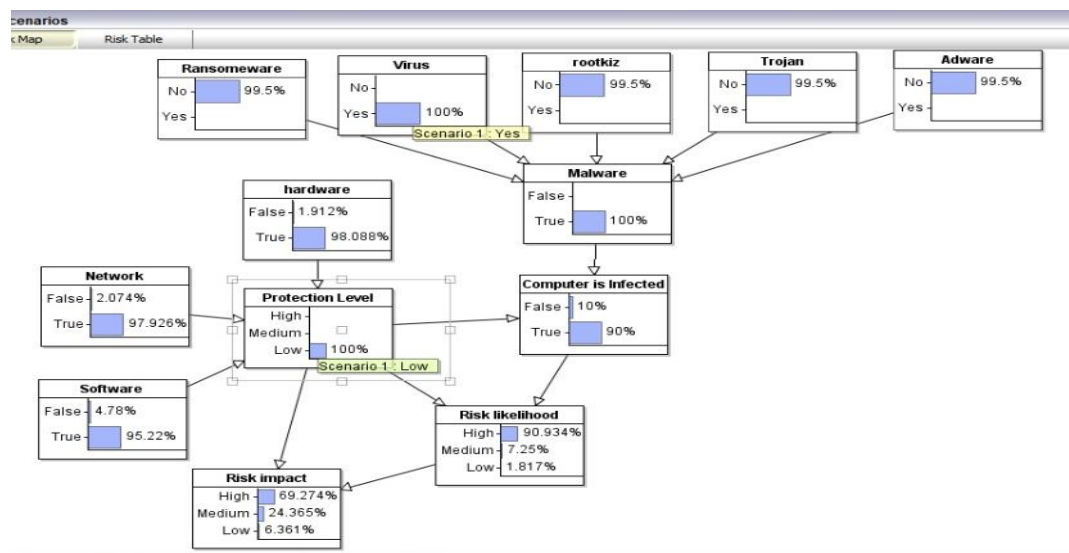


Figure 6-53: Low protection level of a computer with a virus

Figure 6-53 illustrates the presence of malware attacks caused by viruses. The networked device protection level is 100% low owing to 97% of unprotected networks, 95% unsafe software, and 98% vulnerable hardware resulting in a low protection level that influences 90% of the risk likelihood and 69% of the high-risk impact.

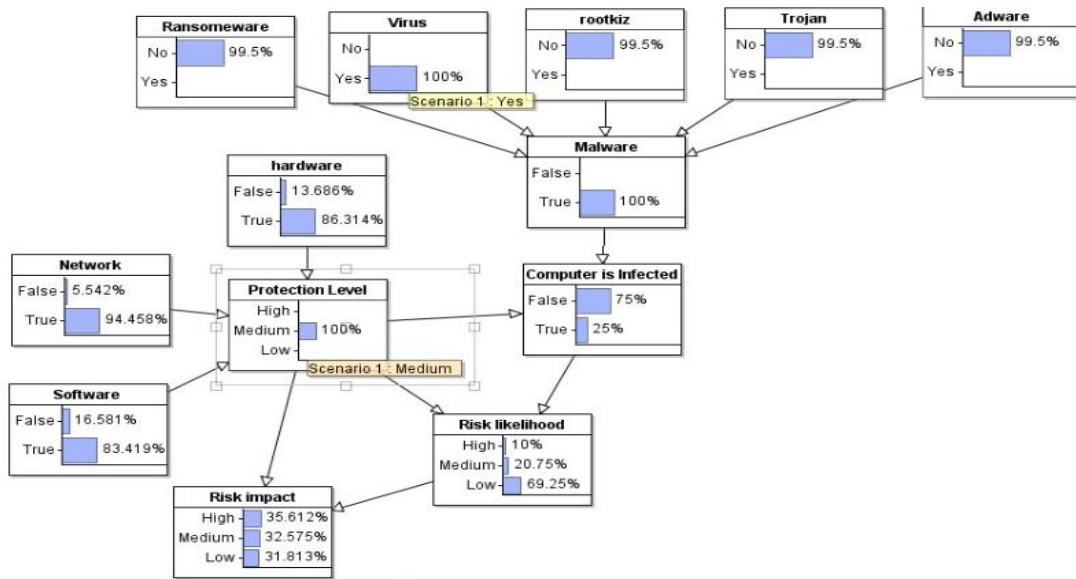


Figure 6-54: Malware at a medium protection level

Figure 6-54 revealed that malware was detected caused by the virus. The infection in the computer is 25% owing to the medium protection level caused by 86% of the hardware protection, 94% of the network protection and 83% of the software. The protection level results in 69% of the risk likelihood and 35% of the risk impact.

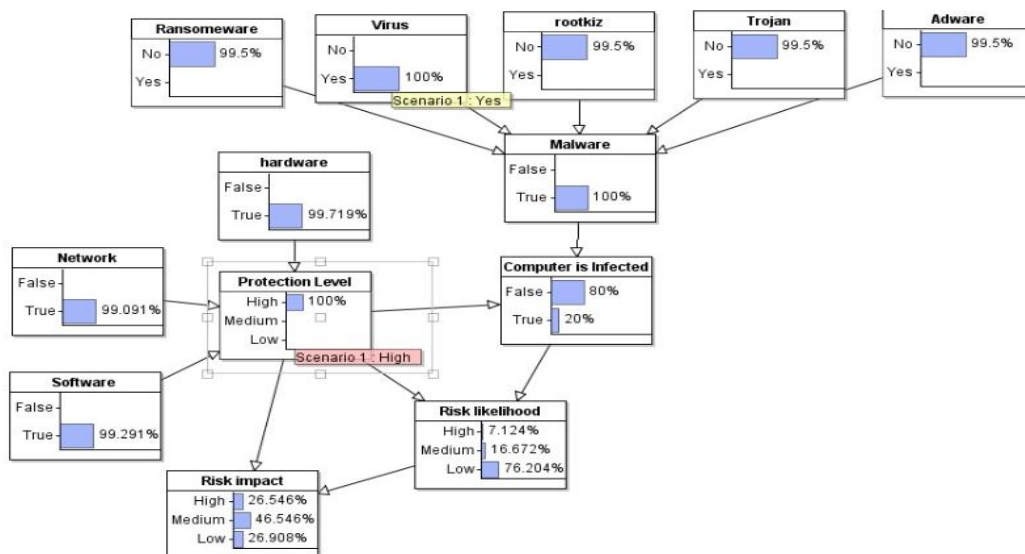
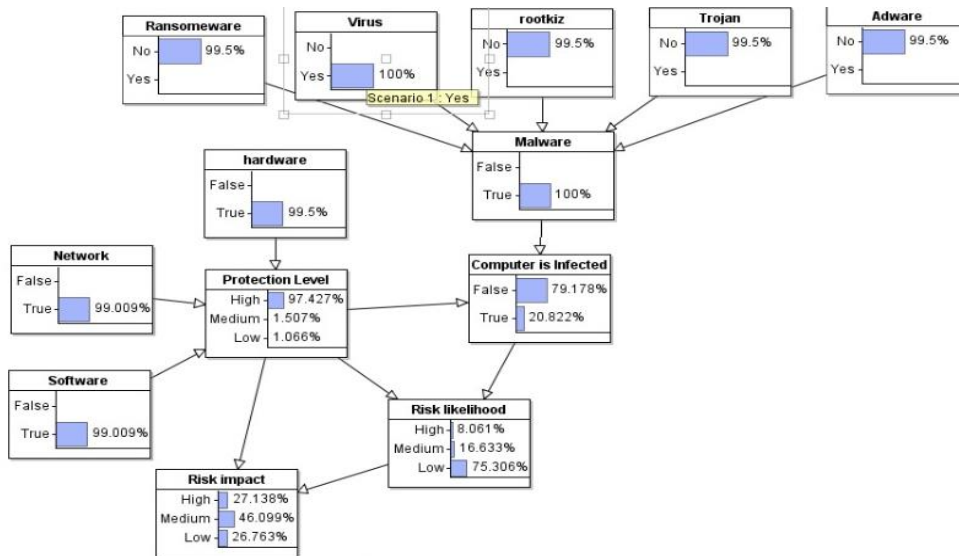


Figure 6-55: High protection for a low computer malware infection

Figure 6-55 shows viruses as malware that has infected the computer, which is 100% protected. So the protection is 99% at the hardware, software, and network level. Seventy-six per cent of the low-risk likelihood results from a 100% protection level. The scenario showed a 46% medium-risk impact.



**Figure 4656: High malware infection at a high protection level**

Figure 4656 shows 20% of the detected computer virus infection. The scenario has 99% hardware, software, and network protection, resulting in a 97% protection level. This case yielded 75% of low-risk likelihood and 46% of risk impact.

### 6.10.2 Discussion and Recommendations

The illustrations demonstrated the risk likelihood and impact caused by malware attacks in different scenarios. The outcome of the scenarios is influenced by the network's security level, software and hardware. The scenarios revealed different malware attacks, such as Ransomware, viruses, rootkits, Trojan and adware. Regardless of the malware attack on the business system, the business network becomes vulnerable. Organisations could be affected by malware attacks on their computers, network, software, or hardware, but the risk impact depends on the protection level. Some users accept information from unknown devices that are connected to the network. Mainly, the malware is caused by unsecured systems and employee ignorance.

The impact of malware results in data leakage (Alexei & Alexei, 2021). Organisations should prioritise the device's safety to reduce the discontinuity of the device. Proper malware awareness education is essential to improve the privacy and safety of the device. The practice of safety measures is essential to minimise and reduce malware risks and improve the lifespan of a device.

## 6.11 SIMULATED SCENARIO 4: OBSERVATIONS OF THE PHISHING ATTACK

Phishing attacks as a social engineering threat focus on stealing credit card information and login details (Salem et al., 2010). The attacker pretends to be a trusted recipient, attracting victims to open their emails. Victims are often lured to follow the malicious links that lead to the malware's installation. The successful installation results in the system malfunctioning, showing unauthorised access to private and

sensitive information or ransomware (Choo, 2011). The event happens by compromising the available security measures to gain access to the network so that the attacker can distribute the malware (Rizvi et al., 2020). The phishing strategies could use the victims' details to process unauthorised purchases or steal identity and finances (McMahon, Bressler & Bressler, 2016). Depending on the attack level, some phishing schemes could compromise the privacy of information, its integrity, and confidentiality.

The various strategies include vishing, Smishing, whaling, pharming, spear, and deceptive phishing. Even though the attackers use different phishing strategies, their ultimate goal is to gain the victim's trust and deceive them so that they can benefit. For example, deceptive phishing threatens to lure the victims with a force of urgency. Fraudsters' spear-phishing customises emails using the recipient's name or the name of a reputable company to trick the victim into assuming they know each other. Mostly they use legitimate organisations to steal private and sensitive data such as login details or personal data (Bisson, 2021). With all the criminal attacks on businesses, the consequences of phishing attacks are difficult to recover from and result in significant financial loss, a bad reputation, loss of client trust, declined production, and business growth (Demirkan, Demirkan & McKee, 2020). The following section illustrates the relationships between the variables in determining the risk probability of phishing attacks.

### **6.11.1 Results**

A phishing attack demonstrates the fraudulent loss of information through the deception of the victim. The victim believes the form of communication is legitimate and hands over the login details and credit card numbers without proper investigation. As used in the scenario, an email attracts the victim so that the perpetrator may gain access and steal user data through an email phishing attack. Using AgenaRisk, the scenario uses the graphical representation to show the variables and the relationships between variables to determine the risk probability. The risk likelihood and impact are influenced by the phishing attack, the current protection level, and user awareness. The protection level and user awareness regarding security awareness and skills play a significant role in risk exposure. Different conditions of the phishing attack scenarios are described below.



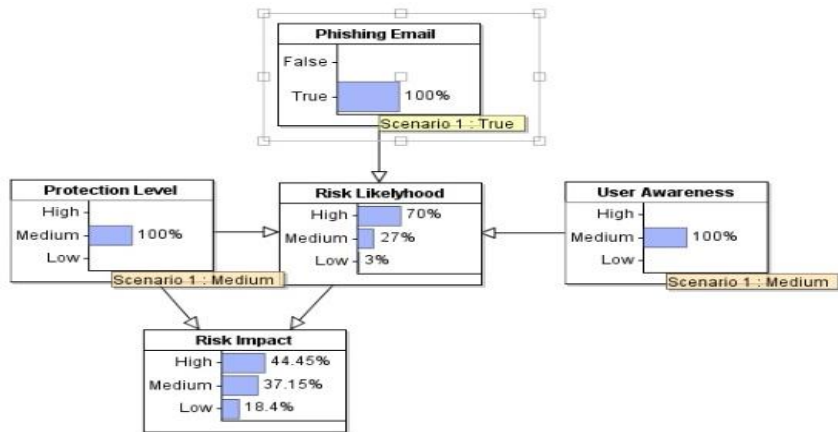


Figure 4-57: No phishing, with high protection level and user awareness

Figure 4-57 shows the phishing email attack at a high protection level and medium user awareness, resulting in a 70% high-risk likelihood and a 44% high-risk impact.

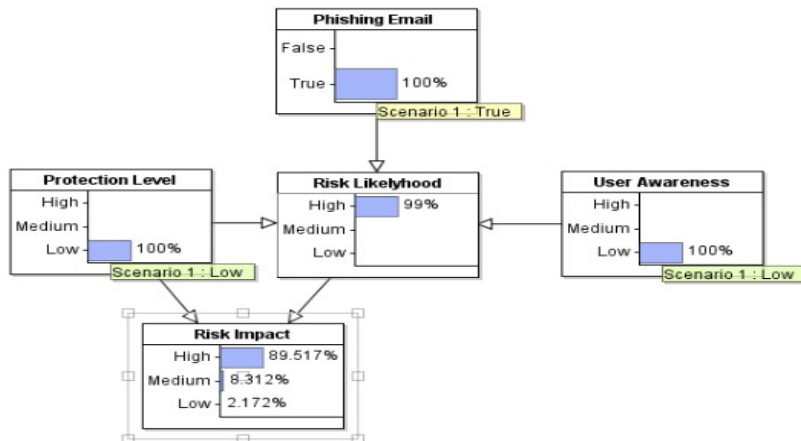


Figure 4-58: Phishing with high protection level and low user awareness

Figure 4-58 shows the phishing email attack on a high protection level and low user awareness, resulting in a 99% high-risk likelihood and 89% high-risk impact.

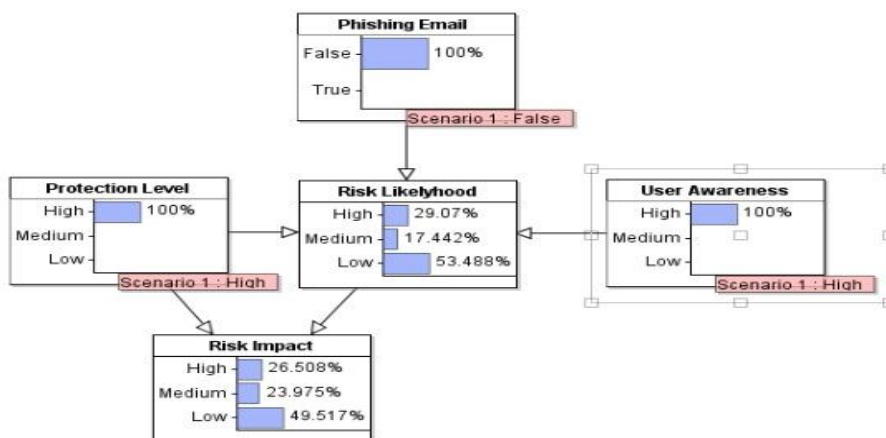
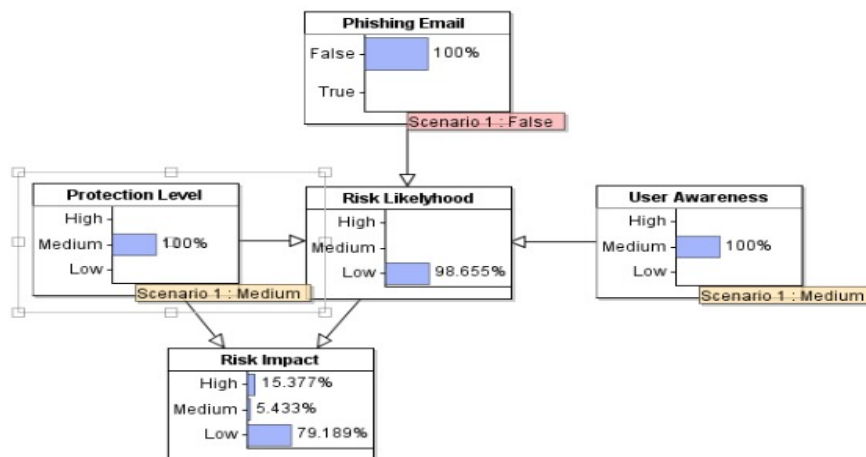


Figure 6-59: No Phishing email, high protection & user awareness

Figure 6-59 shows no phishing email attack on a high protection level and user awareness level, resulting in a low-risk likelihood and a 49% low-risk impact.



**Figure 6-60: Phishing email with high awareness, medium protection**

Figure 6-60 presents the phishing attack on medium-level security. When user awareness is medium, the risk likelihood becomes 98% low and the low-risk impact of 79%. The discussions and the recommendations of this case scenario are presented below.

### 6.11.2 Discussion and Recommendations

Phishing is a cybersecurity attack that uses messages or emails when malicious recipients pretend to be trusted people or reputable sources. This scenario demonstrates the phishing attack in the form of an email. Cybercriminals do anything to gain unauthorised access to the system through fraudulent communications. The criminals deploy their strategies to target their range of victims. The scenarios above revealed various risk probabilities and impact outcomes that businesses could experience. The results revealed that employee awareness of the cybersecurity guidelines and procedures has an impact on securing the systems and the protection level of the systems.

Amankwa, Loock, and Kritzinger (2015) believe that businesses should prepare cybersecurity training and awareness campaigns that align with long-term business goals. Their deceptive power and innovative strategies require businesses to implement proactive security measures at the top (Perez, 2020). Continuous cybersecurity awareness training should enforce good security practices and improve cyberhygiene. Good security practice reduces the amount of clicking on external links. Similarly, businesses should clearly understand their culture, human actions, and behaviour to support awareness training that best suits the organisational, human, and business processes (Santos-Olmo et al., 2016; ENISA, 2019).

The protection measures at all levels of the business should be highly considered. For this case, the companies could enforce multifactor authentication (2FA), which adds more security by verifying sensitive applications. In a phishing attack where the attacker compromises the username and password, the 2FA mechanism improves security by using a device (smartphone) for verification. This practice involves regular password changes and adherence to the accepted password criteria not to use the same password for multiple applications. Likewise, businesses should have dedicated cybersecurity personnel or management personnel to enforce and monitor the use of the improved password policies (Ncubukezi, 2021).

Even though businesses may not spot all phishing-related attacks because of their rapid evolution, it becomes essential for all institutions to use up-to-date security measures. In addition, companies must conduct regular training and awareness programmes to keep all staff on top of the attack's evolution.

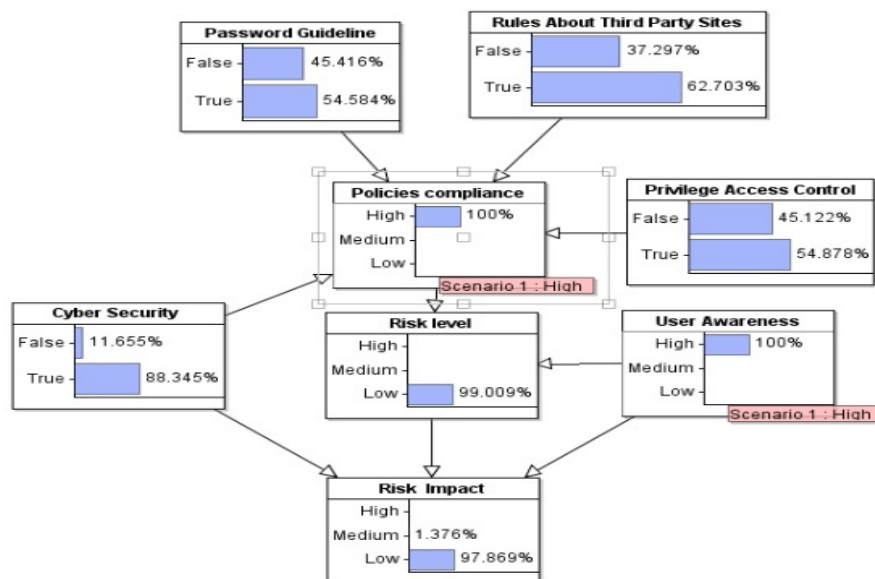
#### **6.12 SIMULATED SCENARIO 5: ADHERENCE TO POLICIES, GUIDELINES, AND RULES**

This section presents the last case used to demonstrate the probability of the risk being influenced by the protection level, the presence of the rules, and cybersecurity guidelines that describe what can be done and not done to the business's resources. The increased presence of cyberthreats is becoming complex and requires a consolidated approach that suggests a solution (Eugen & Petruț, 2018). Businesses should have a structured, documented policy to guide and improve the safety and security of valuable business assets regardless of their size. Most SMEs currently do not have structured policies that address the existing cybersecurity strategy (CISOMAG, 2020). The absence of cybersecurity guidelines, rules, and policies in the business sector becomes the channel and can lead to a major downfall for businesses. Most businesses pay little attention to the policies that address the appointment of a dedicated cybersecurity officer and visible management that enforces compliance to improve the safety and security of the resources. SMEs may not have enough resources to develop policies and therefore lack understanding of the effectiveness of the policy.

The cybersecurity policy clearly defines the procedures and rules for employees with access to business resources: the policy guides business resources, security threats, strategies to mitigate the vulnerability, and intrusion detection. The policy addresses guidelines about emails, data confidentiality, BYOD, rules, passwords, physical security, network, wireless and incident response. The presence of the cybersecurity policy outlines what employees can do and not do with the business's resources, clarifying the restrictions and consequences for ignoring the rules.

### 6.12.1 Results

This scenario demonstrates the impact of cybersecurity guidelines and procedures in a business setting. In this case, password guidelines, third-party guidelines, cybersecurity guidelines (devices and systems), and access control policies improve security procedures and policy compliance. The password guideline presents a set of steps guiding password usage and criteria. The duration and use of the password should be addressed. In addition, the guidelines for using third-party software should be clarified. Cybersecurity guidelines present the rules guiding the accepted use of the assets, account access, and information described. The overall policy compliance represents the enforcement of the guidelines, continuous monitoring of its effectiveness, and improvement to keep up to date. User awareness presents employee IT cybersecurity skills and knowledge applied to improve the safety and privacy of the computer and information. Every user on the system has privileges, so privileged access to the account restricts which user profiles are allowed to perform on the system. In this scenario, various variables with their relationships that help determine the risk likelihood and impact, with the help of AgenaRisk, are presented in a graphical representation. The following graphical representations demonstrate the case of the use of policies and rules.



**Figure 6-61: Partial cybersecurity, password, and access to third-party websites**

Figure 6-61 demonstrates 54% of the application guideline, 62% of the rules, 54% of proper access control privileges, and 88% of the cybersecurity procedures, resulting in 100% policy compliance. The policy compliance and 100% user awareness in this scenario contribute to 99% of the low-risk probability, equating to 97% of the risk impact.

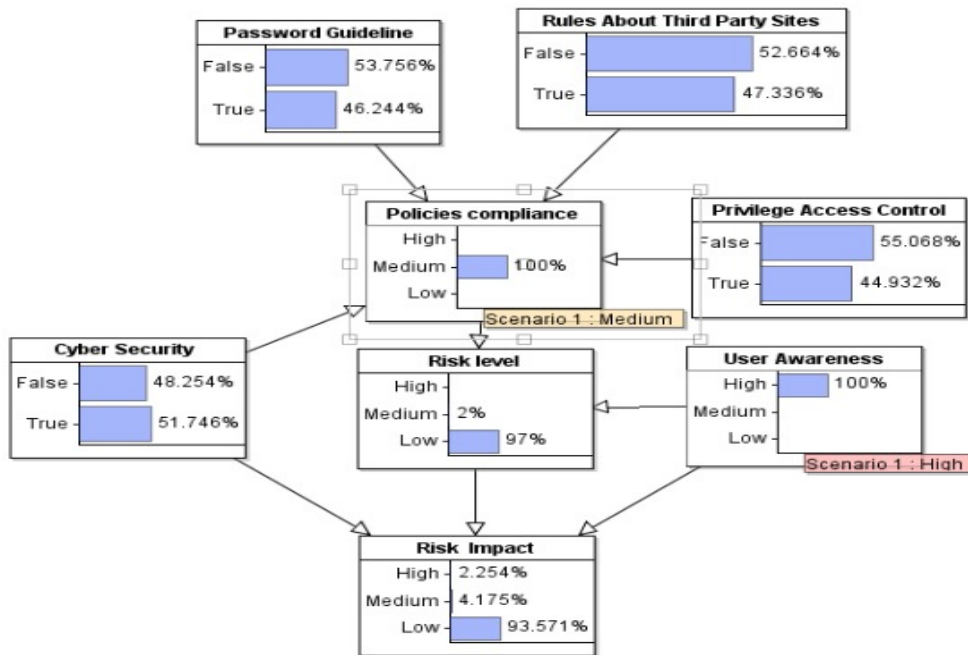


Figure 6-62: Partial cybersecurity, password, and access to third-party guidelines with medium compliance

Figure 6-63 shows medium policy compliance owing to 46% of password guidelines, 47% of rules about third-party sites, 44% of privilege access control, and 51% of cybersecurity compliance. Cybersecurity compliance is 51%, and user awareness is 100%, while 97% is for low-risk probability, influencing 93% of the risk impact.

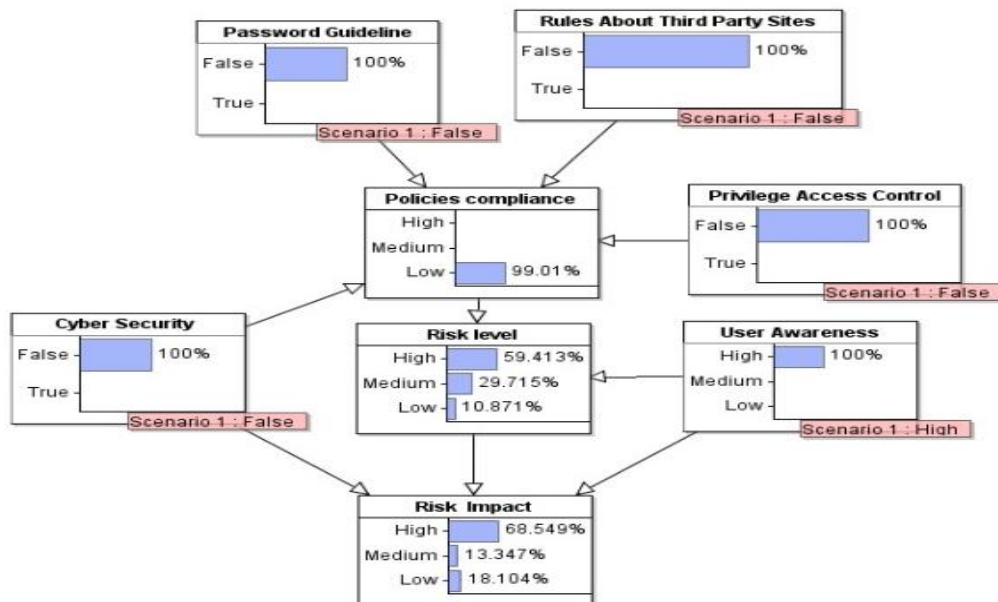


Figure 6-63: No cybersecurity, password, and access to third-party guidelines

Figure 6-63 reveals a 59% high-risk probability that influences 68% of the risk impact owing to 100% user awareness, 99% policy compliance, and 100% cybersecurity compliance. The policy compliance is affected by no password guidelines, no rules relating to third-party use, and a lack of compliance for access control privileges.

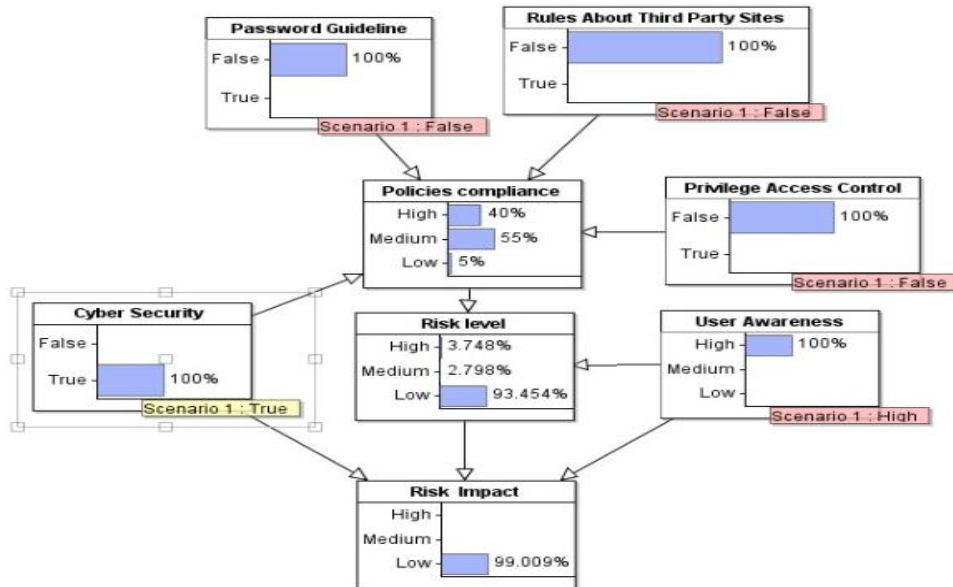


Figure 6-64: No password guideline and access to third-party websites

Figure 6-64 demonstrates a case scenario with no password guidelines, rules about access to third-party sites, no guideline about using account access privileges, and the presence of cybersecurity guidelines. All these aspects affect overall policy compliance, with user awareness informing 93% of low-risk probability and 99% of the risk likelihood.

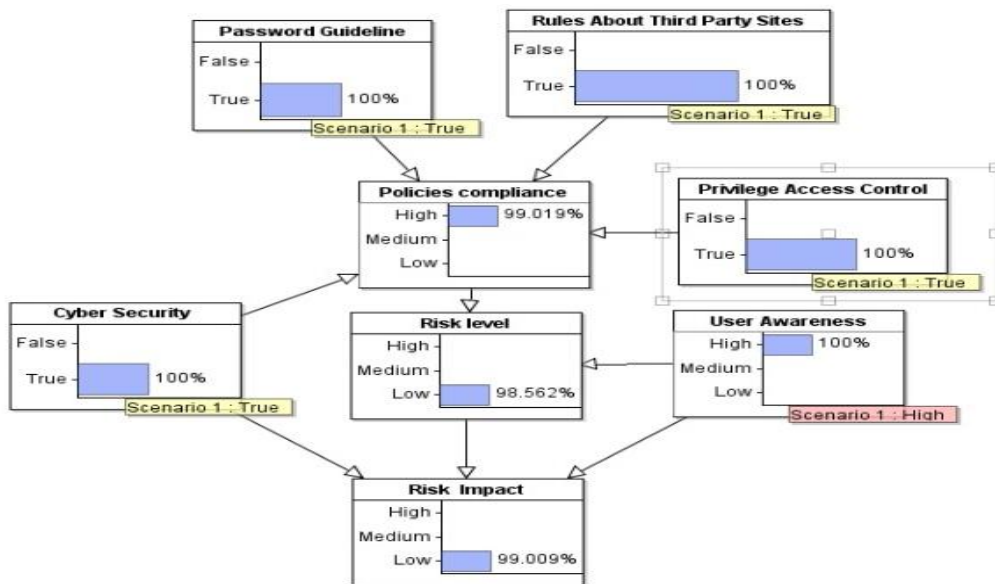


Figure 6-65: Presence of cybersecurity and user awareness

Figure 6-65 illustrates 100% presence of the password guidelines, 100% rules about using third-party sites, 100% privileged access control, and 100% cybersecurity guidelines, which results in 99% high policy compliance and adherence to the available security rules. The combination of 99% policy compliance and 100% user awareness results in a 98% risk probability, while the risk impact equates to 99%.

### **6.12.2 Discussion and Recommendations**

The openness of the device on the Internet requires standards that guide its use against possible cyberthreats and attacks (Li et al., 2019; Hoffmann et al., 2020). Patterson (2017) highlights the fact that the SME sector often pays little attention to cybersecurity. It is time to devise strategies to guard against the intruding and diverse persuasive range of cyberattacks. This case scenario presented variables that connect to determine the risk likelihood. As illustrated in the scenario, the more likely a risk is, the more vulnerable a business could be. Ifinedo (2012) states that sensitive organisational data should always be protected against criminals.

Owing to the negative impact of the risk in the sector and its exposure to cyberattacks necessitates the identification and application of solid safety practices (Brunner et al., 2020). The enforcement of strong and effective cybersecurity measures can be guided by clear guidelines with a detailed set of procedures and rules that describe what could be done and not done to protect organisational resources and information (Li et al., 2019). The scenario revealed that an adequate user-awareness level reduces risk probability. As a result, Ng and Xu (2007) explain that adequate training and awareness programmes for employees are a significant safety measure and improve security actions, attitudes, and behaviour.

For competitive advantage, businesses use complicated systems that require complex measures. For this case scenario, it is recommended that every organisation prioritise the safety and security of the overall business assets and information. All businesses should enforce the use of a password created with acceptable criteria, data leak prevention, monitoring techniques, and firewalls to filter incoming and outgoing traffic. Each of the mentioned security measures should have a clear, descriptive guideline that shares how each should be effectively used to improve cyberhygiene for all business assets. Even though the literature states that some employees do not pay attention to the policies, rules and guidelines (Han, Kim & Kim, 2017), living policy documents must exist and be reviewed regularly. In addition, some SMEs continue to take security for granted even though there is a provision in the policy document (Ifinedo, 2012).

The above case scenarios present the most commonly experienced risks in the SME sector. The graphical representations revealed different risk scenarios, which produce different risk probability outcomes and their impact. The risk probability outcomes presented in the cases more or less indicate how businesses could be exposed to cyber risk. These contributing factors compromise businesses and exposure to computer and information security. Unfortunately, assets and information security cannot be taken for granted. The criminals always advance their strategies to compromise security at all organisations. Cyberattacks target all business aspects, as demonstrated in the case scenarios. For

example, cyberattacks aim at unsecured end devices to gain unauthorised access and information stored on the resource.

Similarly, emails could be vulnerable to phishing attacks when less security is applied with minimal user awareness about cybersecurity. Human error is also a major agent in system and information vulnerability owing to employee ignorance and poor decision-making influenced by their levels of skills, attitudes, and behaviours (Richardson et al., 2020). In addition to unsecured networks, minimal user awareness becomes a channel for cybercriminals to deploy strategies that will activate the installation of harmful malware attacks.

Lastly, policies are the documents that are supposed to effectively guide the business resources and properly handle business information. So, every business needs dedicated cybersecurity personnel to enforce the policies and review their adoption. Similarly, to improve the state of security in the SME sector, it is also of good value for businesses to have a system that regularly sends reminders for every activity performed on the system. The system should send notifications when:

- A user is registered on the system,
- Applications are started and stopped,
- The call log is cleared,
- Several devices have the same malware signatures,
- Sensitive and private files and folders are changed,
- Executable files are processed and stored,
- An unknown IP address sends information to the network,
- The firewall denies incoming traffic from an unknown source,
- More than three unsuccessful login attempts occur on the device and username,
- A host receives malware,
- The device sends a message to more than ten other devices at once,
- A filtered message comes in from an unknown source.



**Table 4-19: Summary of the scenario cases**

Type Attack	Risk cause	Attack strategies	Risk Impact	Risk consequence	Mitigation strategy	Risk category
<ul style="list-style-type: none"> <li>• End devices</li> </ul>	<ul style="list-style-type: none"> <li>• Human actions</li> <li>• Ignorance - poor decision-making</li> <li>• Lack of employee skills</li> <li>• No device encryption</li> <li>• Lack of device management</li> </ul>	<ul style="list-style-type: none"> <li>• Theft, loss,</li> <li>• Third-party involvement</li> <li>• Malware attack</li> <li>• Unauthorised access to devices</li> </ul>	<ul style="list-style-type: none"> <li>• Poor business growth</li> <li>• Fraudulent acts</li> <li>• Lack of client trust</li> </ul>	<ul style="list-style-type: none"> <li>• Loss of information</li> <li>• Loss or stolen devices</li> <li>• Denial of service</li> <li>• Poor performance and economic growth</li> <li>• Loss of clients</li> <li>• A slow or unusable computer.</li> </ul>	<ul style="list-style-type: none"> <li>• User awareness and training</li> <li>• Two-factor authentication</li> <li>• Use of firewalls and passwords</li> <li>• Device encryption</li> <li>• Physical protection and regular backups</li> <li>• Secure connections and the websites</li> <li>• Use updated software,</li> <li>• Shutting down the devices</li> <li>• Checking physical surroundings when working online</li> </ul>	<ul style="list-style-type: none"> <li>• Asset</li> <li>• Information</li> <li>• System</li> </ul>
<ul style="list-style-type: none"> <li>• Human errors</li> </ul>	<ul style="list-style-type: none"> <li>• Planned and accidental actions</li> <li>• Ignorance - poor decision-making</li> <li>• Lack of skills</li> <li>• No management involvement</li> </ul>	<ul style="list-style-type: none"> <li>• No clear guidelines for cybersecurity procedures</li> <li>• Incomplete configuration management</li> <li>• Unauthorised use of access rights</li> <li>• Lack of skills</li> </ul>	<ul style="list-style-type: none"> <li>• Loss of information</li> <li>• Lack or loss of client trust</li> <li>• Financial loss,</li> <li>• Declined production and business growth</li> </ul>	<ul style="list-style-type: none"> <li>• Lack of a cybersecurity policy</li> <li>• Bring your own device</li> <li>• Physical security</li> <li>• Identity theft, fraud.</li> <li>• Deletion, theft and corruption of data.</li> </ul>	<ul style="list-style-type: none"> <li>• Up-skill employees</li> <li>• Limiting personal information</li> <li>• Regular backups</li> <li>• Restrict access to systems</li> <li>• Use firewall and antiviruses</li> <li>• Regular software updates</li> <li>• Management involvement in enforcing compliance</li> <li>• Reporting cyber crimes</li> <li>• Enable click for plug-ins</li> </ul>	<ul style="list-style-type: none"> <li>• Information and</li> <li>• System Security</li> </ul>
Malware	<ul style="list-style-type: none"> <li>• Human errors</li> <li>• Unsecured networked systems</li> <li>• Lack of cybersecurity guidelines</li> </ul>	<ul style="list-style-type: none"> <li>• Worms, Trojan, viruses and spyware)</li> <li>• Phishing scams</li> <li>• Unrestrained web browsing</li> <li>• Bad password</li> <li>• Human errors</li> </ul>	<ul style="list-style-type: none"> <li>• Malfunctioning of servers</li> <li>• Unexpected system and network failure</li> <li>• Limited access to resources</li> <li>• Data breaches</li> <li>• Compromised system and information security, privacy and safety</li> </ul>	<ul style="list-style-type: none"> <li>• Identity theft.</li> <li>• Deletion, theft and corruption of data.</li> <li>• Denial of service</li> <li>• Fraud-freeze access until payment is made</li> <li>• Captures private information</li> </ul>	<ul style="list-style-type: none"> <li>• Use of firewalls, latest active antivirus, &amp; antispyware</li> <li>• Multifactor authentication</li> <li>• Use of antiviruses and antispyware</li> <li>• Restrict access to third-party software and other links</li> <li>• Management involvement in enforcing compliance</li> <li>• Always removing less-used applications</li> <li>• Use of updated operating systems, plugins and browser</li> <li>• No clicking of unknown links on emails and other unknown downloads</li> </ul>	<ul style="list-style-type: none"> <li>• Device access</li> <li>• Network security</li> <li>• System Security</li> </ul>
Phishing attack	<ul style="list-style-type: none"> <li>• Social engineering attacks</li> </ul>	<ul style="list-style-type: none"> <li>• Vishing</li> <li>• Deceptive Phishing</li> <li>• Spear phishing</li> <li>• Whaling</li> <li>• Smishing</li> <li>• Pharming</li> </ul>	<ul style="list-style-type: none"> <li>• Financial loss,</li> <li>• Bad reputation,</li> <li>• Loss of client trust</li> <li>• Declined production and</li> <li>• Business growth</li> </ul>	<ul style="list-style-type: none"> <li>• Stealing or revealing sensitive data (login details, credit card information)</li> <li>• Unauthorised installation of malware software</li> <li>• Freezing systems</li> <li>• Loss of identity</li> <li>• Unauthorised purchases</li> </ul>	<ul style="list-style-type: none"> <li>• Use of firewalls to avoid phishing scams</li> <li>• User awareness through reminders and training</li> <li>• Regular improved security</li> <li>• Use HTTPS</li> <li>• Send security reminders</li> <li>• Use two-factor authentication</li> <li>• Regular backups</li> </ul>	<ul style="list-style-type: none"> <li>• Email</li> <li>• Network</li> <li>• Server</li> </ul>
Poor adherence to policies and guidelines	<ul style="list-style-type: none"> <li>• No management commitment</li> <li>• No dedicated cybersecurity personnel</li> </ul>	<ul style="list-style-type: none"> <li>• Messages</li> <li>• Email</li> </ul>	<ul style="list-style-type: none"> <li>• Mistakes leading to a significant data breach</li> </ul>	<ul style="list-style-type: none"> <li>• Data breaches</li> </ul>	<ul style="list-style-type: none"> <li>• Use of firewalls</li> <li>• Use and management of passwords</li> <li>• Use of strong password criteria</li> </ul>	<ul style="list-style-type: none"> <li>• Network</li> <li>• Password</li> <li>• Device</li> </ul>

	<ul style="list-style-type: none"><li>• Poor compliance with guidelines and procedures</li></ul>		<ul style="list-style-type: none"><li>• Ignorance can lead to legal fines, loss of client trust and</li><li>• Bad Reputation</li></ul>		<ul style="list-style-type: none"><li>• Restricted access</li><li>• 2-factor authentication</li><li>• Enforce policy compliance</li><li>• Use of pop-up blocker to limit unauthorised access</li></ul>	
--	--	--	--	--	--	--

### 6.13 CONCLUSION

This chapter demonstrated the development and evaluation of the different graphical models and simulated scenario cases that demonstrated the relationships between the dependent and independent variables in determining the probabilities of the risks and their impact on different scenarios. The variables used with the AgenaRisk are selected from the collected data and connected to produce an outcome. The variables demonstrate other cases to identify and represent relevant uncertainties. The models designed and developed in this study capture uncertain relationships based on simulated and experimental results. The different cyberrisk scenario cases showed the relationships with the variables and connections to each variable in determining each case's risk probability and impact. Using the AgenaRisk package, each case scenario presented a graphical representation of the variables that generate the risk probability for SMEs. Each case study scenario illustrates the results, discussions, and recommendations to reduce cyberrisks.

The five developed simulated risk case scenarios illustrated their risk likelihood and the risk impact that results in a data breach. The study described the end devices, human factors, malware attacks, phishing attacks, and the lack of policies and guidelines. The study also showed the type of attack linked to a risk cause, attack strategy, risk impact, risk consequence, mitigation strategies and risk category. The listed risks are the most dominant attacks which the SME sector experienced. SMEs are vulnerable to cyberattacks, and yield highly rated risks that negatively impact on business

The demonstration of various scenarios indicated the risk consequences that affect the business's general privacy, safety, and security. The cases showed relationships between the variables, risk source, risk likelihood, protection measures, and risk consequence. The risk probability can be low, medium, or high based on the presence of the variables and their relationships. In addition, the risk likelihood equates to the consequence of risk—the lower the risk, the low the impact. Even though cases demonstrated varied probabilities, the results necessitate implementing effective and proactive security measures. In addition, the work illustrated inadequate measures likely to expose businesses to a diverse range of cyberrisks.

The following section assesses cyberrisks by applying risk management techniques in the cybersecurity context by performing the qualitative risk methodology to analyse and identify SMEs' common cyberrisks. Quantitative risk assessment plays a crucial role in effective decision-making about cybersecurity strategies (Wang, Neil, and Fenton, 2020).

## **SECTION D: RISK EVALUATION AND CONCLUSION**

### **SECTION D: RISK EVALUATION AND CONCLUSION**

#### Evaluation of risk management techniques and conclusion

This section presents Chapter 7 and Chapter 8.

Chapter 7 applied the risk management techniques to assess the severity of the risks based on risk probability and consequences. The assessment is based on the risk matrix. It uses sensitivity techniques such as sensitivity analysis, Tornado graphs, decision tree analysis, risk scenarios, expected monetary value, and the expected maximum value. Risk treatment, monitoring, and reporting techniques are also discussed, and further recommendations are made.

Chapter 8 concludes the study by reviewing the objectives and presenting the research implications, outcomes, and contributions. The study's limitations, recommendations, and future work were accounted for, and the study concludes with a summary.

## **CHAPTER 7: RISK MANAGEMENT TECHNIQUES**

### **7.1 INTRODUCTION**

Before addressing the details of this chapter, it is essential to give an account of the previous chapters, which discussed the overview of the small business sectors with regard to cybersecurity and the empirical study. Section A presented the study background and reviewed relevant literature about cybercrimes, risks and their impact on SMEs. Section B presented the qualitative research findings and discussed them further. This study used thematic analysis and descriptive statistics to analyse and interpret data from the research participants. For thematic analysis, the results were presented according to the themes. The study accounted for the relevance of the cybersecurity framework, risk management standards, and the adoption of the Bayesian Network tools with AgenaRisk. The NIST cybersecurity framework was presented in detail in Section B, the risk management standards were illustrated in Section D, and the use of the AgenaRisk package was presented in Section C discussed the research methodology adopted to carry out the work.

The current chapter presents risk management processes (RMP) of ISO 3000: 2009. Risk management is essential for future planning based on what could go wrong and the related countermeasures to minimise risk exposure changes (Tranchard, 2018). This study focused on the cyberrisks at SMEs in South Africa (SA). This study adopted risk management processes indicated in Figure 7-66 to assess the cyberrisks experienced by the small business sector. The study discussed each process of cyberrisks in the small business sector further.

### **7.2 RISK MANAGEMENT PROCESSES**

As cited in the Project Management Body of Knowledge (PMBOK, 2013) (PMI, 2008), the risk management process has seven phases, namely communication and consultation, establishing the context, risk identification, risk analysis, risk evaluation, risk treatment and review, and monitoring (ISO, 2009), which are illustrated in Figure 5-66. They are discussed in detail below.

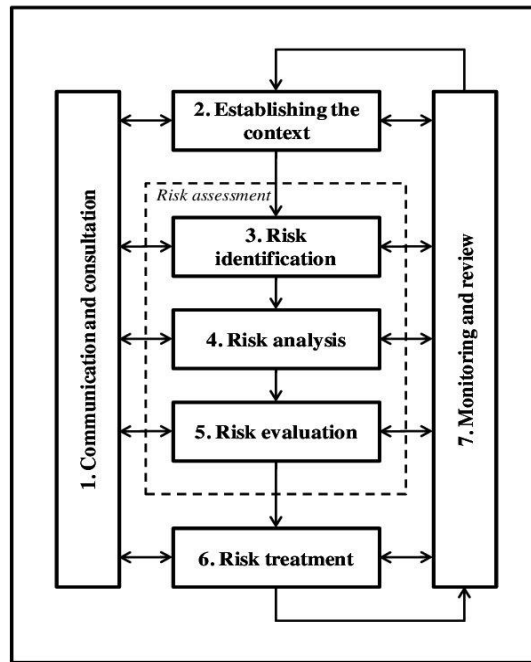


Figure 7-66: Risk management process from ISO 31000:2018

### 7.2.1 Communication and Consultation

As explained in Chapter 1, the study aimed to perform a risk analysis to design, develop and evaluate the cyberrisk tool for SMEs. So this work selected a sample of research participants based on the following criteria:

**Participants:** the SMEs had a range of one (1) to one hundred and fifty (150) employees who are based in SA from the construction, waste management, transport, and motor trade, ICT, electrical, gas and water, real estate, accommodation and catering, manufacturing and retail sectors. The IT and business managers, employees, chief information officers, and departmental technical heads were selected from these sectors. The researcher used purposive sampling to select a total of forty-five (45) participants to gather relevant information and explain the research findings further.

**Data-collection methods:** The study combined open-ended qualitative and quantitative questionnaires on google forms with interviews. Interviews were conducted with the security specialists to understand the cybersecurity risks, likelihood of risk, impact, monetary value, and protection measures in cybersecurity better. The questionnaires were used for business managers, IT managers, and chief information officers. The triangulation of the data sources, which are interviews and questionnaires provided exploratory and qualitative data. Most participants completed the survey, while some were unavailable for the interviews because of the pandemic. All the questions answered the main research question stated in Section 1.

**Data analysis:** This study used thematic analysis to analyse the collected exploratory and non-quantifiable information in the survey and interviews. These were interpreted to produce meaning. The research questions were then categorised to classify the gathered data from the survey and interviews. The completed questionnaire and interview data collected were transcribed and then analysed using thematic analysis to determine the business background, types of cyberthreats or attacks, sources of cybersecurity risks, and protection measures. The concepts were determined, and similarities merged where necessary. The analysis determined and generated the meaning of the SMEs' experiences with regard to interactions and situations. In addition, the study used the RMP to analyse the risk likelihood, impact, and expected monetary value. The work also used quantitative techniques such as decision tree analysis and cybersecurity risk scenarios. Furthermore, sensitivity analysis, tornado graphs, and the EMV to assess cyberrisk likelihood were implemented using the AgenaRisk package.

### **7.2.2 Establish the Context: Cyberrisks in SMEs**

Technology gained popularity in the different sectors, and the Covid-19 pandemic exposed quantified cybercriminals deploying innovative strategies. The increased cyberattacks and threats exposed the state of cybersecurity in various business sectors, leaving them vulnerable to cybercrimes. Benz and Chatterjee (2020) explained that SMEs are the most susceptible institutions which are not ready for cybersecurity risks and resilience against attacks. Every opportunity of cyberthreat in the business system causes damage to the business system, which becomes an ultimate cyberrisk.

Even though the SMEs are not all focusing on the same business, the impact of cybercrimes affects their growth and business continuity. The results revealed the effects of the cyberrisks are related and somehow dependent on one another. With the number of reported cyberthreats and attacks, businesses have noted the change in their business dealings, such as the loss of profit, delayed economic growth, client loss, daily business disruptions, lack of customer trust, and a dented reputation of the business. Cybercrime's impact remains a major and challenging issue in all institutions that mostly use the Internet as the main communication tool. The following findings from the consulted businesses are the leading results of the negative cyberrisks.

- **Financial loss** – Most businesses lose profit when there has been a delay or disruption in business activities. During the Covid-19 pandemic, many businesses had to meet the demands of paying ransomware to cybercriminals. Without new prospects, some businesses saw their profits fall, or the business did not do well while it had to pay the overheads such as the rent and marketing for new clients. At times, criminals gain unauthorised access to financial information systems for personal gain.
- **Dented business reputation** – Through the use of accessible and inappropriate passwords, criminals had gained access to the company's resources. During Covid-19 times, most

businesses lost their good reputations as clients cancelled their contracts. This meant a reduced source of income because of poor delivery, which eventually resulted in client loss.

- **Client loss** – Clients can always lose interest in businesses for different reasons. Discontinuation of the product by the supplier or delayed delivery leads to the loss of clients. The clients look for other business suppliers to meet their demands within an expected time frame.
- **Daily business disruptions** – In any business sector, unforeseen circumstances such as sudden load shedding, late delivery of the products and poor communication from the suppliers or third parties require interim measures. Daily business disruption can also be caused by a less-informed employee who accepts or downloads inappropriate content from unsecured websites, eventually affecting the system which leads to regular business delays.
- **Lack of trust** – clients can easily terminate their contracts or services when their needs are not adequately met. Sometimes, clients lose the trust they have in the supplier, which, at times, the supplier may not have control over. Sometimes, the businesses lose the client's information owing to negligence, a lack of skills or through inappropriate ways of securing information and information storage.
- **Business discontinuity**- This is the last stage of the business's existence. Some of the reasons for ending the business are a lack of experience, delayed delivery of the products from the suppliers, limited or insufficient business capital, unexpected delays in growth and inexperienced or poor management.

The results showed some great similarities collaboration among different business participants with regard to the common types of cyber-attacks and threats experienced. Even though most businesses are the victims of cyberrisks and crimes, some businesses still do not disclose the forms of cyberattacks they experience (Hubbard, 2019). It becomes quite difficult for businesses to recover from the effects of cybercrimes (Bendovschi, 2015). In addition, it is difficult for the business to fully recover customer trust, its reputation and its profits (Ncubukezi & Mwansa, 2021b). However, the main resources businesses lose owing to their dependency on the Internet are their information system and finances (Balan et al., 2017).

Similarly, Brockett et al. (2012) also share the same sentiments about losing a business's information systems and reputation. Tam, Rao and Hall (2021) explain that cybercrimes negatively affect the state of information security, the economy and business growth. In addition, the increased cyberattacks harm businesses extensively economically (Teufel et al., 2020). Increased cybercrimes have greatly affected the economic growth of SA businesses (Hubbard, 2019). Even though the 'blanket approach' may not be appropriate for all businesses and institutions, this study recommends effective best practices cited



by Ncubekezi (2022a), Kayumbe and Michael (2021) and Ncubekezi and Mwansa (2021a), as well as Coventry et al. (2014). These best practices include regular system and software updates, enforcing proper and accepted password criteria, using strong antivirus programs, antispyware and active firewalls, proper computer shutdowns, secure connections and websites, regular training on phishing scams and limiting the use of passwords in a public space.

### **7.3 RISK IDENTIFICATION**

Several factors cause cyberrisks in private and public business domains (Shevchenko et al., 2021). Cyberrisks are multifaceted and dynamic and have different impacts, making them difficult to handle without classifying them. Peters, Shevchenko and Cohen (2018) and the Joint Research Centre (2019) explain that these cyberrisks include technical, behavioural and cultural aspects. Risk classification identifies the source of the risk by allocating a unique reference (Nasir, Naderi & Momeni, 2020). Each cyberrisk is given a risk code used for the risk matrix. To effectively conduct risk management in any organisation, it is vital to understand the list and categories of possible risks. Those risks should be kept and stored on a risk registry. These cyberrisks are thoroughly identified and outlined in Table 7-20.

Table 7-20 summarises the collected risks subjective to business sector perceptions. The table illustrates the risk causes, risk numbers and risk categories. The risk number presents a numbered list of the analysed risks. The collected risks were related to system users which generated human-related risks, which could either be genuine human errors or initiated by criminals. This requires the documentation of all the business stakeholders and system users, where the potential contributors are the employees of the businesses, third parties and clients. The business employees can be computer literate or illiterate with some understanding of the policies and guidelines to carry out the business objectives. However, employees with limited understanding and skills can become the link for criminals.

Knowledgeable employees can ignorantly make decisions based on their attitude and stress levels because they are overworked, thereby exposing the system. Third parties present external links that supply and support the business. Business customers interact with the system to receive the service. They can be internal or external customers who can pose risks to the systems. For example, a customer can send an email that can be phishing. Criminals use the system for their benefit. They deploy strategies that expose the business to risks and leave the system vulnerable to threats (Paulsen, 2016). The results revealed that the businesses experienced various threats resulting in common risks. These threats exposed business information systems, files, end devices, network devices, policies, email and employees (Pritom et al., 2020). Businesses experience various intrusions, unauthorised access to their systems and malfunction of resources, insider attempts and planned attempts. This study reviewed the collected data to identify the common cyberrisks SMEs are experiencing and classified risks into five

categories: risks caused by human factors, phishing or network-related risks, technological risks and device-related risks.

### 7.3.1 Cyberrisk Register

Identifying risks helps to understand the nature of the possible risks yielding either a positive or negative impact. This phase captures all experienced cyberrisks from the perceptions of each participating business sector, promoting communication and feedback among the stakeholders. These risks help to identify the risk assumptions, causes and anomalies. Identifying cyberrisks, especially during the Covid-19 pandemic, exposed risks at SMEs. This phase determines potential risks and is performed before conducting a qualitative and quantitative risk assessment to develop the risk register to analyse, prioritise and monitor risks. The risk identification techniques are used to identify the common cyberrisks at the SMEs in SA. Cyberrisks at businesses have gained widespread interest in academic and business institutions. Ncubekezi, Mwansa and Rocaries (2020b) conducted a study determining cyber hygiene in small businesses. Their results revealed several threats and attacks related to the root causes of cyberrisks in business sectors.

Risk identification addresses the questions of when, how, which and where the risk can take place (Tranchard, 2018). For example: When can a cyberrisk take place? How can the risk happen? Which business assets could be affected by cyberrisks? And where can cyberrisks be found in a business? Those risks are outlined in Table 7-21, guided by the contents of risk identification in Table 7-20. The risk identification table lists the risk categories as technological, technical, managerial and human factor risks. The list of assets that get affected by risks has been outlined. Risk identification as an ongoing task in any business or organisation focuses on documenting and listing risks experienced by organisations in order assist businesses to better understand their potential risks.

**Risk number:** This presents the numbering used to identify the risk in the risk register.

**Cyberrisk:** Any form of dependent and independent financial loss, damage or disruption caused by the failure of a resource.

**Risk code:** Each identified risk is given a unique code used to determine the risk from the list.

**Risk cause:** Presents the source of the risk, which triggers vulnerability in the business system.

**Risk category:** The risk categories present the related potential cyberrisk causes which can be evaluated and responded to. These are the malware or technological risks, devices or technical systems, human factors, policies and lack of guidelines.

**Table 7-20: Analysis of cyberrisks, their causes and the source (Data source: Survey, 2021)**

Risk #	Risk	Risk code	Cause	Category
1	Unauthorised access to software	UAccSof	Poor guideline compliance, malware, criminals, employee ignorance	Technological risks, malware
2	Unauthorised access to rooms or facilities	UAccRo	Employee ignorance, poor implementation of security measures	Device security
3	Unauthorised user registration	UUseReg	Poor security compliance, inside attempts	System security, lack of guidelines
4	Unauthorised access to data and files	UAccDatF	Criminals, inside attempts, poor security compliance	System security, lack of guidelines, human factors
5	Unauthorised access to devices	UAccDev	Criminals, inside attempts, poor security compliance, malware, phishing	Human factors, poor security compliance
6	Stolen devices and information	StoDevI	No device encryption, no backup plan	Devices
7	Outdated antivirus and antispyware	OAnti	Easiest gateway for cybercriminals, loss of data caused by software failures & no software compatibility	Human factors, malware
8	Faulty network connectors and transmission media	FauNeT	Loss of data and network connection	The device, human factors
9	Old equipment and device failure	OEFail	Failure to perform preventive maintenance, improper operation, misconfiguration	The device, human factors
10	Malfunctioning of the system or network	MalFir	Failure to perform preventive maintenance, improper operation	Poor policy compliance, human errors
11	Open wireless network	OnWiN	Unauthorised network access, slow network speed owing to unauthorised devices	Poor policy compliance, human errors
12	Human errors	HumErr	Poor decision-making, lack of skilled personnel, ignorance, stress owing to staff shortage	Poor policy compliance, human errors
13	Use of incorrect password criteria	InPas	Poor password generation, no regular reminders to change passwords	Human factors, poor policy compliance
14	No policy or guidelines	NoPolic	Lack of dedicated personnel and management	Poor policy compliance
15	Fraud or stolen information	FrStea	Phishing, criminal actions or inside attempts	Phishing, human factors
16	Malware (Viruses, worms, Trojan)	Mal	Malfunctioning of the network, data loss, financial loss	Malware
17	Accidental installation of unsecured applications	AccInst	Phishing, malware	Malware, phishing
18	Regular system and application failure	SysFai	Malware, social engineering attempts, denial of service, phishing	Poor policy compliance, human errors, phishing
19	Unauthorised modification, deletion, loss of data and information	ModDa	Data theft, human errors, phishing	Poor policy compliance, human errors
20	Denial of service and network downtime	DoS	Prolonged network performance when opening files or accessing websites, unavailable websites, or unable to access any website.	Malware, Poor policy compliance, human errors, network
21	Hardware and software failure	HSwaFai	Old hardware equipment and obsolete software, phishing	Poor policy compliance, human errors, malware, phishing
22	Bad management	BdMan	No clear guidelines, misalignment with business objectives	Poor policy compliance, human errors
23	Misconfiguring the device	MSConf	Weak passwords, no data encryption, no access restrictions and mismanaged permission controls	Human factors, poor policy compliance
24	Poor delivery of outsourced IT services	OITSer	Biased software decisions, compromised security	Human factors, poor policy compliance
25	Use of USB	UUSB	Criminals, inside attempts, lack of guidelines	Malware, device security & Poor policy compliance
26	Lack of data confidentiality	LaDC	Data breach, compromised system, lost or stolen device, phishing	Poor policy compliance, human errors, phishing
27	Lack of data integrity	LaDI	Human errors, malicious attacks, malfunctioning devices, phishing	Poor policy compliance, phishing

Table 7-21 summarises the collected cyberrisks according to the different risk categories. Table 7-20 shows 27 risks, colour-coded according to the risk categories to make 60 identified cyber-related risks. **Table 7-21** shows the breakdown of the risks.

**Table 7-21: Total number of identified risks (Data source: Survey, 2021)**

Risk Category	Identified risk
Devices or technical systems	7
Technological risks/malware	8
Phishing and network	7
Human factors/human errors	20
Lack of policies & guidelines	19
<b>Total</b>	<b>61</b>

The findings revealed various identified threats that different business sectors have experienced, yielding various risks. As shown in Table 7-20, these are unauthorised accidental and planned threats, information misuse by authorised personnel, data breach, leakage or loss, and service disruption owing to a lack of strong guidelines and policies. The respondents revealed that these risks affect strategic planning, the business’s reputation, operational events and transactional actions, which lead to poor compliance. The following section determines the inherent risk and impact based on the identified cyberthreats.

### **7.3.2 Identified Cyberrisk Categories**

Cyberrisks emerge from several cyberattacks, threats and crimes committed by criminals or illiterate employees. Some of the most important and most deadly cyberthreats occurred during the Covid-19 global pandemic. These cyberthreats range from browsing applications and mobile applications to malicious domains, ransomware, social media messaging, distributed denial of service (DDoS) attacks, malware on the systems and websites, spam emails or compromised emails and distributed denial of service (Khan, Brohi & Zaman, 2020). Cyberattacks can use the standalone device or the cyberspace on a networked device to attack SMEs. The research participants shared most of the attacks and threats; they were then identified and grouped into different cyberrisk categories. The identified risk categories are human factors, phishing and network-related risks, malware and technology, devices, technical systems and policies and guidelines.

#### **7.3.2.1 Human factors**

Among other cyberrisks, human factors result in remarkable damage to businesses and remain the primary security concern. Cyberrisks affect various businesses by connecting to standalone or networked computers. In addition, Kobis (2021) believes that the human factor plays a major role in infiltrating sensitive information. The results revealed that human users use infected memory sticks on standalone computers. An example would be when an employee ignorantly follows the websites' links that gather sensitive information. This action results in increased unauthorised information disclosure

and data breaches (Richardson et al., 2020). Sometimes, legitimate users perform activities under pressure, resulting in common and unplanned mistakes. In addition, human factors can result from employee understaffing or work demands. Sometimes, human factors result from the lack of support and awareness training leading to unacceptable behaviour. These common human factors are mainly the mistakes caused by poor decision-making (Sasse, Brostoff, & Weirich, 2001), becoming the loophole for cyberthreats and attacks. Likewise, some employees' attitudes influence their decision-making (Richardson et al., 2020).

### **7.3.2.2 Phishing and network-related risks**

During the COVID-19 pandemic, all institutions had to rely on cyberspace for business visibility and to attract new markets (Ncubekezi, Mwansa & Rocaries, 2021). Convenient access to cyberspace grants cybercriminals a chance to explore new markets in all institutions, especially where cybersecurity is not prioritised. Results indicated that the participants become the victims through hackers manipulating the website scripts. Some participants experienced phishing attacks through their emails and phones when users curiously opened fake emails out of ignorance and recklessness. Some emails may have an attachment of the malware, which automatically installs when it is opened. Over and above phishing, some participants experienced denial of service, network or device exploitation, and the ultimate data breach. According to the Ponemon Institute (2018), through networked devices, cybercriminals gain unauthorised access to the business network to access, read, alter and delete private business information. SMEs need a detailed guide that protects the business networks and data to ensure that activities are safe and secure. It has been mentioned that the lack of financial resources of the SME prevents it from applying complex, multifaceted and reasonable security systems for cyber risk mitigation (Antunes et al., 2021).

### **7.3.2.3 Malware and technology-related risks**

The research participants indicated that malware attacks mostly gain access through network interfaces to penetrate business systems. Sometimes the malware attacks are transmitted through memory sticks which become insider-generated. The users sometimes accidentally install the infected installation package of the illegitimate program available on the site to trick uninformed users. Some users become the channel of malware attacks owing to quick and easy access to free and infected software packages on the Internet. The criminals on the network use and deploy malware on the business systems and devices (Millaire, Sathe & Thielen, 2015; Hiscox, 2019;), while the less skilled people who access less protected web pages become extremely dangerous for the business and are difficult to mitigate (Ndeda & Collins, 2019). As a result, ignorant users download and install software from unverified sources (Kobis, 2021).

#### **7.3.2.4 Devices and technical systems**

The devices (end or intermediary devices and peripherals) form part of the business systems. Devices connected to the Internet or functioning on their own may be the main entrance for victims of cybercrimes. The criminals use open interfaces on the networked devices, while standalone devices get affected through external hard drives for information exchange. Sometimes, the devices and technical systems get stolen, intruded upon, or information is lost. Some cybercrimes can be dependent and independent of the Internet (McGuire & Dowling, 2013).

#### **7.3.2.5 Lack of policies and guidelines**

These are essential for every business to guide the use of business resources and implement proper and proactive cybersecurity measures which protect the business and the employees (Eiza et al., 2021). The business rules, procedures and guidelines should have detailed information about processes to be followed when handling business activities (Antunes et al., 2021). Employees have become the easiest and the weakest link in institutions (Von Solms & Von Solms, 2014). Therefore, all business institutions need to have a detailed document that guides them on how to use the resources. As a result, most employees do not pay proper attention to password creation, especially if there is no enforced guideline, which becomes a loophole for criminals. Often, end-users focus on memorable, easy and convenient passwords. The absence of a policy document or poor enforcement of the proper rules, policies, procedures and guidelines become a loophole for many cybercriminals (Mugarura & Ssali, 2020). SMEs should enforce the policies and procedures (Ncubukezi, 2022).

### **7.3.3 Ranking of Cyberrisks**

The study used low, medium and high impact ratings. A low rating presents a minimal impact, the medium shows a damaging impact, which is recoverable, and the high rating shows a substantial impact. So the sum of the identified risks is summarised according to their priorities. Table 7-22 shows the identified risk categories ranked from low, medium to high to determine the risk priorities. These identified risks are based on the list of shared common risks which businesses experienced. These are listed in Table 7-20. Old and emerging risks are identified and prioritised from low, medium to high with reference numbers for the risk categories. These priority levels rank the listed collected risks to develop efficient response plans focusing on items with a higher priority. For every business, the risk priorities are usually aligned with the business's risk management plan, business objectives and risk response.

**Table 7-22: Ranking of the identified risks (Data source: Survey, 2021)**

Risk Category	Low [0-3]	Medium [4-6]	High [7-10]	Total
Technical/ Systems/Devices	1[2]	2[8,9]	4 [3,4,6,25]	7
Technological risks/Malware	1 [7]	3 [1,1,25]	4 [16,17,20, 21]	8
Human factors	4 [5,7,8,9]	9 [10,11,12 ,22, 23,24, 25, 13,21]	7[3,15,18,19,20,26,27]	20
Phishing/ network	0	1[15]	6 [17,18,20,21,26,27]	7
Policies & guidelines	3[10, 21,25]	7 [3,4,5,2,11,12,14]	9 [18,19,20,22,23,24,25,26,27]	19
<b>Total</b>	<b>9</b>	<b>22</b>	<b>30</b>	<b>61</b>

The qualitative risk analysis is presented in the section below based on risk estimation, impact analysis and final risk scoring. The application of the qualitative risk analysis is explained below in relation to the cyberrisks in the small business sectors.

#### 7.4 RISK ANALYSIS TECHNIQUES

This study used qualitative and quantitative risk analysis techniques; this section presents the application of qualitative risk analysis techniques to describe the likelihood of risk at SMEs and its impact to determine the risk matrix. Risk analysis is applied in the context of cybersecurity to analyse cyberrisks at SMEs in SA.

##### 7.4.1 Risk Probability and Impact Assessment

As the qualitative risk analysis uses probability and impact assessment, Table 7-23 presents the risk, the basic measure used to determine the risk probability and the consequence assessment based on the scale, probability, time, cost and scope. The scale indicates the risk rating based on the influencing risk probabilities, time of occurrence, amount caused by the risk and its impact. If the likelihood of the risk occurrence is high, it is very high for every risk. Similarly, if the risk occurs more frequently, then the risk is also very high. So, every possibility of risk is assigned costs and the frequency at which the risk occurs to determine the rating of the risk impact. Table 7-23 brings a common understanding of risks. This phase provides quality risk assessments to ensure reliability and data, providing the risk matrix that brings a common understanding when performing the overall risk likelihood and impact.

**Table 7-23: Risk probability and impact assessment**

Scale	Probability	Time	Cost	Scope
Very high	>75%	>4 months	900K – 1M	Severe Impact
High	55-74%	1-3 months	500K- 899K	Major impact on overall business functions
Medium	30-54%	2-4 weeks	300K-499K	Some impact on the key business areas
Low	11-29%	1-2 weeks	100K-299K	Low impact on business functionality
Very low	1-10%	6 days	0K-99K	Minor impact on business operations

After developing a common measure for risk probability and impact assessment, the following section unpacks how the risk impact technique is used to measure cyberrisks.

### 7.4.2 Risk Impact Technique

The impact analysis is essential in every organisation in order to produce a recovery plan focusing on identifying the potential cyberrisks and their probability of occurrence. The impact analysis describes a particular cyberrisk cause, threat occurrence and severity of the impact on the business system, providing information on how each cyberrisk can be treated. In the business system, a cyberattack can temporarily interrupt the business service, resulting in a single point of failure or an entire business system failure. Thus, estimating the impact of potential cyberthreats on assets is essential. Table 7-24 shows the impact values, the impact ratings, their description and the related cost. The impact values range from 0.1 for a negligible rating to 1.0 for a high rating. The impact ratings range from 1 for a minor impact to 5 for a high impact. The ratings determine the impact of the risks according to their severity. The lower the impact value, the safer the business and the higher the impact value, the more it can become dangerous to the business. Each impact rating has a descriptive statement that explains the consequence and the related cost of the impact on the budget. The cost of the impact value which has a range of 10% determines the impact rating which indicates the severity of the risk. A minor impact cost is fifteen percent more on the budget, while moderate rating costs sixteen to twenty-five percent more on the budget and a major impact costs twenty-six to thirty-five more than the budget.

**Table 7-24: Definitions of impact values ((Guided by (PMBOK, 2013))**

Impact value	Impact rating	Rating	Description	Cost
0.1	Negligible	1	Threats have no potential harm	Does not affect the budget
0.3	Minor	2	Threats seem normal and are acceptable	< 15% more on the budget
0.5	Moderate	3	Threats exist which can expose the business to risks	16-25% more on the budget
0.7	Major	4	The threat exists and needs remedial actions	26-35% more on the budget
1.0	Severe	5	Urgent threat to the organisation exists	>36% more on the budget

Now that we have clarified the impact ratings, it becomes essential to clarify the risk likelihood values so that the probability and impact analysis can be evaluated. The probability estimation is presented below.

### 7.4.3 Probability Estimation Technique

When conducting the probability and impact analysis, the risk likelihood values are essential for presenting the cyberrisk matrix. The probability of the risks is presented concerning the risk likelihood rating, with the quantitative likelihood rating values and their description. Table 7-25 shows the risk likelihood ranging from rare, unlikely to happen, moderate likelihood of occurring and certain to happen. All these qualitative likelihood values are assigned quantitative values, which are the ratings from 1 to 5 and the likelihood score from 3% to 100%. In addition, the table also shows the description of the likelihood rating and its criteria concerning the negative effect on the business system, which exposes the systems, information, assets and personnel. Therefore, the description shows the level of vulnerability of the business.



**Table 7-25: Definitions of likelihood values ((Guided by (PMBOK, 2013))**

Qualitative values Likelihood	Quantitative values		Description and the criteria
	Rating	Likelihood score	
Rare	1	3%	Vulnerability is not a concern and could have a <b>negligent effect</b> on the business system's operation, assets and employees. Relevant security controls are implemented, assessed and effective
Unlikely to happen	2	4-20%	Vulnerability is of minor concern and could have <b>limited effects</b> on the business system's operation, assets and employees. It might cause <b>minor financial loss, minor damage to assets and minor loss of employee information.</b> The effectiveness of the measures could be improved and relevant controls are implemented but with minimal effectiveness.
Moderate chance	3	21-50%	Vulnerability is a moderate concern that could severely affect the business system's operation, assets and employees. It might cause <b>minor financial loss, minor damage to assets and minor loss of employee information.</b> Relevant security controls are partially implemented but somewhat effective.
Likely to happen	4	51-79%	Vulnerability is highly concerning, which could severely affect the business system's operation, assets and employees. It might cause <b>major financial loss, damage to assets and loss of employee information.</b> Relevant security controls are planned but not effectively implemented but somewhat effective
Certain to happen	5	80-100%	Vulnerability is exploitable, resulting in <b>multiple effects</b> on the business system's operation, assets and employees. Relevant security controls are not planned and implemented. No security measure could be identified.

After clearly describing the risk impact and likelihood, the researchers conducted the risk probability and impact analysis. The risks analysed in this study were collected from the research participants and were identified and categorised in Section 2. The following section illustrates the cyberrisk impact and risk probability in the SME sector in SA.

#### 7.4.4 Risk Consequence and Scoring

Table 7-26 shows the qualitative values, which are the risk likelihood values ranging from rare, unlikely to happen, moderate chance of occurring, more than likely to happen to certain to happen. The table also shows the quantitative values, which include the risk likelihood rating between 1 and 5 and the corresponding risk score, which ranges from 3% to 100%/ The risk consequence has values from 1 to 5, where its values carry a risk description which is negligible, minor, moderate, major and severe.

**Table 7-26: Risk likelihood, likelihood score and the risk consequences**

Qualitative values Likelihood	Quantitative values		Risk consequence	
	Rating	Likelihood score	Value	Description
Rare	1	3%	1	Negligible
Unlikely to happen	2	4-20%	2	Minor
Moderate	3	21-50%	3	Moderate
Likely to happen	4	51-79%	4	Major
Certain to happen	5	80-100%	5	Severe

**Table 7-27** shows the risk scoring and the criteria used to calculate the final risk rating based on the risk consequence multiplied by the risk probability. When the output of the risk consequence and the

probability amounts to a range of 1 to 5, the risk scoring becomes 1 and the final risk rating becomes minor. At the same time, if the risk consequence and probability fall into the 6 to 10 range, then the scoring is 2 and the final scoring becomes low. So, for every risk consequence and the probability, there is a corresponding risk score and final risk rating, as shown in Table 7-27.

Table 7-27: Risk scoring

Consequence*Probability	Risk scoring	Risk rating
1-5	1	Negligible
6-10	2	Minor
11-15	3	Moderate
16-20	4	Major
21-25	5	Severe

## 7.5 RISK EVALUATION

This phase is used to support operational decisions by comparing the risk analysis results with the established risk criteria to determine the appropriate course of action. The study used the matrix to identify levels for different cyberrisks.

### 7.5.1 Matrix Identifying Levels for Cyberrisks

As described earlier, some cyberrisks can be harmful to any business. The cyberrisk harm depends on the risk impact and probability of risk at any business.

Table 7-28 shows a 5\*5 risk matrix of the likelihood and impact of cyberrisk to determine the risk score that categorises the risks as low, medium and high. While levels for the risk probability are rare, unlikely, possible, will occur and certain, the impact levels range from deficient, low, medium, high and very high. The intersection of the horizontal and vertical lines determines the actual level of risk, which could be negligent, minor, moderate, major, or severe. The risk probability and impact matrix illustrate the values and ratings determining the overall risk matrix.

Table 7-28: 5\*5 Risk Probability and Impact Matrix

Risk probability	Risk Impact				
	1 Negligible	2 Minor	3 Moderate	4 Major	5 Severe
1 Rare	1 Negligible	2 Negligible	3 Negligible	4 Negligible	5 Negligible
2 Unlikely Could occur	2 Negligible	4 Negligible	6 Minor	8 Minor	10 Minor
3 Possible Might occur	3 Negligible	6 Minor	9 Minor	12 Moderate	15 Moderate
4 Will Occur Likely to occur	4 Negligible	8 Minor	12 Moderate	16 Major	20 Major
5 Certainly Expected	5 Negligible	10 Minor	15 Moderate	20 Major	25 Severe

## 7.5.2 Application of the Probability/Impact (P-I) Rating

Even though the study gathered so much information, this section focuses only on the probability and impact risk rating, translated as the Risk rating = Risk impact \* Likelihood. Different risk categories are thoroughly explained using the probability risk measure and its impact on producing the risk value. While Table 7-25 defines and describes the risk probability values, Table 7-24 defines the risk impact values. Each probability and impact value demonstrates some level of vulnerability of the business, system, information and personnel. This section's probability and impact rating is based on the identified cyber risk categories: devices and technical systems, technological risks and malware, phishing and network, human factors and policies and guidelines.

### 7.5.2.1 Technical, systems and the device's risk scores

Table 7-29 shows the risk category, the item and probability analysis and its impact on determining the risk value. This table presents the devices and technical systems as the risk category that focuses on the risk items, namely: unauthorised access to the buildings, faulty network connectors and transmission media, old equipment and device failure, unauthorised user registration, unauthorised access to data and files, stolen devices and information, and the use of a USB. Each item shown in Table 7-29 has a corresponding risk probability for information analysed and presented in Table 7-25 and risk impact in Table 7-24. Each risk item's risk value (P\*I) is the product of the relevant risk likelihood and impact, where each value informs the final risk scoring level. The final risk score informs the risk control measures that should be applied to each risk item to reduce, mitigate, separate and avoid the risk.

**Table 7-29: Devices and technical systems risk probability, impact and value (Data source: Survey, 2021)**

Risk category	Risk item	Probability	Impact	Risk value (P*I)	Risk score
Devices and Technical Systems	Unauthorised access to rooms or facilities	2	3	6	Minor
	Faulty network connectors and transmission media	2	4	8	Minor
	Old equipment and device failure	1	2	2	Negligible
	Unauthorised user registration	3	5	15	Moderate
	Unauthorised access to data and files	4	5	20	Major
	Stolen devices and information	5	5	25	Severe
	Use of USB	5	5	25	Severe

### 7.5.2.2 Technological and malware risk values

Table 7-30 presents the technological and malware category with risk items which are unauthorised access to the software, outdated antivirus and antispyware, malware (viruses, worms, Trojan), accidental installation of unsecured applications, denial of service and network downtime, hardware and software failure as well as the use of a USB. Each of these risk items carries a risk probability and

the risk impact is defined in Table 7-25 and Table 7-24 to calculate the final risk score. The final risk score is defined in Table 7-27. So the higher the risk score, the more vulnerability it causes.

**Table 7-30: Technological/Malware risk probability, impact and value (Data source: Survey, 2021)**

Risk category	Risk item	Probability	Impact	Risk value	Risk score
Technological/ Malware Risks	Unauthorised access to software	3	4	12	Moderate
	Outdated antivirus and antispymware	4	3	12	Moderate
	Malware (viruses, worms, Trojan)	4	4	16	Major
	Accidental installation of unsecured applications	4	4	16	Major
	Denial of service and network downtime	3	3	9	Minor
	Hardware and software failure	2	2	4	Negligible
	Use of USB	4	3	12	Moderate

### 7.5.2.3 Phishing and network risk values

Table 7-31 shows the phishing and network risk category and related items identified in Table 7-20. Each identified risk item is calculated to produce the risk value that informs the main risk control measures to be proactively deployed to reduce and avoid the risk with their consequences. The recorded risk probability is defined in Table 7-26 and the risk impact is explained in Table 7-25. So the risk value is the result of both the risk probability and the risk impact of the fraud or stealing information, denial of service and network downtime, hardware and software failure, lack of data confidentiality, data integrity and accidental installation of insecure applications and systems.

**Table 7-31: Phishing and network risk probability, impact and value (Data source: Survey, 2021)**

Risk category	Risk item	Probability	Impact	Risk value	Risk score
Network and phishing	Fraud or stealing of information	3	5	15	Moderate
	Accidental installation of unsecured applications	4	4	16	Major
	Denial of service and network downtime	2	3	6	Minor
	Hardware and software failure	2	4	8	Minor
	Lack of data confidentiality	3	5	15	Moderate
	Lack of data integrity	3	5	15	Moderate

### 7.5.2.4 Human factors risk values

The human error category is presented in Table 7-32 with its related identified risk items, the corresponding risk probability and the impact that results in the risk value. The risk items are listed in

Table 5-32. The recorded risk probability and impact are defined and described in Table 7-25 and Table 7-24. The risk value is also defined in Table 7-27, determining the risk score, which explains SMEs' ultimate level of vulnerability.

**Table 7-32: Human factors risk probability, impact and risk value (Data source: Survey, 2021)**

Risk category	Risk item	Probability	Impact	Risk value	Risk score
Human factors	Unauthorised access to data and files	4	5	20	Severe
	Unauthorised access to devices	3	4	12	Moderate
	Outdated antivirus and antispyware	4	5	20	Severe
	Faulty network connectors and transmission media	2	3	6	Minor
	Old equipment and device failure	2	3	6	Minor
	Malfunctioning of the system or network	3	4	12	Moderate
	Open wireless network	3	4	12	Moderate
	Human errors	5	5	25	Severe
	Use of incorrect password criteria	4	5	20	Severe
	Fraud or stealing of information	3	5	15	Moderate
	Regular system and application failure	3	4	12	Moderate
	Unauthorised modification, deletion, loss of data and information	4	5	20	Severe
	Denial of service and network downtime	3	4	12	Moderate
	Hardware and software failure	3	4	12	Moderate
	Bad management	4	5	20	Severe
	Misconfiguring the device	3	5	16	Major
	Poor delivery of outsourced IT services	3	3	9	Negligible
	Use of USB	3	4	12	Negligible
	Lack of integrity	4	5	20	Severe
Lack of data confidentiality	4	5	20	Severe	

#### 7.5.2.5 Policies/Guidelines risk values

Table 5-33 shows the category of the policies and guidelines with their cyberrisk items to calculate the value of the risk in terms of the likelihood of risk and the impact. The related risk items listed in Table 5-33. The risk probability values are based on Table 7-24 and their risk impact is defined in Table 7-25. So, the value of the risk is the outcome of the probability and impact of the risk. The risk values determine the risk score that helps to determine the appropriate security measures that will proactively improve the safety and security of the business.

**Table 5-33: Policies/Guidelines risk probability, impact and risk value (Data source: Survey, 2021)**

Risk category	Risk item	Probability	Impact	Risk value	Risk score
Policies and guidelines	Unauthorised user registration	4	5	20	Major
	Unauthorised access to data and files	5	5	25	Severe
	Unauthorised access to devices	4	4	16	Major
	Malfunctioning of the system or network	3	5	15	Moderate
	Open wireless network	3	3	9	Minor
	Human errors	4	5	20	Major
	Use of incorrect password criteria	5	5	25	Severe
	Regular system and application failure	5	5	25	Severe
	Unauthorised modification, deletion, loss of data and information	5	5	25	Severe
	Denial of service and network downtime	3	4	12	Moderate
	Hardware and software failure	2	4	8	Negligible
	Bad management	4	5	20	Major
	Misconfiguring the device	4	5	20	Major
	Poor delivery of outsourced IT services	3	4	12	Moderate
	Use of USB	4	4	16	Major
Lack of data confidentiality	5	5	25	Severe	
Lack of data integrity	5	5	25	Severe	

### 7.5.3 Risk Classes

Generally, risks are categorised according to the classes ranging from Class I to Class IV. Table 7-34 presents the definition of each class and the related identified cyberrisks to rate and assess the level of collected risks experienced by the SME sectors. Each risk class has a corresponding definition and a risk-related identified risk number, as illustrated in Table 7-20. Class I presents a collection of the identified risks which are acceptable impacts. Class II presents acceptable risks while the service is used; threats should be monitored to observe any abnormalities. Class III presents an unacceptable risk; mitigation measures should be considered based on different scenarios. In Class IV, measures to reduce risks must be implemented for extremely high risks. Classes I to IV have a risk impact ranging from negligible to severe. Each class has a group of related cyberrisks and attacks belonging to the severity level of the risk. Eight risks belong to both Class I and Class II. Class III has 18 related risks and class IV has 16 related risks.

**Table 7-34: Definition of risk classes (Data source: Survey, 2021)**

Risk classes	Definitions	Collected risk item
<b>Class I</b>	Acceptable risk	[2,5,7,8,9,10,21,25]
<b>Class II</b>	Acceptable risk. While the service is used, threats should be monitored to observe any abnormalities.	[2,5,7,8,9,10,21,25]
<b>Class III</b>	Risk is not acceptable. Based on different scenarios, mitigation measures should be considered.	[1,12,2, 3,4,5,8,9,10,11, 13,14,15,11,22,23,24,25]
<b>Class IV</b>	Extremely high risk. Measures to reduce risks must be implemented	[3,4,6,15,16,17,18,19,20, 21,22,23,24,25,26,27]

### 7.5.4 Vulnerability Assessment

At SMEs, vulnerability assessment is performed to evaluate the cyberrisk likelihood of a cyberthreat. The study used the qualitative approach to categorise cyber vulnerability into low, moderate or high. It considers the SME assets, threats, mitigation strategies and impact. This study determines the vulnerability categorisation of the SME system where the metrics were identified in Table 7-20 to be assessed, as shown in Table 7-35. This matrix was analysed and categorised based on the interrelated threat effects for the devices and technical systems, technological risks and malware, human factors, phishing or network, and policies and guidelines. Each vulnerability category is grouped and arranged based on its severity in the system ranging from low, moderate to high, as can be seen in Table 5-35.

**Table 7-35: Matrix that influences vulnerability (Data source: Survey, 2021)**

Threat matrix	SME cybersecurity vulnerability		
	LOW	MODERATE	HIGH
Devices/ Technical systems	[2]	[8,9]	[3,4,6,25]
Technological/Malware	[7]	[1,1,25]	[16,17,20, 21]
Human factors	[5,7,8,9]	[10,11,12,22,23,24,25, 3,21]	[3,15,18,19,20,26,27]
Phishing/network		[15]	[17,18,20,21,26,27]
Policies and guidelines	[10, 21,25]	[3,4,5,2,11,12,14]	[25,18,24,19,20,27,22,23,26]

### 7.5.5 Summary of Gathered Risks

Table 7-36 summarises the identified risks belonging to different categories, with their forms of attack, risk event, asset, security principle, risk cause, risk impact and the risk consequence. The risk categories present related and grouped risks according to their nature in the business sector. The recorded risk categories are adopted from Table 7-21. The cyberrisk categories are devices and technical systems-related risks, technological risks and malware, including phishing and network, and human factors, which consist of planned and unplanned risks. The listed cyberrisks are triggered by different cyberthreats and attacks relating to the business resources, such as the network, technical systems, technologies, people, rules and guidelines that directly or indirectly affect various business assets.

All these gathered risks affect the security principles, which are confidentiality, integrity and availability, abbreviated as (CIA). These three security principles form part of the information security training that minimises the potential of security risks. So, every cyberrisk is motivated and specific, which could be planned or unplanned. The planned risks could be caused by unauthorised access or intentional cybercriminal acts, while the unplanned risks could be human or employee-generated based on their computer literacy level. Regardless of their sources, risks result in a risk event that carries either a positive or a negative impact and a consequence for the business system. Every risk at the business carries a certain impact and consequence. If the risk is negative, the impact is also negative; if the risk is positive, then the impact is also positive. A negative risk poses negative consequences, as presented in Table 7-36.

**Table 7-36: Description of collected cyberrisks table (Data source: Survey, 2021)**

Risk Category	Form of attack	Asset	Security principle	Risk cause	Risk event	Risk Impact	Risk consequence
Device or technical risks	<ul style="list-style-type: none"> <li>• Hardware &amp; software failure</li> <li>• Human error</li> <li>• Malicious attacks</li> <li>• Old equipment</li> <li>• Network downtime and denial of service</li> </ul>	<ul style="list-style-type: none"> <li>• End devices</li> <li>• Files</li> <li>• System</li> </ul>	<ul style="list-style-type: none"> <li>• Availability</li> <li>• Confidentiality</li> <li>• Integrity</li> </ul>	<ul style="list-style-type: none"> <li>• Human actions</li> <li>• Ignorance - poor decision-making</li> <li>• Lack of employee skills</li> <li>• No device encryption</li> <li>• Lack of device management</li> </ul>	<ul style="list-style-type: none"> <li>• Theft, loss or robbery</li> <li>• Third-party involvement</li> <li>• Malware attack</li> <li>• Unauthorised access to devices</li> </ul>	<ul style="list-style-type: none"> <li>• Poor business growth</li> <li>• Fraudulent acts</li> <li>• Lack of client trust</li> <li>• Loss of intellectual property</li> <li>• Poor economic growth</li> </ul>	<ul style="list-style-type: none"> <li>• Loss of information</li> <li>• Lost or stolen devices</li> <li>• Denial of service</li> <li>• Poor performance and economic growth</li> <li>• Loss of clients</li> <li>• A slow or unusable computer.</li> </ul>
Malware or technological and phishing risks	<ul style="list-style-type: none"> <li>• Cybersecurity incidents such as <b>malware</b></li> <li>• Cyberattacks,</li> <li>• Password theft</li> <li>• <b>Phishing</b></li> <li>• Device encryption cracking and data access problem</li> <li>• Misconfiguration of the device</li> <li>• Poor implementation of the device security measures</li> </ul>	<ul style="list-style-type: none"> <li>• Network</li> <li>• Device</li> <li>• Websites</li> <li>• Third parties</li> </ul>	<ul style="list-style-type: none"> <li>• Availability</li> <li>• Confidentiality</li> <li>• Integrity</li> </ul>	<ul style="list-style-type: none"> <li>• Human errors</li> <li>• Unsecured networked systems</li> <li>• Lack of cybersecurity guidelines</li> <li>• Network and software vulnerabilities</li> <li>• Improper security architecture</li> </ul>	<ul style="list-style-type: none"> <li>• Worms, Trojan, Viruses and spyware)</li> <li>• Phishing scams</li> <li>• Unrestrained web browsing</li> <li>• Bad password</li> <li>• Human errors</li> </ul>	<ul style="list-style-type: none"> <li>• Malfunctioning of servers and computers</li> <li>• Unexpected system and network failure</li> <li>• Limited access to resources</li> <li>• Compromised system and information security, privacy and safety lead to data breaches</li> </ul>	<ul style="list-style-type: none"> <li>• Identity theft.</li> <li>• Deletion, theft and corruption of data.</li> <li>• Denial of service</li> <li>• Fraud – freeze access until payment is made</li> <li>• Captures private information</li> <li>• Loss of reputation;</li> </ul>
		<ul style="list-style-type: none"> <li>• Email</li> <li>• Network</li> <li>• Servers</li> </ul>	<ul style="list-style-type: none"> <li>• Availability</li> <li>• Confidentiality</li> <li>• Integrity</li> </ul>	<ul style="list-style-type: none"> <li>• Social engineering attacks</li> <li>• Phishing, intrusion and malware attacks</li> <li>• Password attacks</li> <li>• Malware such as spyware, viruses, worms and ransomware</li> <li>• Software downtime and regular pop-up messages</li> <li>• Inadequate software security</li> <li>• Outdated software and applications</li> </ul>	<ul style="list-style-type: none"> <li>• Vishing</li> <li>• Deceptive Phishing</li> <li>• Spear phishing</li> <li>• Whaling</li> <li>• Smishing</li> <li>• Pharming</li> </ul>	<ul style="list-style-type: none"> <li>• Financial loss</li> <li>• Bad reputation</li> <li>• Loss of client trust</li> <li>• Declined production and business growth</li> </ul>	<ul style="list-style-type: none"> <li>• Stealing or revealing sensitive data (login details, credit card information)</li> <li>• Unauthorised instalation of malware software</li> <li>• Freezing systems</li> <li>• Loss of identity</li> <li>• Unauthorised purchases</li> </ul>
Human factors	<ul style="list-style-type: none"> <li>• Poor decision-making</li> <li>• Lack of management involvement</li> <li>• Work overload &amp; stress</li> <li>• Ineffective access &amp; resource management.</li> <li>• Outsourced IT services</li> <li>• Poor configuration management</li> <li>• Malicious and accidental activities</li> <li>• Careless handling of data</li> </ul>	<ul style="list-style-type: none"> <li>• Employees</li> <li>• Files</li> <li>• Websites</li> <li>• Third parties</li> </ul>	<ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Integrity</li> </ul>	<ul style="list-style-type: none"> <li>• Planned and accidental actions</li> <li>• Ignorance - poor decision-making</li> <li>• Lack of skills</li> <li>• No management involvement or cybersecurity personnel</li> </ul>	<ul style="list-style-type: none"> <li>• No clear guidelines for cybersecurity procedures</li> <li>• Incomplete configuration management</li> <li>• Unauthorised use of access rights</li> <li>• Lack of skills</li> </ul>	<ul style="list-style-type: none"> <li>• Loss of information</li> <li>• Lack of client trust</li> <li>• Financial loss</li> <li>• Loss of client trust</li> <li>• Declined production and business growth</li> </ul>	<ul style="list-style-type: none"> <li>• Lack of a cybersecurity policy</li> <li>• Take your own device to work</li> <li>• Physical security</li> <li>• Identity theft, fraud.</li> <li>• Deletion, theft and corruption of data.</li> </ul>
		<ul style="list-style-type: none"> <li>• Adherence to policies and guidelines</li> </ul>	<ul style="list-style-type: none"> <li>• Network</li> <li>• Password</li> <li>• Device</li> <li>• Email</li> <li>• System</li> </ul>	<ul style="list-style-type: none"> <li>• Poor compliance with guidelines and procedures</li> <li>• Low-security awareness and understanding</li> <li>• Poor password creation and management</li> </ul>	<ul style="list-style-type: none"> <li>• Message</li> <li>• Email</li> </ul>	<ul style="list-style-type: none"> <li>• Mistakes leading to a significant data breach</li> <li>• Ignorance can lead to legal fines, loss of client trust</li> <li>• Bad Reputation</li> </ul>	<ul style="list-style-type: none"> <li>• Data breaches</li> </ul>



## 7.6 QUANTITATIVE RISK ANALYSIS

In contrast to qualitative risk analysis, quantitative risk analysis assigns money values that are independently objective to risk assessment elements to assess the potential of a loss. Owing to its objectivity, the quantitative risk analyses bring out the direct costs because of their objectivity in their assessment, which fits all the business sector's needs and situations. When performing the quantitative risk analysis, it is important to consider the potential of loss relating to the delayed process or destruction of the service. This will help estimate the risk probability of failure or occurrence, which could also help determine the annual loss of expectancy. So, for every risk calculated, appropriate and proactive measures should be deployed to reduce, avoid, separate and mitigate risks, even though these measures will have different cash flow scenarios.

For example, phishing and network-related risks need different strategies to system or device-related risks. The network may require an extensive security upgrade which consists of a firewall that filters traffic on the network. The firewall could also have an intrusion-detection system, which might be expensive and potentially have an extended cash-flow duration. Alternatively, there should be a need to constantly hire a specialised security consultant who will regularly assess, enforce and monitor the services on a timely basis. This measure would be covered in a short period, even though it would still cost the business money. Even though some industries use the quantitative cyberrisk assessment, Shukla et al., (2022) state that financial and insurance companies most commonly adopt quantitative cyberrisk analyses. Insurance and financial institutions often assess the risk likelihood and its frequency in their institutions. Lo and Chen (2012) explain that many organisations commonly use statistical and mathematical tools to organise related risks to determine the risk probability and damage amount, which affects the overall business assets. The aim of using the business's own statistical and mathematical tools is to define and differentiate between acceptable and unacceptable levels of risk (Nosworthy, 2000).

Shukla et al., (2022) explain that the direct or indirect costs of the risk are measured based on the values assigned to business assets, processes, risk impact and the costs to recover the damage. In quantitative risk management, thorough planning and preliminary work are required to collect all the elements' precise values. These elements present control effectiveness, asset values, threat frequency and control cost (Lo & Chen, 2012). Feng and Li (2011) explain that risk analysis and assessment expose the risk as the threat likelihood and the expected loss. The actual risk can be estimated using a numeric value that determines the risk likelihood and impact in the business sectors (Smit & Watkins, 2012). However, the effects can be time and financial (Van Niekerk, 2017). This study has drafted the priority values relating to the business assets and their values, as shown in Table 7-37.

The asset evaluation will be used with quantitative risk assessment techniques. The analytical, probabilistic and unconventional quantitative cybersecurity risk management analysis methods will be discussed below.

## **7.6.1 Quantitative Analytical, Probabilistic and Unconventional Techniques**

Different analytical methods can be adopted in quantitative analysis. Generally, sensitivity analysis is widely used to determine the variation in values of the independent variables directly affecting the dependent variables. This study used the sensitivity analysis and scenario analysis described below. These two quantitative analytical methods are used simultaneously to predict the cyberrisks in the small business sector in SA. The economic and financial sectors focus on predicting the share prices to determine the interest-related rates (Aldhamari et al., 2022).

Scenario analysis pays more attention to the effect of risk in a certain situation. This analytical method uses specific information for certain scenarios to change the model's variables. This ultimately produces an outcome for real-life cases. An example would be the sudden global Covid-19 pandemic which quantified the cyberrisks in all institutions or a crash of the market stock and a change owing to the regulations in certain sectors. Section C presented the use of AgenaRisk simulation software to simulate and present five scenarios relating to cyberrisks at SMEs. These scenarios include network and phishing, human factors, technological risks and malware, guidelines and policies and devices and technical systems. These analytic methods are presented below.

### **7.6.1.1 Sensitivity Analysis using Conditional Probability Tables and Tornado graphs**

This study used the Bayesian network tools with the AgenaRisk package to simulate the potential cybersecurity risk probabilities and their impacts in the business space. The Bayesian model (BM) is part of the graphical probabilistic models that use the Bayesian inference analysis. The detailed demonstration of the cyberrisks in the SME sectors is clearly described and accounted for in Section C. This section demonstrates a sensitive analysis of the different cyberthreats and attacks which result in different cyberrisks. This section only presents the sensitivity analysis, which challenges the reliability, difference and significance of the assumptions to address the 'what if' analysis. The sensitivity analysis presents the quantitative technique for determining variables that have a greater impact on risk (Cox, 2008).

The Project Management Institute (PMI) (2013) states that the variables estimate risks with potential impact and determines the changes in objectives and uncertainties that are correlated, along with the effect of each element on the objectives. They also provide an assessment of the likelihood that project decisions will be affected by risk measures, resulting in the desired outcome. In general, only scenarios with the greatest risk are taken into account in the sensitivity analysis. These analyses can be lengthy and expensive, which is often why qualitative analyses such as the likelihood and impact matrix identify the risks of greatest concern (Iloiu & Csiringa, 2009).

This study used the AgenaRisk package with the Bayesian Network tools to conduct an extensive sensitivity analysis of the different scenarios to check the sensitivity of the answers against the technique and its related

parameters. The different cases are presented in detail in Section C. This section of the study thus provided a hypothetical analysis of these cases. This work analysed the sensitivity of the AgenaRisk package in isolation, in that if numerous interrelated parameters relate to the answer, then the researcher only considers the effect of one parameter at a time. For the tool's effectiveness, the researcher determined the technique's sensitivity to the Conditional Probability Tables (CPT).

The sensitivity analysis communicates data and outcomes, understanding the link between the input and output variables while identifying sensitive variables. It then helps to make assumptions that allow decision-making and examines the amount of risk in given scenarios. The tornado graphs are generated based on the study's scenario analysis presented in Section C. In addition, the sensitivity analysis and tornado graphs are performed on key risk categories which are: human factors, devices and technical systems, technological risks and malware, phishing and networks, and policies and guidelines. The identified cyberthreats and attacks are presented below

#### 7.6.1.1.1 The human factor: Planned and unplanned attacks' sensitivity analysis

Figure 7-67 shows the risk likelihood for the planned attacks. The risk likelihood ranks from low, medium to high, while the planned attack has Boolean values (true and false). When the risk likelihood is true, it gets a high rating of the risk likelihood. When the risk likelihood is false, then the likelihood is low.

		Planned Attack	
		False	True
Risk Likelihood	High	0.336	0.664
	Medium	0.952	0.048
	Low	0.672	0.328

**Figure 7-67: Risk likelihood for planned attacks (Data source: Survey, 2021)**

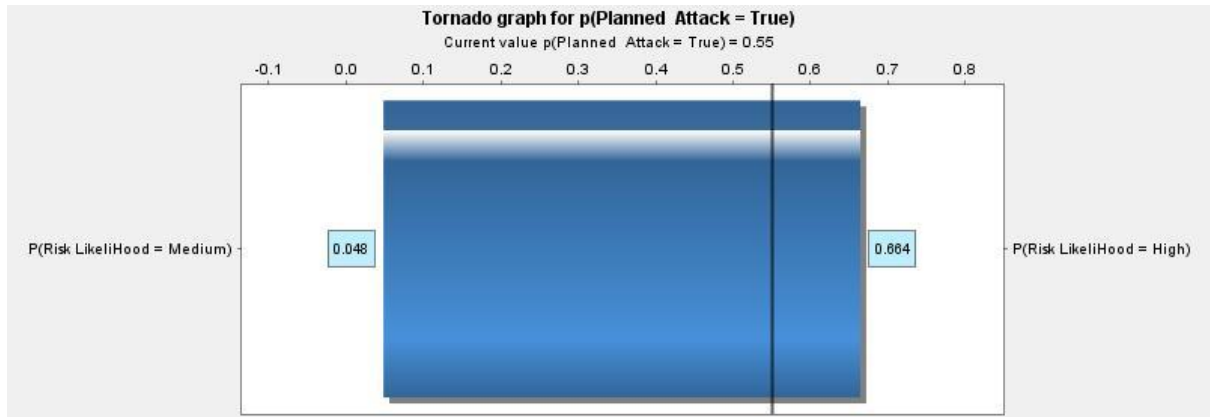
Figure 7-68 shows the sensitivity analysis for the unplanned attacks, which are actions performed by insiders. These attacks could be activities that are the result of poor decision-making with regard to the system of an ignorant, extremely tired and computer illiterate employee. Unplanned attacks hold the Boolean values (true and false) while the risk likelihood ranks from low, medium to high. The risk likelihood value becomes high when the planned attack is true and the risk likelihood becomes low when the planned attack is false.

		Risk Likelihood		
		High	Medium	Low
Unplanned Attack	False	0.563	0.427	0.01
	True	0.978	0.018	0.004

**Figure 7-68: Risk likelihood for unplanned attacks (Data source: Survey, 2021)**

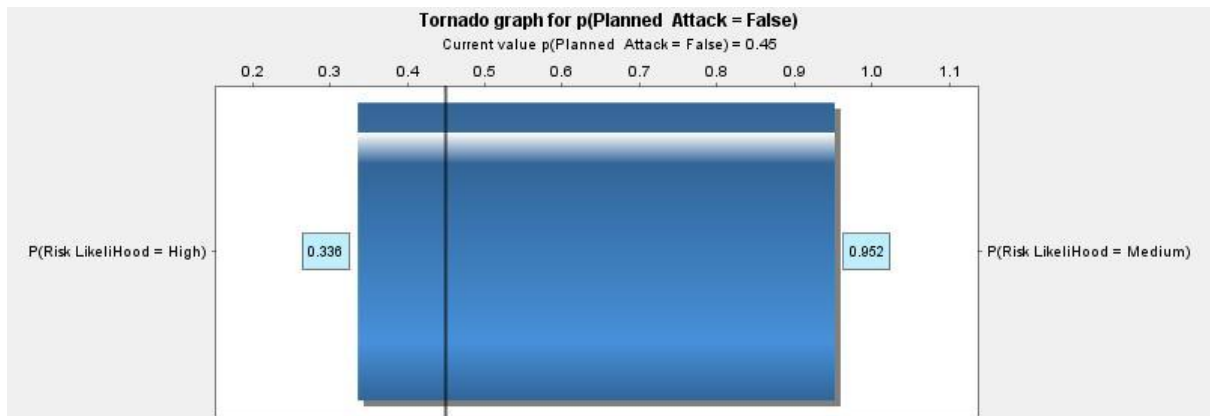
### 7.6.1.1.2 Tornado graphs for human factors: Planned and unplanned attacks

The Tornado chart was used to evaluate the sensitivity analysis of planned and unexpected human-induced attacks. Figure 7-69 shows the planned attack that carries a true value with medium (0.048) and high risk (0.664) likelihood.



**Figure 7-69: Tornado graph for planned attack = True**

Figure 7-70 shows the false planned attack with high (0.336) and medium (0.952) risk likelihood.



**Figure 7-70: Tornado graph for planned attack = False**

### 7.6.1.1.3 Conditional Probability Table for Devices and Technical Systems

This section presents the conditional probability table for the devices and technical systems, which has the threat level ranked high, medium and low, while the data breach has two Boolean states, which are true and false. Figure 7-71 shows the CPT for devices and technical systems with a false data breach when the threat level is high (0.007), medium (0.347) and low (0.646). The data breach is true when the threat level is high (0.631), medium (0.311) and low (0.058).

		Threat Level		
		High	Medium	Low
Data breach	False	0.007	0.347	0.646
	True	0.631	0.311	0.058

Figure 7-71: CPT for device and technical systems (Data source: Survey, 2021)

#### 7.6.1.1.4 Tornado graphs for devices and technical systems

The three Tornado graphs present different rankings of the threat levels, which are high, medium and low and two Boolean values (true and false) for the data breach. The Tornado technique examined the sensitivity analysis for the device and technical systems-related risks.

Figure 7-72 shows the Tornado graph for a false (0.007) data breach and (0.631) threat level.

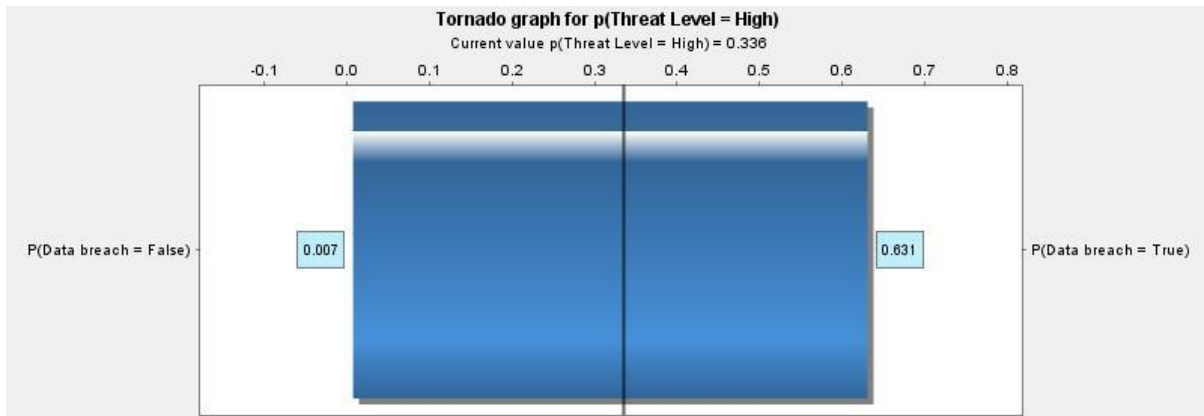


Figure 7-72: Tornado graph for false data breaches and high threats level

Figure 5-73 shows the Tornado graph for a true (0.311) data breach and (0.347) medium threat level.

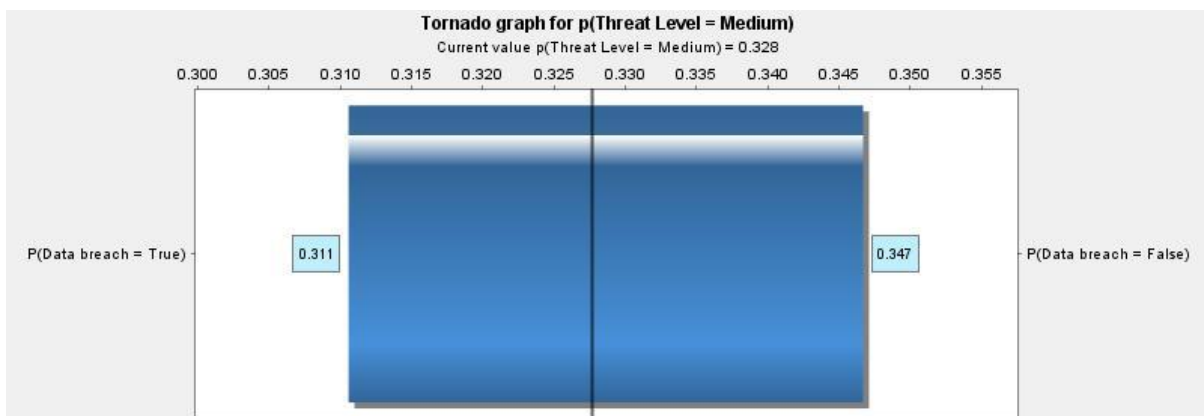


Figure 5-73: Tornado graph for true data breach and medium threats level

Figure 7-74 shows the Tornado graph for a true (0.058) data breach and (0.648) low threat level.

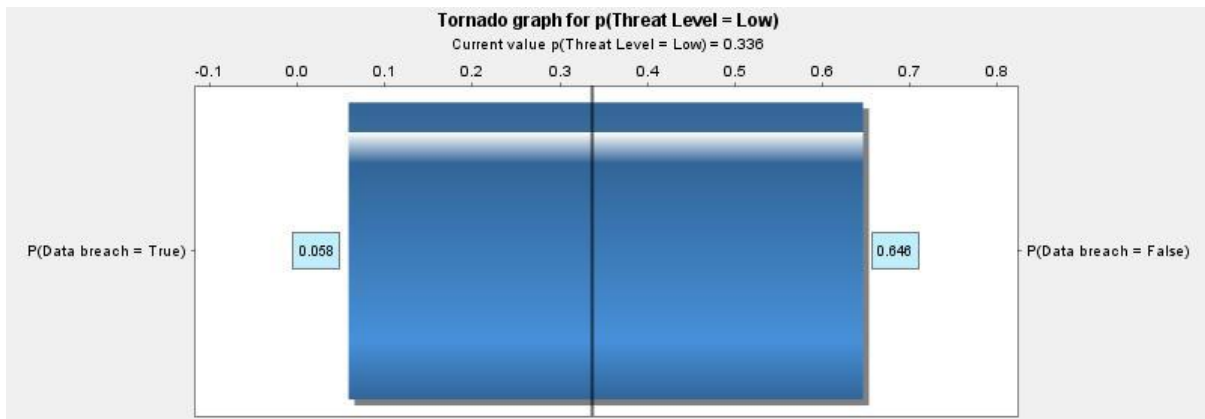


Figure 7-74: Tornado graph for true data breach and low threats level

### 7.6.1.1.5 Conditional Probability Table for Malware and Technological Risks

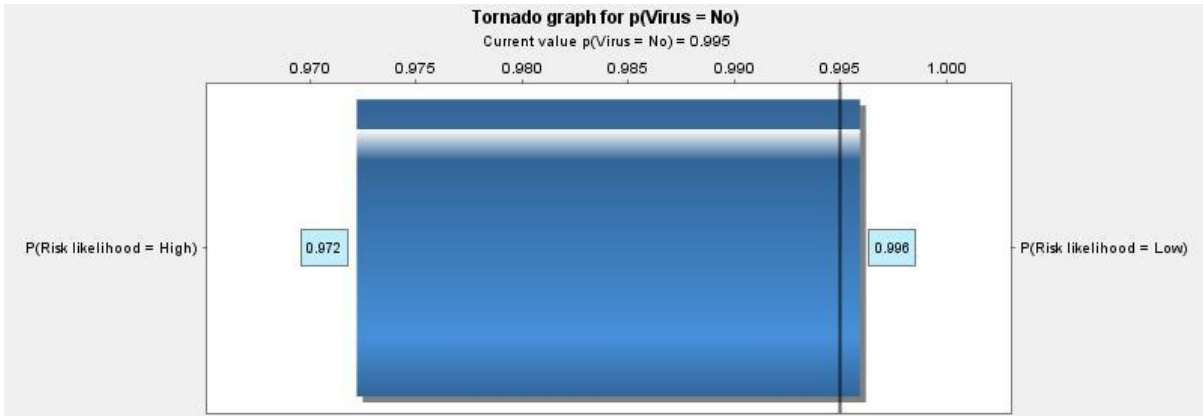
Conditional probability tables were used to assess the sensitivity analysis for the virus as malware. The virus has two Boolean values, which are yes and no, while the risk likelihood is ranked high, medium and low. As shown in Figure 7-75, when the risk likelihood is high and the virus is no, then the output is (0.972). While the virus is yes, then the output is (0.028). When the risk likelihood is medium, then the outputs are (0.985) for a no virus and (0.015) for a yes. When the virus is no, the risk likelihood is (0.096) and when it is yes, the risk likelihood is 0.004.

		Virus	
		No	Yes
Risk likelihood	High	0.972	0.028
	Medium	0.985	0.015
	Low	0.996	0.004

Figure 7-75: Virus CPT (Data source: Survey, 2021)

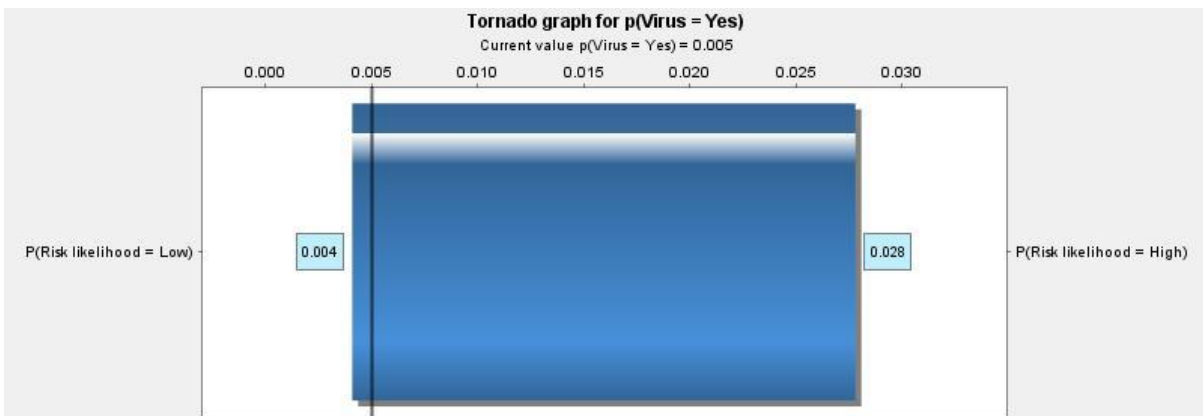
### 7.6.1.1.6 Tornado Graphs for Malware and Technological Risks

There are two Tornado graphs generated for the malware and technological risks. These graphs are for the presence of the virus as a malware attack and when there is no virus. The outputs for the possible states are illustrated on each graph. Figure 7-76 shows the Tornado graph for no virus, where 0.972 presents the high-risk likelihood and 0.995 is for a low-risk likelihood.



**Figure 7-76: Tornado graph for no virus**

Figure 7-77 shows the Tornado graph for when there is a virus as malware, where 0.004 presents the low-risk likelihood and 0.028 is for a high-risk likelihood.



**Figure 7-77: Tornado graph for yes virus**

#### 7.6.1.1.7 Conditional Probability Table for Phishing and Network

This section presents the sensitivity analysis of phishing and the network conditional probability table. Figure 7-78 shows the phishing and network conditions with the risk impact ranked high, medium, and low, while the risk likelihood is ranked very low, low, medium, high, and very high. A very low-risk likelihood and high-risk impact produce (0.333). A very low-risk likelihood and medium-risk impact produce (0.333). A very low-risk likelihood and low-risk impact produce (0.333). A low-risk likelihood and high-risk impact produce (0.333). A low-risk likelihood and medium-risk impact produce (0.333). A low-risk likelihood and low-risk impact produce (0.333). A medium-risk likelihood and high-risk impact produce (0.333). A medium-risk likelihood and medium-risk impact produce (0.333). A medium-risk likelihood and low-risk impact produce (0.333).

		risk impact		
		High	Medium	Low
Risk Likelihood	Very Low	0.333	0.333	0.333
	Low	0.333	0.333	0.333
	Medium	0.333	0.333	0.333
	High	0.333	0.333	0.333
	Very High	0.333	0.333	0.333

Figure 7-78: Phishing and network CPT (Data source: Survey, 2021)

### 7.6.1.1.8 Tornado Graphs for Phishing and Network

Tornado graphs are presented to demonstrate the variation in terms of the variables for phishing and network category. Three graphs illustrate sensitivity analysis for the risk likelihood and the risk impact that are presented below. Figure 7-79 shows the Tornado graph of the phishing and network with a very low (0.333) risk likelihood and high (0.333) risk impact.

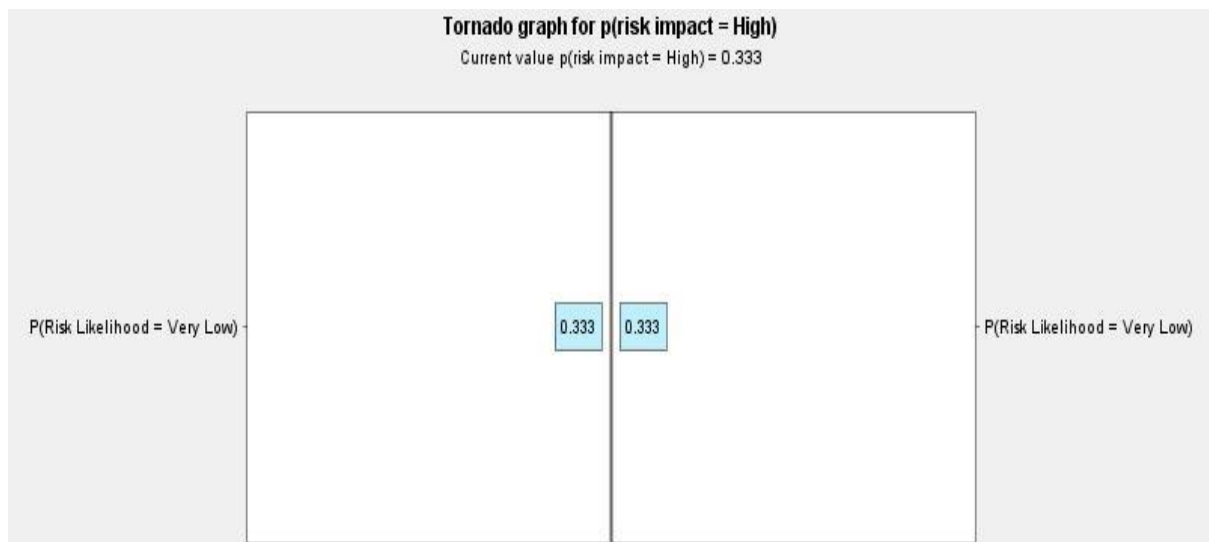
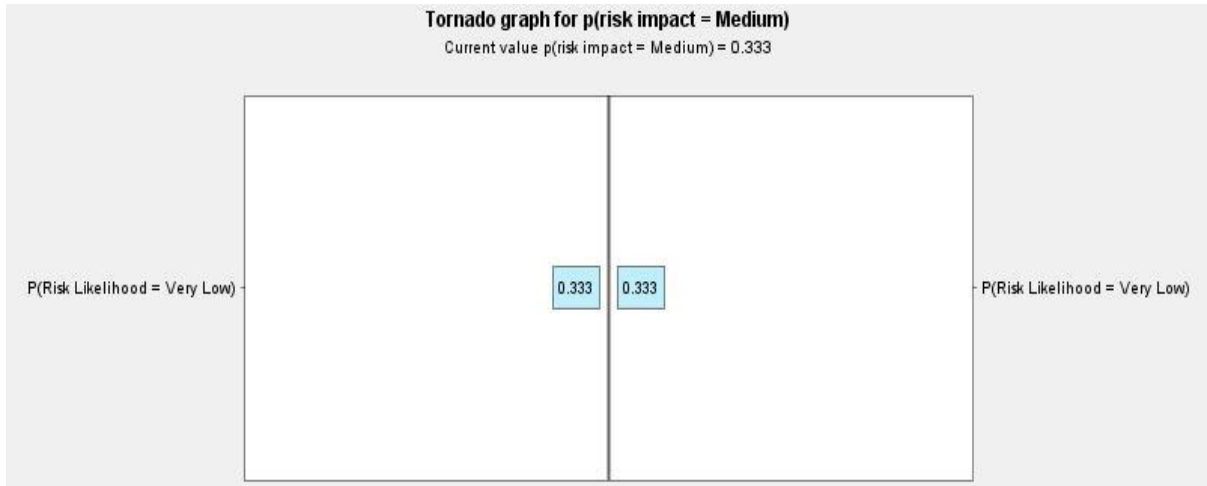


Figure 7-79: Tornado graph for very low-risk likelihood and high impact

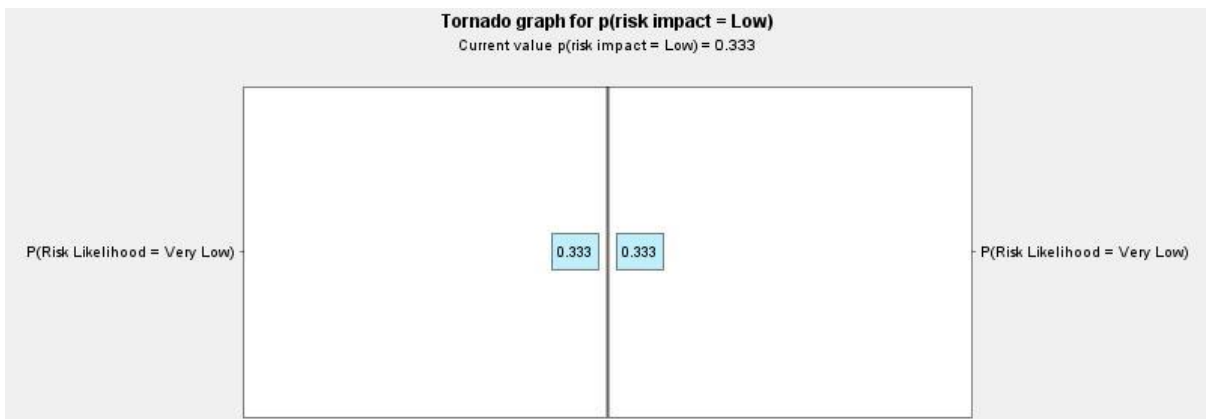
Figure 7-80 shows the Tornado graph of the phishing and network with very low (0.333) risk likelihood and medium (0.333) risk impact.





**Figure 7-80: Tornado graph for very low-risk likelihood and medium impact**

Figure 7-81 shows the Tornado graph of the phishing and network with very low (0.333) risk likelihood and low (0.333) risk impact.



**Figure 7-81: Tornado graph for very low-risk likelihood and low impact**

**7.6.1.1.9 Conditional Probability Table for Lack of Policies and Guidelines**

Figure 7-82 shows the sensitivity analysis through the CPT for the policies and compliance that should be done by business employees and third parties. The level of policy compliance depends on the implementation level, which is ranked from high, medium to low. The policy compliance impact level is also ranked from high, medium to low. For this case, if the policy compliance is low, then the impact level becomes 0.02 for a high rating, 0.08 for a medium rating and 0.9 for a low rating.

		Risk Impact		
		High	Medium	Low
Policies compliance	High	0.02	0.08	0.9
	Medium	0.02	0.08	0.9
	Low	0.02	0.08	0.9

**Figure 7-82: CPT for lack of policies and guidelines (Data source: Survey, 2021)**

### 7.6.1.1.10 Tornado Graphs for Lack of Policies and Guidelines

Tornado graphs for the lack of policies and compliance risk category are presented in this section. This theme produced three vertical graphs demonstrating the impact of policy compliance, which is rated low, medium, and high, with low, medium, and high policy compliance. The outcomes of the analysis are presented in the graphs below. Figure 7-83 shows a Tornado graph for a low (0.9) impact on a high (0.900) policy compliance level.

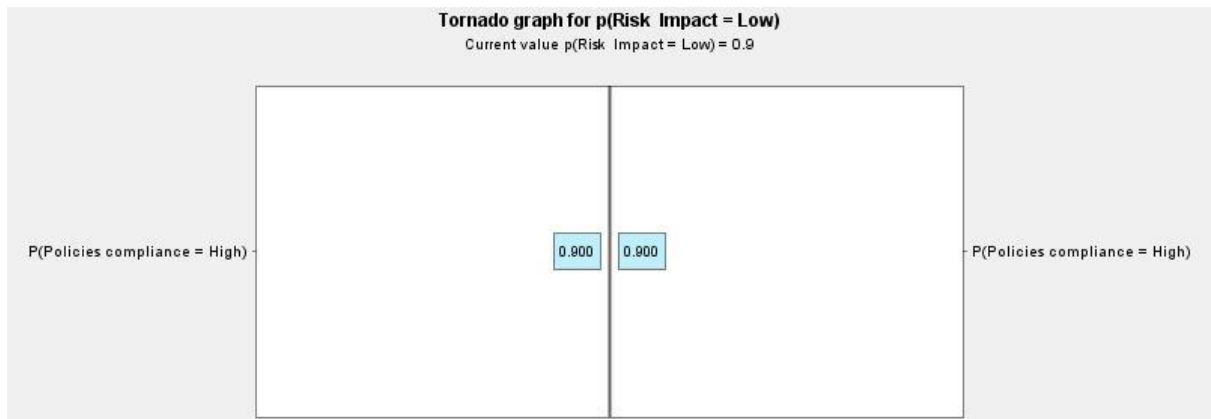


Figure 7-83: Tornado graph for a low impact on a high policy compliance

Figure 7-84 shows the Tornado graph for a medium (0.08) impact on a high (0.080) policy compliance.

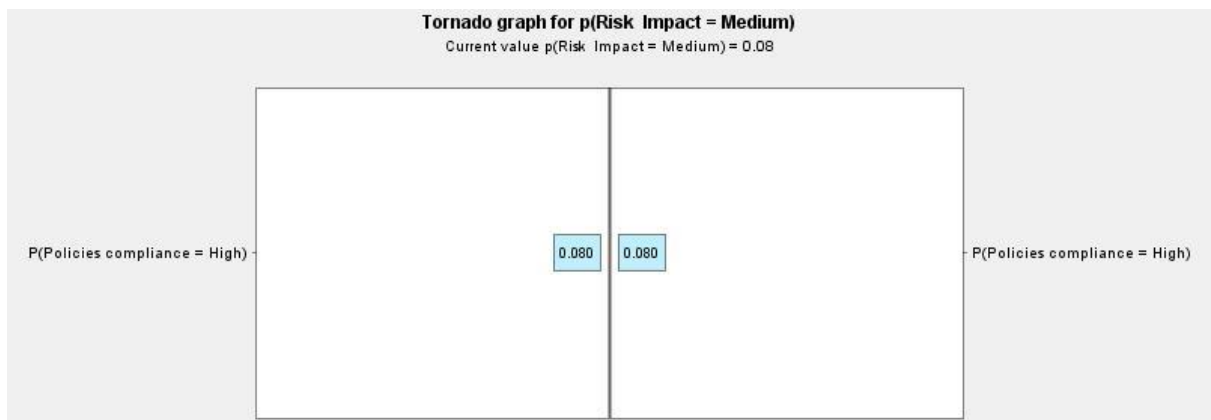
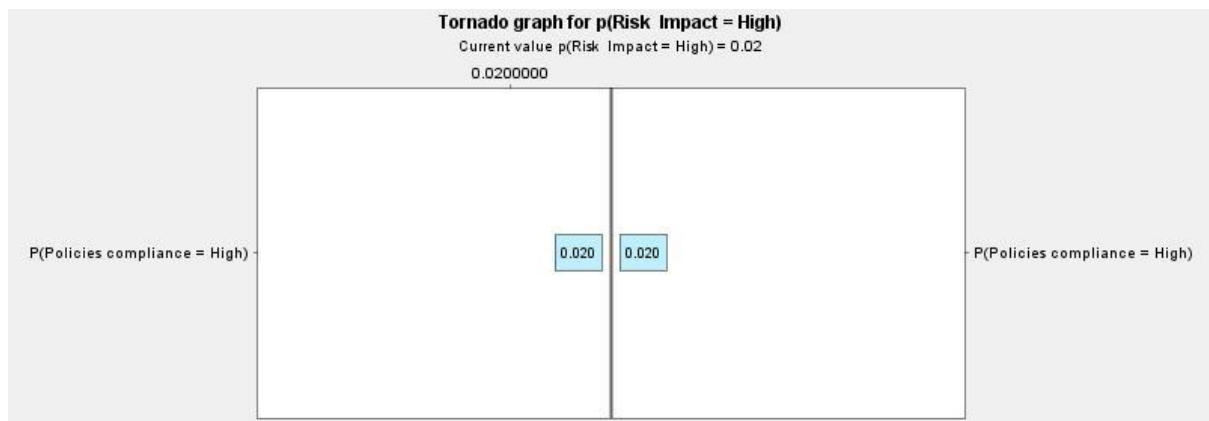


Figure 7-84: Tornado graph for a medium impact on a high policy compliance

Figure 7-85 shows a Tornado graph for a high (0.02) impact on a high (0.020) policy compliance.



**Figure 7-85: Tornado graph for a high impact on a high policy compliance**

The following section presents the expected monetary value technique for different risk categories.

### 7.6.1.2 Expected Monetary Value (EMV)

According to the PMBOK (2017), an EMV is a quantitative analysis or a statistical concept for calculating the outcomes based on the different future scenarios for risks that could or may not occur. Purnomo and Wiguna (2021) describe the EMV as a weighted likelihood of the output, which carries more details about the severity of the risks to prioritise a response plan. EMV also acts as a valuable technique for quantitative risk analysis by predicting threat outcomes of uncertain future risk scenarios, which could yield a negative or positive result (Dash, 2017). EMV is also a mathematical calculation technique that determines the probability of risk and its impact when the probability of risk presents the probability of occurring and the risk impact as the cost of the risk (Metsänen, 2022). The cost value is assigned for each identified risk. This value takes into account both the likelihood and potential implications of the risk event. The formula to calculate the EMV is the probability multiplied by the cost of identified risk, which is denoted as  $EMV = Probability \times Cost\ Impact$ .

Where: P = probability of the risk and CI = Cost impact if the risk occurs.

EMV is a tool used to manage the risk based on the various cyberrisk future scenarios, so in this study, the EMV is calculated based on the collected results and identified risks. The risk scenarios used in this study are based on real-life cases of SMEs facing uncertainties in their future business operations, especially after the Covid-19 Pandemic. This technique is applied to guide risk mitigation for any possible risks and bring insights to future cases. All the discussed techniques are applicable to quantifying the possible cyberrisks at businesses. Therefore, estimating a possibility can be the calculated amount required to determine and control all identified risks (Vivian, 2013). Table 7-37 indicates the values relating to the business's assets as advised by the participants. So the information in Table 7-37 is also used to calculate the EMV for this study. EMV is calculated based on the risk categories, namely devices or technical systems; phishing and network; human factors; malware or technological risks, as well as policies and guidelines.

**Table 7-37: Asset evaluation**

Priority Value	Asset	Asset value
1	Facilities, system and network operation	R100 000
2	Clients' data or information integrity and confidentiality Employee data confidentiality and integrity	R100 000 R100 000
3	Confidentiality and integrity of data management control	R100 000
4	The device, services and application operation and availability	R90 000
5	Lack of policies and guidelines	R70 000

Table 7-38: EMV for devices and technical systems shows EMV calculations for devices and technical systems. The calculation includes the per cent of risk probability as shown in Table 7-25 multiplied by the cost impact in Table 7-24, which is based on the asset values in Table 7-37.

**Table 7-38: EMV for devices and technical systems (Data source: Survey, 2021)**

Risk category	Risk item	Probability %	Cost Impact	EMV
Devices /Technical Systems	Unauthorised access to rooms or facilities	11%	R11 000	R1 210
	Faulty network connectors and transmission media	11%	R11 000	R1 210
	Old equipment or device failure	1%	R4 500	R450
	Unauthorised user registration	55%	R30 000	R16 500
	Unauthorised access to files	55%	R30 000	R16 500
	Stolen devices and information	75%	R32 400	R24 300
	Use of USB	75%	R32 400	R24 300

Table 7-39 shows the phishing and network EMV where the calculation is based on the probability per cent and multiplied by the cost impact (based on the asset value).

**Table 7-39: Phishing and network EMV (Data source: Survey, 2021)**

Risk category	Risk item	Probability %	Cost Impact	EMV
Phishing and Network	Fraud or stealing of information	30%	R20 000	R6 000
	Accidental installation of unsecured applications	55%	R2700	R14 850
	Denial of service and network downtime	11%	R15 000	R1 650
	Hardware and software failure	11%	R11 000	R1 210
	Lack of data confidentiality	75%	R30 000	R22 500
	Lack of data integrity	75%	R30 000	R22 500

Table 7-40 shows the EMV calculations for human factors. All the risk items have the probability percentage and the cost impact value that produces the EMV.

**Table 7-40: Human factors EMV (Data source: Survey, 2021)**

Risk category	Risk item	Probability %	Cost Impact	EMV
Human factors	Unauthorised access to data and files	55%	R36 000	R19 800
	Unauthorised access to devices	30%	R30 000	R9 000
	Outdated antivirus and antispyware	55%	R36 000	R19 800
	Faulty network connectors and transmission media	11%	R11 000	R1 210
	Old equipment and device failure	1%	R4 500	R450
	Malfunctioning of the system or network	30%	R30 000	R9 000
	Open wireless network	30%	R30 000	R9 000
	Human errors	75%	R25 200	R18 900
	Use of incorrect password criteria	55%	R70 000	R38 500
	Fraud or stealing of information	30%	R36 000	R10 800
	Regular system and application failure	30%	R30 000	R9 000
	Unauthorised modification, deletion and loss of data	75%	R36 000	R27 000
	Denial of service and network downtime	30%	R30 000	R9 000
	Hardware and software failure	30%	R32 000	R9 600
	Bad management	55%	R36 000	R19 800
	Misconfiguring the device	30%	R36 000	R10 800
	Poor delivery of outsourced IT services	30%	R14 000	R4 200
	Use of USB	55%	R18 000	R9 900
Lack of integrity	75%	R30 000	R22 500	
Lack of data confidentiality	75%	R30 000	R22 500	

Table 7-41 shows the malware and technological risks EMV for each risk item based on the probability of the risk item multiplied by the cost impact.

**Table 7-41: Malware and technological risks EMV (Data source: Survey, 2021)**

Risk category	Risk item	Probability %	Cost Impact	EMV
Malware/ Technological risks	Unauthorised access to software	30%	R30 000	R9 000
	Outdated antivirus and antispyware	55%	R18 000	R9 900
	Malware (viruses, worms, Trojan)	55%	R27 000	R14 500
	Accidental installation of unsecured applications	55%	R27 000	R14 500
	Denial of service and network downtime	30%	R30 000	R9 000
	Hardware and software failure	11%	R13 500	R1 485
	Use of USB	55%	R18 000	R9 900

Table 7-42 shows the policies and guidelines EMV for each risk item based on the probability of the risk item multiplied by the cost impact.

**Table 7-42: Policies and guidelines EMV (Data source: Survey, 2021)**

Risk category	Risk item	Probability %	Cost Impact	EMV
Policies and guidelines	Unauthorised user registration	55%	R30 000	R16 500
	Unauthorised access to data and files	75%	R30 000	R22 500
	Unauthorised access to devices	55%	R28 000	R15 400
	Malfunctioning of the system or network	30%	R30 000	R9 000
	Open wireless network	30%	R27 000	R8 100
	Human errors	55%	R36 000	R19 800
	Use of incorrect password criteria	75%	R22 000	R16 500
	Regular system and application failure	75%	R 35 000	R26 250
	Unauthorised modification, deletion and loss of data	75%	R36 000	R27 000
	Denial of service and network downtime	30%	R30 000	R9 000
	Hardware and software failure	11%	R13 500	R1 485
	Bad management	55%	R36 000	R19 800
	Misconfiguring the device	55%	R36 000	R19 800
	Poor delivery of outsourced IT services	30%	R18 000	R5 400
	Use of USB	55%	R18 000	R9 900
	Lack of data confidentiality	75%	R30 000	R22 500
Lack of data integrity	75%	R30 000	R22 500	

The above tables have illustrated the EMV for the identified cyberrisk items in their categories. So every risk item calculated indicates some form of the budget which businesses should consider and accommodate to promote business continuity.

The following section presents the analysis of the value of information configurations for the identified risk categories.

**7.6.1.3 Value of Information Configuration for Cyberrisks Scenarios**

This section presents the value of information (VOI) configuration used with AgenaRisk for different cyberrisk scenarios. The configuration highlights the nodes used, the total time to build the risk scenarios in seconds, the EMV, the expected value given perfect information (EV|PI), and the expected values of partially perfect information (EV(P)PI) for each configuration.

**7.6.1.3.1 Human factors configuration information**

Figure 7-86 displays the unexpected attack as a decision node, the probability of risk as an uncertainty node, and the impact of risk as a utility node. This scenario took 71ms to perform the analysis of the expected maximum value (EMV), the expected value given perfect information (EV|PI), and the expected values of partially perfect information (EV(P)PI).

VOI Configuration	
Decision Node	Unplanned Attack [M2]
Uncertainty Nodes	Risk LikeliHood [M4_1]
Utility Node	Risk Impact [M5]
Optimisation Type	maximum
Scenario	Scenario 1

Total build time: 71 ms

Expected Maximum Value (Utility|Decision) – EMV

Expected Value Given Perfect Information – EV|PI

Expected Value of (Partially) Perfect Information – EV(P)PI

**Figure 7-86: Configuration information for human factors**

As shown in Figure 7-87, the EMV of human factors is 0.277 with two different risk likelihood conditions, EV|PI of 0.273 and EV(P)PI of -0.004. In addition, the unplanned attacks have two Boolean states, which are true and false, while the risk likelihood is ranked low, medium and high.

EMV		0.277	
Risk.LikeliHood.[M4_1]		EV PI	0.273
		EV(P)PI	-0.004
		Unplanned Attack	
		False	True
Risk LikeliHood	High	0.27	0.27
	Medium	0.287	0.287
	Low	0.29	0.29
EV PI = 0.812 * 0.27 + 0.182 * 0.287 + 0.007 * 0.29 = 0.273			
EV(P)PI = 0.273 - 0.277 = -0.004			

**Figure 7-87: Human factors' EMV**

### 7.6.1.3.2 Devices and Technical Systems' Tree Analysis

Figure 7-88 shows the configuration for the devices and technical systems with the probability of risk as a decision node, the level of protection of the device as an uncertainty node and the impact of risk as a utility node. This scenario took 122 minutes to perform the analysis of the expected maximum value (EMV), the expected value given perfect information (EV|PI), and the expected values of partially perfect information (EV(P)PI).

VOI Configuration	
Decision Node	Risk likelihood [M7]
Uncertainty Nodes	Device Protection Level [M1]
Utility Node	Risk Impact [M8]
Optimisation Type	maximum
Scenario	Scenario 1

Total build time: 122 ms

Expected Maximum Value (Utility|Decision) – EMV

Expected Value Given Perfect Information – EV|PI

Expected Value of (Partially) Perfect Information – EV(P)PI

**Figure 7-88: Configuration information for devices and technical systems**

As shown in Figure 7-89, devices and technical systems' EMV is 0.759 with two different malware conditions, EV|PI of 0.728 and EV(P)PI of -0.031. In addition, the device protection has three rankings of low, medium and high, while the risk likelihood is ranked low, medium, and high.

<b>EMV</b>		<b>0.759</b>	
<b>Device Protection Level [M1]</b>		<b>EV PI</b>	<b>0.728</b>
		<b>EV(P)PI</b>	<b>-0.031</b>
Click to show/hide details			
		<b>Risk likelihood</b>	
		High	Medium
		Low	
<b>Device Protection Level</b>	High	0.65	0.68 <b>0.767</b>
	Medium	0.553	0.563 <b>0.683</b>
	Low	0.283	<b>0.3</b> 0.23
EV PI = 0.859 * 0.767 + 0.071 * 0.683 + 0.07 * 0.3 = 0.728			
EV(P)PI = 0.728 - 0.759 = -0.031			

**Figure 7-89: Devices and technical systems' EMV**

### 7.6.1.3.3 Malware and Technological Risks

Figure 7-90 shows the decision node as the risk likelihood, malware as the uncertainty node and the risk impact as the utility node. This scenario took 91 mins to perform the analysis of the expected maximum value (EMV), the expected value given perfect information (EV|PI) and the expected values of partially perfect information (EV(P)PI).

VOI Configuration	
Decision Node	Risk likelihood [M8]
Uncertainty Nodes	Malware [M0]
Utility Node	Risk impact [M12]
Optimisation Type	maximum
Scenario	Scenario 1

Total build time: 91 ms

Expected Maximum Value (Utility|Decision) – EMV

Expected Value Given Perfect Information – EV|PI

Expected Value of (Partially) Perfect Information – EV(P)PI

**Figure 7-90: Configuration information for malware and technological risks**

As shown in Figure 7-91, malware and technological risks EMV is 0.517 with two different malware conditions, EV|PI of 0.517 and EV(P)PI of 0. In addition, the malware has two Boolean states, true and false, while the risk likelihood is ranked low, medium and high.



<b>EMV</b>		<b>0.517</b>		
<b>Malware.[M0]</b>	<b>EV PI</b>	0.517		
	<b>EV(P)PI</b>	0		
<b>Risk likelihood</b>				
		<b>High</b>	<b>Medium</b>	<b>Low</b>
<b>Malware</b>	False	0.417	0.467	<b>0.517</b>
	True	0.417	0.467	<b>0.517</b>
EV PI = 0.98 * 0.517 + 0.02 * 0.517 = 0.517				
EV(P)PI = 0.517 - 0.517 = 0				

**Figure 7-91: EMV for malware and technological risks**

**7.6.1.3.4 Application of Policies and Guidelines Level**

Figure 7-90 shows the risk level as the decision node, policy, and compliance as the uncertainty node, and the risk impact as the utility node. This scenario took 49 mins to perform the analysis of the expected maximum value (EMV), the expected value given perfect information (EV|PI), and the expected values of partially perfect information (EV(P)PI).

<b>VOI Configuration</b>	
Decision Node	Risk level [M3]
Uncertainty Nodes	Policies compliance [M0]
Utility Node	Risk Impact [M7]
Optimisation Type	maximum
Scenario	Scenario 1

Total build time: 49 ms  
 Expected Maximum Value (Utility|Decision) – EMV  
 Expected Value Given Perfect Information – EV|PI  
 Expected Value of (Partially) Perfect Information – EV(P)PI

**Figure 7-92: Configuration information for policies and guidelines**

As shown in Figure 7-93, in policies and guidelines, EMV is 0.793 with two different conditions for the protection level: EV |PI of 0.793 and EV (P)PI of 0. In addition, policy compliance has three rankings, low, medium and high, while the risk likelihood is ranked low, medium and high.

<b>EMV</b>		<b>0.793</b>		
<b>Policies.compliance.[M0]</b>	<b>EV PI</b>	0.793		
	<b>EV(P)PI</b>	0		
Click to show/hide details				
		<b>High</b>	<b>Medium</b>	<b>Low</b>
<b>Policies compliance</b>	High	0.247	0.333	<b>0.793</b>
	Medium	0.247	0.333	<b>0.793</b>
	Low	0.247	0.333	<b>0.793</b>
EV PI = 0.1 * 0.793 + 0.3 * 0.793 + 0.6 * 0.793 = 0.793				
EV(P)PI = 0.793 - 0.793 = 0				

**Figure 7-93: Policies and guidelines' EMV**

### 7.6.1.3.5 Phishing and Network

For this phishing and the network case, a decision node used was the email phishing node with an uncertainty node presenting the protection level and the utility node is the risk impact, as shown in Figure 7-94. This scenario took 63 s to perform the analysis of the expected maximum value (EMV), the expected value given perfect information (EV|PI) and the expected values of partially excellent information (EV(P)PI).

VOI Configuration	
Decision Node	phishing email [M1]
Uncertainty Nodes	protection level [M0]
Utility Node	risk impact [M3]
Optimisation Type	maximum
Scenario	Scenario 1

Total build time: 63 ms

Expected Maximum Value (Utility|Decision) – EMV

Expected Value Given Perfect Information – EV|PI

Expected Value of (Partially) Perfect Information – EV(P)PI

**Figure 7-94: Configuration information for phishing and network scenario**

The phishing email depends on the protection level. As shown in Figure 7-95, phishing and network’s EMV is 0.459 with two different conditions for the protection level, which are EV|PI of 0.459 and EV (P)PI of -0. The result of the EV|PI value is -0 minus the same value. In addition, the phishing email has two Boolean conditions, which are true and false, while the protection level has ranked levels low, medium, and high.

EMV		0.459	
protection.level.[M0]		EV PI	0.459
		EV(P)PI	-0
		phishing email	
		False	True
protection level	High	0.627	0.243
	Medium	0.5	0.23
	Low	0.251	0.172
EV PI = 0.333 * 0.627 + 0.333 * 0.5 + 0.333 * 0.251 = 0.459			
EV(P)PI = 0.459 - 0.459 = -0			

**Figure 7-95: Phishing and network’s EMV**

The following section presents cyberrisk scenarios and the decision tree analysis of the risk cases.

### 7.6.1.4 Cyberrisk Scenarios and the Decision Tree Analysis

This study, the scenario analysis and the decision trees are based on the cyberrisks shared by the study participants, described in the above sections, and classified according to the different risk categories. Scenario analysis focuses on predicting the probability of the risk occurring or the risk consequences (Kishita et al., 2016). It also helps to explore future trends in a specific period. One of the key stages when using scenario analysis is to identify the future trends, uncertainties and the key factors that disturb the main plan. The scenario analysis helps to separate and identify the main trends (certainties or uncertainties) by looking at the trends that may not or may be significant or may not change. The action is essential because it avoids frustration and improves efficiency while saving time. On the other hand, the tornado graphs present the tool to depict the sensitivity of

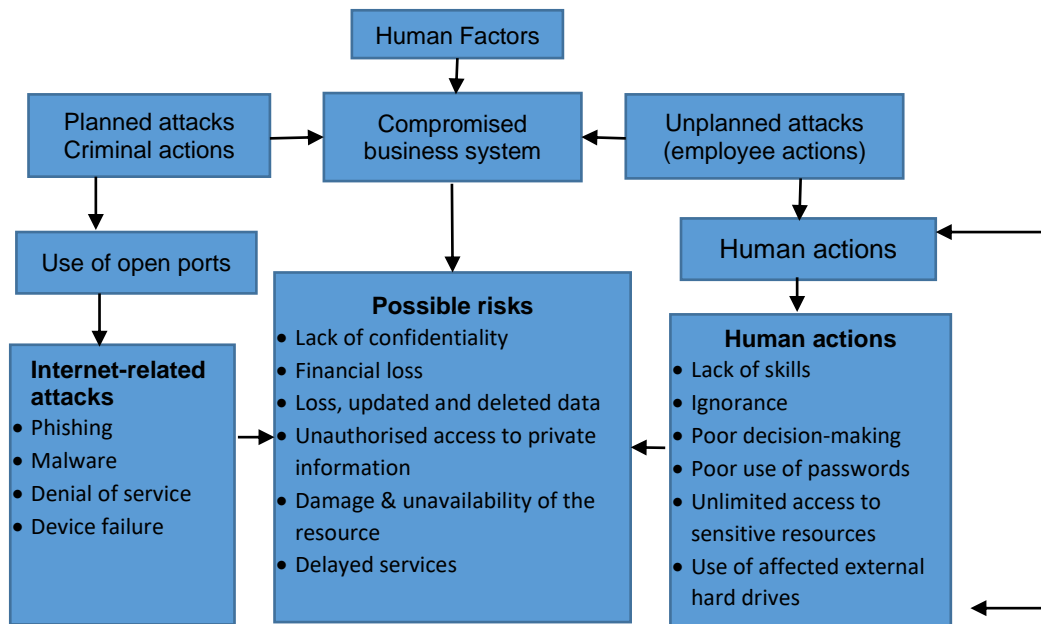
a result to changes in selected variables. In this study, these graphs illustrate the uncertainty factors that greatly influence the impact to single out the significance objectively.

On the other hand, the decision trees present the process of drawing and illustrating risks in a graphical form to distinguish between where risks can be controlled and the probability of the risk occurrence (Metsänen, 2022). This process demonstrates the alternative solutions available to solve a given and specific risk or problem by determining the most convenient and effective strategy. It also shows the possible decision options. The decision trees compare cyberrisk probabilities and rewards between various decisions. The following section presents the risk scenarios with the simulated decision tree analysis.

#### **7.6.1.4.1 Human Factor Scenario and the Decision Tree Analysis**

This section illustrates the human factor decision tree analysis demonstrating the risk likelihood for the planned and unplanned attacks. An unexpected attack could be an ignorant employee downloading a file or software from unverified sources. In contrast, a planned attack could be a criminal who has gained unauthorised access to the business system. Figure 7-96 shows the risk likelihood associated with unplanned and planned attacks caused by human factors in a decision tree.

Both the actions performed by the employees and the criminals happen through interaction with the business system. For planned attacks, the criminals use every possible entry, including unsecured ports, to gain access to the system and its related resources. The planned attacks are phishing, malware, denial of service, and device failure. Unplanned attacks are the lack of skills, ignorance, poor decision-making, poor implementation, unlimited access to sensitive resources, and use of the affected external hard drives. These attacks pose risks related to the lack of confidentiality, financial loss, other losses, manipulation and deletion of sensitive data, unauthorised access to private information, damage or unavailability of a resource, and delayed services.

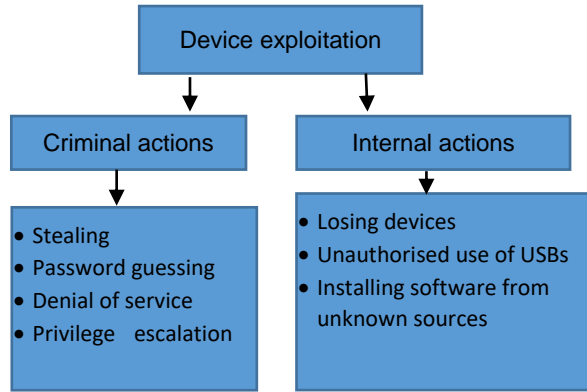


**Figure 7-96: Risks associated with planned and unplanned attacks**

#### 7.6.1.4.2 Devices and Technical Systems Decision Tree Analysis

Devices are primarily used as a tool to access business services. In the business sector, there are both networking devices (routers, switches, hubs), while the end devices can be smartphones, notebooks, laptops and desktops. If these devices are connected to the network, they could be exposed and vulnerable to cyberthreats and attacks, which cause risks to businesses. Criminals and employees take advantage by gaining unauthorised access to the networked devices by using a piece of code to cause and trigger unintended behaviour on the device. This process hijacks authorised users' actions by deploying a code that manipulates the device.

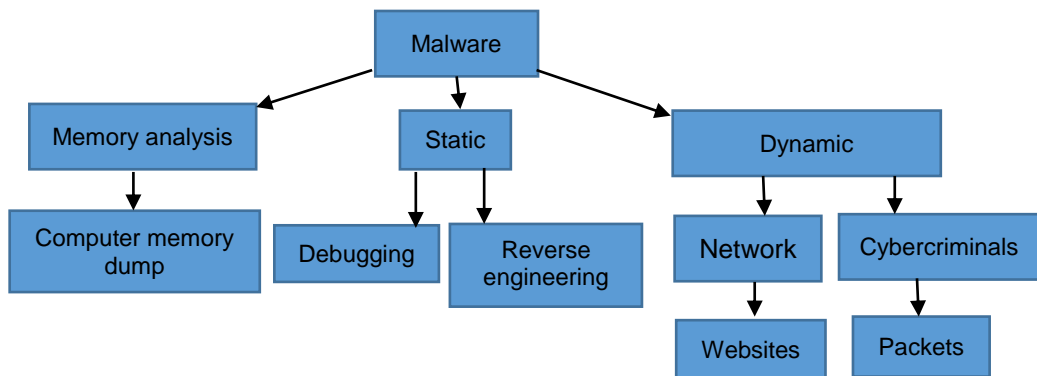
Criminals deploy a software code to guess and steal the passwords so that they may gain unauthorised access to the business systems. They could also affect the network so that it may not be available and could also hijack user privileges. Employees could ignorantly perform activities that leave the business system vulnerable. Some employees could lose the device, which could land in the criminals' hands. Sometimes, the employees use unsecured memory sticks for information exchange. Those memory sticks could have malware that triggers device exploitation. In addition, using the Internet could result in device exploitation because employees could ignorantly download software from unknown sources. These activities are shown in the next diagram.



**Figure 7-97: Device exploitation**

### 7.6.1.4.3 Malware and Technological Risks Decision Tree Analysis

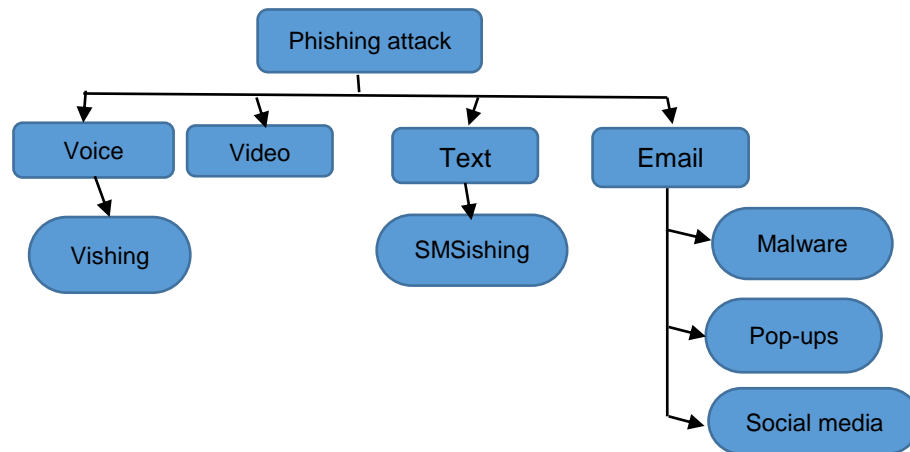
Malware attacks can result in various business risks, such as denial of service, man-in-the-middle attack, or network, device or system failure. The malware attacks can be static or dynamic, with memory analysis as a component. Static malware takes the form of debugging and reverse engineering. The memory analysis is conducted on the computer memory dump, while the dynamic malware affects the network and can also be caused by cybercriminals. On the network, the malware gains access through the websites, while cybercriminals can access the network packets. Regardless of the malware strategy used, businesses remain under attack and no uniform strategy can be used to reduce risks.



**Figure 7-98: Malware attacks**

### 5.5.1.4.4 Phishing and Network Attack Tree Analysis

Phishing is a common Internet fraud that takes place when private and personal information using easy and complicated automated phishing strategies take place, resulting in a threat (Rastenis et al., 2020). Figure 19 shows the phishing tree attack through different voice, video, text and email strategies.

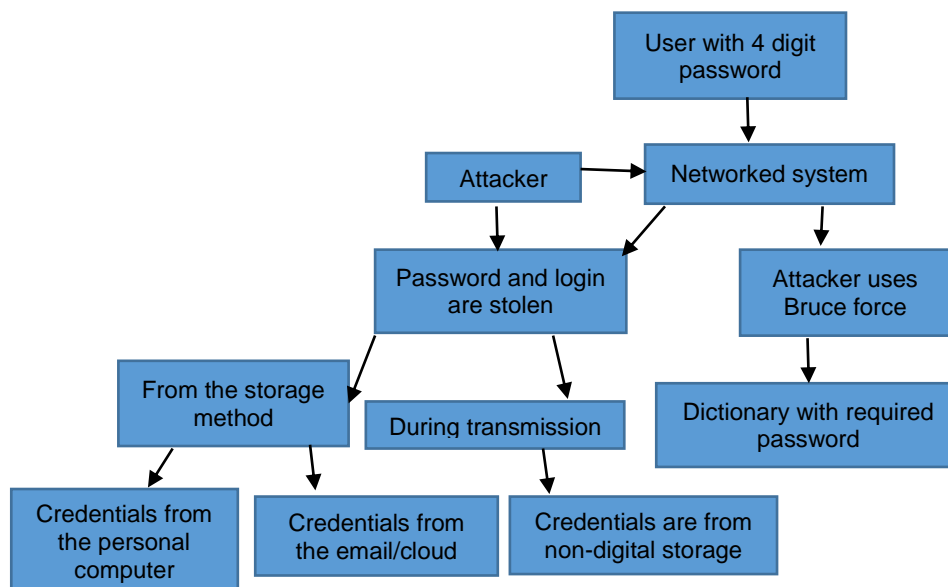


**Figure 7-99: Phishing and network decision tree**

Based on the scenario above, businesses can be exposed to phishing attacks. So, businesses should take the initiative and responsibility to train and equip their employees. Adequate training for all employees would reduce the risk likelihood and the impact of the risk. For each phishing risk, there is a consequence that is equivalent to the mitigation cost. The tree indicates the different strategies deployed on the network or the phones.

#### **5.5.1.4.5 Lack of Policies and the Guidelines Scenario with the Decision Tree**

This attack tree analysis illustrates the SME's lack of a password usage policy. In this case, employees use passwords that do not comply with the acceptable password criteria. An employee accesses the networked system without understanding the risks of using unacceptable password criteria. In this case, the employee used the four-digit year of birth password. The attacker then used two available strategies to steal the passwords. The attacker used Bruteforce, which has a list of all the required passwords. The attacker can also steal an employee's credentials (user name and password), which could be in the place of storage or during the transmission. The password from the place of storage can be available from the personal computer, email, cloud storage or any non-digital storage, such as a post on a desktop computer or laptop computer. This scenario in Figure 7-100 illustrates the risk likelihood of losing a password that is non-compliant owing to the lack of cyber security policies, rules, standards, procedures and guidelines.



**Figure 7-100: No password policy**

### 5.5.1.5 Summary of the Scenarios and the Decision Trees

These decision trees and the scenarios revealed that the small business sector might be aware of possible risks that may arise in the medium or long term. It can be concluded that every key category poses a risk to businesses. These risks may be independent and dependent on each other. Therefore, all businesses must have proactive mitigation plans to reduce and control the risks. The following section addresses the detailed risk control measures which SMEs could use. The scenario analysis illustrated the different incidents or cases in which businesses could be exposed to various cybercrimes and risks. Some of the risks can be planned, others unplanned. The planned cyberrisks require strong measures which address all levels of the business, especially during the Covid-19 global pandemic.

Unplanned attacks can result from human errors caused by employees. Even though there could be several underlying factors, such as ignorance and poor implementation of the security measures owing to lack of understanding, fatigue and understaffing, the unplanned attacks could be avoided. The tornado graphs have also been used to illustrate different scenario cases which result in cybercrimes in the SME sectors. The tornado graphs were designed using the AgenaRisk package with Bayesian tools. The cases used to predict the risk likelihood were based on the simulated case scenarios in Section C. The following section presents the EMV.

## 7.6 RISK TREATMENT

This phase involves selecting proactive and appropriate measures to modify the risks. The possible actions are presented below.

### 7.6.1 Risk Control Options

Risk control is an essential phase that improves the overall health and safety of the enterprise while reducing the chances of losing business assets, finances and people (Zio, 2018). This phase consists of risk response planning and risk control for the cyberrisks that might occur at the SMEs. It is the list of methods used to assess risks and perform mitigation actions to eliminate them. These techniques are drawn from the performed risk assessment relating to human factors, devices, technological risks, malware and phishing-related risks. This stage focuses on the proactive changes implemented to avoid, mitigate or reduce cyberrisks. After conducting the qualitative and quantitative risk assessment, this section presents a risk control plan to identify and evaluate in response to any cyberrisks and potential threats or attacks that pose a risk and might interfere with the main business operations (Sheehan *et al.*, 2021). This process includes the main concepts such as risk avoidance, loss prevention, loss reduction and separation (Reguero *et al.*, 2020)

- **Risk avoidance** – This is the main method to control loss. This concept deals with measures that help to avoid risk and prevent it from happening. All business institutions should look for possible risk exposure or areas that promote business vulnerability.
- **Prevention of loss** – In this case, this concept takes the risk to minimise the chances of loss instead of eliminating it. An example would be for businesses to always have up-to-date antivirus software, which will always look for possible threats and attacks to penetrate the business system. Furthermore, an active firewall will continually filter traffic entering and leaving the network.
- **Reduction of loss** - The risk is considered and seeks to limit and reduce the losses when a threat occurs. This requires businesses to have proactive and adequate security measures that will reduce the chances of risks.
- **Separation** – The process involves separating the main assets to reduce the risk of events that might affect many different office spaces or locations. As a result, if all assets are in one office or building, the risk exposure will be severe and bear consequences. In this case, businesses should always try to separate their servers and services so that they don't belong to the same centralised administration, which results in one point of failure. Separation increases operation chances while reducing business discontinuity probability.

The following section presents response planning as the last stage of the contingency plan for different cyberrisks to which businesses are continuously exposed and vulnerable.

### 7.6.2 Response Plan for Identified Risks

Based on the conducted qualitative and quantitative risk assessment for small enterprises, there is a high need to protect overall business assets to improve business continuity and increase revenues and production. Security measures can be applied to protect the business assets such as people, information, applications and systems, network, and hardware devices. Even though the blanket approach may not be appropriate for all the risk



categories, the study recommends the following risk response plan. The recommended security strategies should be thoroughly implemented, regularly monitored, and enforced by knowledgeable cybersecurity personnel.

### **7.6.3 Contingency plan**

For the interest and improvements of business continuity, businesses need to implement the risk contingency strategies that risk experts often recommend. These strategies proactively respond to the negative and positive risks in the business sectors. The four effective strategies that respond to negative risks are: avoid, accept, mitigate and transfer (Alkinani et al., 2021). The response planning phase focuses on developing response actions with alternative options to reduce and mitigate cybersecurity risks. This phase aligns the risks with their responses, which relate to the risk's severity, cost and feasibility. This phase involved a management plan about possible cyberrisk responses using available resources and consequences to transfer, avoid, mitigate or accept risks. The response plan should involve the identified cyberrisks, all stakeholders who work on the system and the effective strategies associated with each risk. Each business should have dedicated, knowledgeable personnel who lead the team to plan, implement and review the cybersecurity response plan.

## **7.7 MONITORING AND REVIEW**

Monitoring and controlling is the last step in the risk management phases. This phase involves tracking the risks and their potential to cause harm, implementing risk response measures and examining the effectiveness of risk management procedures. This stage is a continuous process to sustain the business to guide and improve the overall cybersecurity risk management process. The process equips and prepares the employees, third parties and management to make informed decisions. Most businesses use monitoring and control as the barometer to determine the effectiveness of risk management to adjust the response plan accordingly and prioritise risks (Alexe et al., 2020).

For proactive risk mitigation, the respondents suggested that businesses should always prioritise the risks, threats and attacks at all levels. This presents an essential step in the risk management process. Some participants indicated that an insurance company helps them to manage risks and limit liability. Businesses should also have a responsible risk management team that will proactively enforce and implement security measures in all business sections. Similarly, the team should ensure that an appropriate risk response is continuously implemented according to the documented plan. Continuous monitoring of risks is essential to proactively manage risk and act promptly when the need arises to determine the nature of the risk, related potential impact and the likelihood of it happening.

## **7.8 RISK REPORTING**

The study adopted qualitative and quantitative methods of cyberrisk assessment. The process includes the identification of the main threats, vulnerabilities and security risks related to the business assets, including security measures to reduce risks. The small business sector is greatly affected by cybercrimes and is always vulnerable to cyberthreats owing to a lack of resources and information technology skills (Berry & Berry, 2018). Cyberrisks are an ongoing challenge in the business sector, especially during the pandemic. With the sudden rise of the global Covid-19 pandemic, many institutions resorted to using the Internet as the main backbone for running their businesses. The Covid-19 pandemic had threatened the safety and security of businesses and other institutions through the increased number of cyber criminals, leaving them vulnerable and exposed to various cyberrisks and threats (Pritom et al., 2020). Even though risks can have a positive and negative impact in the small business sector, cyberrisks have a negative impact on resources or assets and cause financial damage, which leads to a bad business reputation and ultimately forces business discontinuity.

### **7.8.1 Qualitative Risk Analysis**

Qualitative risk analysis assumes that there is already a high degree of uncertainty in the probability and impact values and defines them either subjectively or qualitatively (Elky, 2006). As qualitative methodologies rely heavily on the experience of the analyst, the process and results of the safety and risk assessment are relatively subjective. Where a qualitative method is used, there is no need for probability data; only the estimated potential loss is used (Feng & Li, 2011). Unlike quantitative risk assessment methods, qualitative risk assessment methods are based on the judgment, insight and experience of the team performing this exercise (Lo & Chen, 2012). The qualitative risk analysis is quick, subjective and should be performed continuously. It focuses on the categories of risks to be prioritised and categorised. The threats are ranked low, medium and high, primarily based on the knowledge and judgment of the individuals conducting the analysis. (Nosworthy, 2000).

To effectively address cybersecurity risks at SMEs requires risk analysis and risk evaluation. Generally, cybersecurity risks are caused by exposure to cyberthreats and attacks. For effective risk analysis and evaluations, businesses should identify threats and attacks associated with them and which trigger risks. A risk is a likelihood of a particular threat source being particularly vulnerable and the impact of that adverse event on the system (Nketekete, Emuze & Smallwood, 2016). The study adopted qualitative risk analysis to identify the impact of the risk and the likelihood that the risk will occur. As illustrated in the previous section, the grouping of the collected risks applied the Risk Assessment Matrix (RAM) as a valuable tool to rate each cyberrisk as low [0-3], medium [4-6] and high [7-10].

A cyberrisk assessment identifies the operational, asset and vulnerability risks of organisations. These cyberrisks are categorised according to the business sector's likelihood of risk and its consequences. The risk assessment generates relevant results as it is a major tool. With the information gathered, a risk assessment should show the

organisation's vulnerabilities. This is done by looking at risk probability and impact. Such an event will have to determine the method of risk calculation. At the same time, it determines how the risk has been calculated, while the actual calculation of risk is different depending on the risk assessment methodology used. So this study used qualitative risk analyses of the risk's likelihood to occur and its impact on the organisational reputation and continuity.

The qualitative risk analysis mainly determines the impact of risk and the likelihood of the identified risks occurring. It also identifies areas exposed to risks and improves understanding. Qualitative risk assessment methods are used to evaluate the effects of the identified risk factors and to create priorities to resolve the potential risk. Mazarean (2007) states that actions depend on the information systems' risks. Most qualitative methods are straightforward and easy to use, with fewer technical staff needed at any institution (Panda, 2009). Qualitative methods express risks in the form of descriptive variables rather than specific monetary terms and require less financing, time and effort to implement (Karabacak & Sogukpinar, 2005).

#### **7.8.1.1 Probability/Impact ranking matrix**

In any sector, regular risk assessments become the fundamental stage in managing risks that determine the acceptable level of exposure and proactively implement the required security control measures (Nyanchama, 2005). The ongoing risk assessment process should be regularly reviewed to ensure that safety measures are appropriate. The process of managing cybersecurity measures in institutions involves a budget based on the levels of risk (Paté-Cornell et al., 2018). For every rated risk, there is a budget that should be allocated. It is essential to always perform a regular risk assessment to determine the relevant and latest data that will produce the risk scoring indicating the severity of the consequence.

The study presented the priority values for different risk cases to determine the risk scoring. The priority values ranged from 1 to 5. The study further illustrated the risk matrix with the risk probability and the risk impact. The high-risk impact can result from significant losses of assets or resources, which negatively impact on the safety objectives and reputation of the operational system. Threats whose impact value is lower may result from the loss of certain assets. The risk probability is ranked from rare, unlikely to happen, moderately sure to happen and certain to happen, while the risk impact ranges from negligible, minor, moderate, major and severe. In a risk matrix, the risk scoring determines the risk's severity level. Any business resource with a high score requires many protection measures to prevent compromises. All the assessed risks get classified according to the risks they pose in a business. In addition, risks are also given priority based on the risk values as a guide for applying security measures.

## 7.8.2 Quantitative Risk Analysis Techniques

Quantitative risk analysis is essential for all businesses and employees at different levels. For example, the security personnel can develop innovative security business skills; system administrators can prioritise their projects based on the return on investments and improve their performance. The following section presents the applied quantitative risk analysis methods.

The study adopted both qualitative and quantitative risk analysis techniques to analyse cyberrisks in the SME sectors. The various quantitative risk analysis methods are:

### 7.8.2.1 Sensitivity analysis

Sensitivity analysis is performed through conditional probability tables for handling different cyberrisks. The study used AgenaRisk to analyse the status quo of the cyberrisks at the SMEs in SA. Sensitivity analysis was conducted based on the identified cyberrisks.

### 7.8.2.2 Decision trees and the risk scenarios

This study used decision trees to illustrate the possibilities of cyberrisks at SMEs in SA. The decision trees were presented according to the main identified cyberrisk categories such as human factors, devices or technical systems, phishing and network, policies and guidelines, and malware or technological risks. Every decision tree analysis is based on cyberrisk scenarios. The scenarios used in this study demonstrate the real-life situation of the cyberrisks at SMEs in SA.

**Tornado graphs** – This study used the AgenaRisk package to simulate the cyberrisks at small businesses. These graphs showed the likelihood of different cyberrisks for different risk cases in the small business sector. The Tornado graphs are based on the risk likelihood for each cyberrisk case.

**Expected Maximum Value** – Based on the different cyberrisk cases, the study demonstrated the expected maximum value of a different EV|PI and EV (P) PI for each case.

**Expected Monetary Value** – This study performed and calculated EMV based on the risk probability percentage and the cost impact for each risk item. EMV used the calculated probability percentage as presented in Table 7-25 multiplied by the cost impact in Table 7-24 based on the asset evaluation shown in Table 7-37.

## 7.8.3 Mitigation Techniques for Identified Cyberrisks

After a thorough analysis of cyberthreats and exposure risks in SMEs, it was discovered that every business sector requires proactive mitigation techniques to reduce, avoid and prevent risks. Information security is highly demanded to improve business continuity and reputation (Alahmari & Duncan, 2020). Businesses should adopt relevant and up-to-date strategies and equip their employees to proactively use mitigating strategies for improving the protection and security of information.

Table 7-43 summarises the recommended protection measures for enhancing the safety, privacy and security of the business assets – people, as well as information. Many studies have suggested the best practices which can be used to improve businesses, especially during the Covid-19 global pandemic. The best practices which small businesses can implement and this study recommends a list of the measures which businesses and other sectors can use.

Table 7-43 also stresses the implementation of proper and proactive strategies.

The collected results indicated that cyberrisks could be shared, transferred, accepted and avoided, as shown in Figure 7-101. In one way or another, businesses are quite aware of risk management even though results do not show the thorough application of risk management. The respondents showed some level of responsibility in terms of managing risks. For example, 19% indicated that they share their risks by dividing them among employees or companies. This process requires businesses to merge services and decisions or be in a joint venture to share any possible loss. The electric, gas and water business sectors mostly prefer to share the risks. This focuses on reducing the risk by managing it by more than one candidate or company, while 23% of the respondents transfer their risks. The risks can be transferred to a third party when there is a contractual agreement for shifting the risk. Risk transfer is an approach that presents the financial loss in risk management by selling the risk to other sectors that may be capacitated to handle it. However, only businesses that belong to insurance companies and are policyholders can transfer the risk.

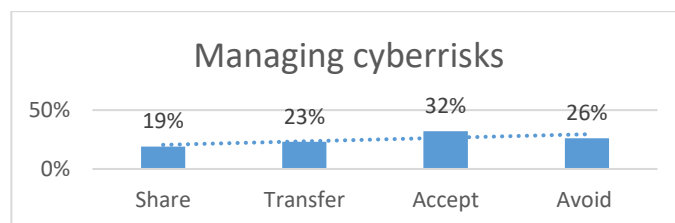


Figure 7-101: Managing cyberrisks (Data source: Survey, 2021)

Thirty-two per cent indicated that they accept the risks by living with them, acknowledging the threat and accepting the consequences. Risk acceptance is sometimes called risk retention by accepting the risk without applying any measures to avoid it. The management of the business would just accept the risk without trying to mitigate or transfer the risk. This is done owing to less attention paid to protecting minor risks and sometimes when the mitigation process might prolong the process or be highly-priced. Owing to the different natures of risks, businesses would accept the risks which cannot be easily mitigated or easily tolerated. Sometimes businesses accept the risks because there would be limited options available or no options at all.

Risk avoidance decreases risk levels by not engaging in certain activities to eliminate the risks and different risk exposures, resulting in high financial loss. Twenty-six per cent of the respondents chose to avoid the risks by leaving the activities that trigger the risks or taking the necessary steps to reduce the risks by performing the likelihood of risk of the negative activity. In this approach, businesses have options to either engage in the risk

or shut down the operation of the risk. For example, if the business has a high risk, then the business can choose to cancel the service to avoid further risks. ICT businesses have options to either deal with failing or overly used networks or deploy an alternative service, which could be cloud-based. The resolution of a cloud-based service would also include scalability and redundancy. In the process, the risk activities get classified to identify low and high risks to avoid the risk, even though not all risks may be possible to avoid. Based on the identified risks, this study recommends the following proactive mitigation strategies shown in

Table 7-43.

**Table 7-43: Recommended mitigation techniques (Data source: Survey, 2021)**

<b>Security controls</b>	<b>Risk category</b>	<b>Recommended Protection Measure</b>
Small business risk management controls	Policies and guidelines	<ul style="list-style-type: none"> <li>• Training all users and employees</li> <li>• Enforcement of cybersecurity and business policies, rules, guidelines, standards, and procedures</li> <li>• Regular review of cybersecurity and business policies, rules, guidelines, standards and procedures</li> </ul>
User provision controls	Human factors (employees)	<ul style="list-style-type: none"> <li>• Use of appropriate and accepted password criteria</li> <li>• Restricted access rights to sensitive information</li> </ul>
User authentication controls	Human factors (users, employees, third parties)	<ul style="list-style-type: none"> <li>• Enforcement and continuous review of cybersecurity and business policies, rules, guidelines, standards and procedures</li> <li>• Use of the multifactor authentication</li> <li>• Use of the firewall to restrict access to the business network</li> <li>• Restricted permission to certain business information and servers</li> </ul>
Administrator rights and privileges	Human factors (employees)	<ul style="list-style-type: none"> <li>• There should be no misuse of the access rights and privileges</li> <li>• Account restrictions</li> <li>• Cybersecurity awareness training and education</li> <li>• Use clear guidelines, procedures and policies that describe the effective use of the system</li> <li>• Review, manage and restrict account access and privileges.</li> <li>• Use strong passwords &amp; password management too</li> <li>• Review online accounts and credit reports</li> </ul>
Physical, facilities & environmental security controls	Technical risk/Network Human factors	<ul style="list-style-type: none"> <li>• Prioritisation of the physical security</li> <li>• All employees, third parties and clients should have user identifiers</li> <li>• Restricted access to unauthorised parties</li> <li>• Equipment and business resources should always be secured and protected using the appropriate security measures.</li> <li>• Lock buildings</li> <li>• Use of biometric devices</li> <li>• Use of access cards</li> </ul>
Data-protection controls	Technical risk/Network Human factors	<ul style="list-style-type: none"> <li>• Restriction of access to authorised personnel only</li> <li>• Use of multifactor authentication</li> </ul>
Continuity of operations controls	Technological risks/ Systems/devices (Network, Hardware and software)	<ul style="list-style-type: none"> <li>• Regularly updated systems</li> <li>• Protection measures should also be kept up-to-date</li> <li>• Firewall to filter incoming and outgoing traffic</li> <li>• Detection systems to proactively reduce and mitigate risks.</li> <li>• Use of multi-factor authentication</li> <li>• Use of antivirus, antispysware</li> <li>• Device encryption and physical security</li> <li>• Use multi-factor authentication</li> <li>• Perform regular software and hardware updates</li> <li>• Periodically back up data</li> <li>• Ensure endpoint protection</li> </ul>

The best practices for small and medium businesses are essential to a hygienic approach to information security, people and resources (Antunes et al., 2021).

## **7.9 CONCLUSION**

In conclusion, risk management is essential for future planning based on what could go wrong and the related countermeasures to minimise risk exposure changes. This study adopted risk management processes to assess the cyberrisks experienced by the small business sector. The study discussed each process of cyberrisks and focused on the cyberrisks faced by SMEs in South Africa (SA). This chapter conducted a quantitative cyberrisk assessment using modeling and analytical techniques to perform sensitivity analysis, scenario analysis, Tornado graphs, decision trees, and EMV to determine the risk likelihood and the risk impact.

## CHAPTER 8: CONCLUSION AND RECOMMENDATIONS

### 8.1 INTRODUCTION

This concluding chapter pulls together this work's different stages to achieve the main goal. The study identified the research objectives that supported the success of the leading research aim, followed by the relevant literature review, and described the method of inquiry used to meet the objectives, followed by the research findings and discussion, the model development, and finally, presented the concluding points that came up from the overall research.

The rest of the work is presented as research implications relating to supporting the objectives set out in Section A, followed by study outcomes, outputs and contribution, study limitations, best practices and recommendations, future research, and concluding remarks. The following section summarises the study objectives and questions described in Section A. The results are presented according to the objectives.

### 8.2 RESEARCH IMPLICATIONS CONCERNING THE RESEARCH OBJECTIVES

The study's main aim was to design, develop and evaluate a cybersecurity tool for small and medium enterprises in South Africa (SA). The three research objectives and questions posed in Chapter 1, which helped achieve the main aim, were answered. The cybersecurity tool as a graphical representation is illustrated in Section C. The tool demonstrated the nodes as variables and arcs as links that connect the dependent and independent variables needed for deployment at SMEs. The nodes present the prior indicators, protection measures, and posterior indicators. The tool also showed the risk probability of the different scenarios, which resulted in a negative impact on any uncertainty.

In addition, the work illustrated and evaluated the developed cybersecurity models in five different simulated case scenarios in Section C. After reviewing the relevant literature in Chapter 2, the research identified three objectives which are addressed below.

#### **Objective 1: Conduct a qualitative cyberrisks analysis to determine the risk matrix**

This study adopted ISO 31000:2018 as the risk management standard with seven processes, which helped to conduct the qualitative cyberrisk assessment. The data used for the assessment were collected from the selected sample of SMEs in different sectors in the country. Data were then analysed according to the related themes to build a risk register for the experienced risks. The related risks experienced were then categorised to form cyberrisk themes. The emerging themes were human factors, phishing and network-related risks, malware and technological risks, devices and technical systems, as well as the lack of policies and guidelines, as shown in Table 7-21. The study developed the criteria for the risk likelihood further, as shown in Table 7-25, and the risk impact in Table 7-24.



Based on the analysis of the collected risks, this work ranked cyberrisks based on the risk matrix using the risk likelihood and the risk impact ratings, which were assigned according to the severity of the risk. Each assessed risk produced outcomes based on the risk matrix, which determined the severity of the risks and suggested risk prioritisation. Risks with higher risk values showed high risks, which had a high impact. So, those risks should be prioritised for risk responses. All the themes with their risks were ranked according to their risk likelihood and the risk impact at the businesses to determine the risk values in the risk matrix.

## **Objective 2: Conduct a quantitative cyberrisk assessment using modelling techniques**

Section D used analytical, probabilistic, and unconventional quantitative techniques to perform sensitivity analysis using the Tornado graphs and expected maximum value. The AgenaRisk package was used to generate the sensitivity tables, Tornado graphs, and the expected maximum value. The study also used the decision trees analysis, scenario analysis, and expected monetary value (EMV).

**Sensitivity analysis:** The sensitivity analysis was conducted using conditional probability tables to determine the variation in values of the independent variables that directly affected dependent variables. For each emerging theme, the sensitivity analysis was performed to determine varied values of the different risks. All the varied values were demonstrated in the previous Chapter 7. The technique assessed the probability of the variable actions, determining the decision to produce an outcome where the risk with the highest percentage was considered sensitive. The sensitivity analysis was performed for the five risk categories.

**Tornado graphs:** These were generated using the AgenaRisk package, which has AI tools to predict the risk likelihood for different risk cases. These graphs form bar charts with different data categories shown in a vertical form rather than the normal horizontal form. This technique was useful for generating the sensitivity analysis by comparing the importance of the given risk variables. For every risk variable used, the level of uncertainty was assessed, showing the low, medium, and high-risk outcomes. This technique demonstrated the uncertain values while other variables played the role of the baseline and stable values, which enabled the assessment of the risks of uncertain variables. All the risk scenarios and cases demonstrated in Section C were analysed.

**Expected maximum value:** This technique is based on the AgenaRisk, where the value of information (VOI) configuration is demonstrated in different cyberrisk scenarios. The configurations showed and highlighted the risk nodes that were used, with the total time to build the risk scenarios in minutes and seconds, the expected maximum value (EMV), the expected value given perfect information (EV|PI) and the expected values of partially perfect information (EV(P)PI) for each configuration. This technique was performed on all the different cyberrisks. The results of each risk case were illustrated in Section C.

**Scenario analysis:** The work also used scenario analysis with the emerged risk categories, which focused on the effect in a certain situation. This analytical method used simulated scenario information to illustrate the different cases with independent and dependent variables, ultimately producing an outcome. The same scenarios

were used to analyse collected risks using the decision tree analysis. The decision tree analysis demonstrated human factors, phishing and network risks, devices and technical systems risks, malware and technological risks, and the lack of policies and guidelines.

**Decision tree analysis:** DTA presented the process of drawing and demonstrating the sources of risks in a graphical form distinguishing between areas where risks can be controlled and the likelihood of their occurrence. This technique showed the areas where alternative solutions and decision options can be deployed for each node or variable. The decision trees compared cyberrisk probabilities and rewards with various decisions. So the decision trees are based on the cyberrisks shared by the study participants.

**Expected monetary value:** EMV weighted the likelihood of the risk output, carrying more details about the severity of the risks to prioritise a response plan. The risk likelihood using the EMV was performed for each cyberrisk category. The EMV acted as a valuable technique that predicted the risk outcomes for uncertain future risks, which yielded either positive or negative outcomes. This mathematical calculation technique determined the cyberrisk probability and the impact as the cost of the risk. So, a cost value was assigned for every risk identified in relation to the probability and potential effect on the risk event.

### **Objective 3: Develop and evaluate a cybersecurity risk tool for SMEs in SA using the AgenaRisk package with Bayesian network tools**

This objective was achieved and presented in Section C. Cybersecurity models were the results of the analysis and alignment with the National Institute of Standards and Technology (NIST) cybersecurity framework presented in Section B. The study developed cybersecurity models as tools, namely the generic model in Figure 6-35, the secondary cybersecurity model in Figure 6-36, the Beta Model in Figure 6-37 and the Alpha Model in Figure 6-38. All these models were the outcome of the analysed results collected from the research sample. The models indicated all the dependent and independent variables and their relationships, including their effect on the impact. Any business sector can be able to reference the models and predict the risk likelihood of the risks.

In addition, this objective involved the development of the five simulated cyberrisk scenarios using the AgenaRisk package to demonstrate the risk likelihood and their impact. The cyberrisk case scenarios are presented in Section C based on the commonly experienced cyberrisks by SMEs. Each case also illustrated the contributing variables to a negative risk that results in a data breach.

## **8.3 OUTCOMES, OUTPUTS, AND CONTRIBUTION**

This section presents a detailed summary of the study outcomes, outputs, and overall contributions. The study outcome relates to the study's main aim, while the research output presents the main thesis that was developed and the related academic papers. The study's contribution relates to the methodological, theoretical, and practical

contributions. Table 8-44 summarises the study's outcome, output, and overall research contribution, explaining each contribution type.

**Table 8-44: The summary of the research outcome, output and contributions**

Contribution	The explanation for the contribution type
• <b>Outcome</b>	Thesis about designing, developing and evaluating the cybersecurity risk model for SMEs. The model determines cyberrisk likelihood for different cyberrisk scenarios.
• <b>Research output</b>	The study produced the thesis dissertation and published research papers in accredited and peer-reviewed conferences or journals: four conference papers, two journal articles, and a poster.
• <b>Methodological contribution</b>	The study used ISO 31000:2018 as the risk management standard and the AgenaRisk package with Bayesian network tools to design a cybersecurity risk model that determines the risk likelihood and predicts the risk impact. In addition, it used the NIST framework to better understand and manage cyberrisks.
• <b>Theoretical contribution</b>	The study contributed to the literature on cybersecurity, risk management, NIST, and the AgenaRisk package. The study used the ISO 31000:2018 standard and the NIST framework to analyse cyberrisks in the SME sector to suggest risk mitigation strategies. In addition, the AgenaRisk package with the Bayesian probabilistic tools was used to design and develop the risk tool that predicts cyberrisks in the SME sector.
• <b>The practical contribution</b>	The research developed five simulated case study-based scenarios to determine the risk probability and impact by demonstrating the effectiveness of the cybersecurity risk tool using the AgenaRisk tool. It also brings insights into the common cybersecurity risks, threats, and attacks in the SME sector. Lastly, the work predicted the risk impact based on the probabilities and illustrated the relationships between the dependent and independent variables.

#### 8.4 STUDY LIMITATIONS

There are several inhibiting issues when conducting a study, including human factors and external factors. The nature of the human element is automatically limited by common mistakes made, businesses, and opportunities that cannot be reached. Likewise, external factors such as the environment in which the research is conducted could limit the study. An example is a public enterprise with developed structures and changes. The researcher reached every available participant that was contacted. The Covid-19 global pandemic affected the study regarding full access to the participants owing to a lack of computer literacy and instant adjustment to cyberspace. In addition, qualitative research demands a lot of time which became a challenge for this study. Lastly, the research participants did not all have time to participate. Consequently, data were also collected from different business sectors in different provinces.

The study used a sample of small and medium enterprises from different business sectors limited to six of the nine provinces of South Africa. The study was limited to South Africa and not to the other neighbouring countries.

#### **8.4.1 Reflection: researcher's experiences during the data collection**

The process of data collection was strenuous and tedious during the research journey and took longer than the researcher had planned. During the first phase, the researcher initially contacted the selected participants, but some of the research participants could not respond to the communications as initially agreed. Some research participants lost their lives owing to Covid-19, which hit the country so hard. This gave the researcher painful experiences, negatively affecting the researcher's mental state and writing momentum.

### **8.5 RECOMMENDATIONS**

After a thorough analysis of the study, there was a need to suggest possible measures to reduce, control and manage the state of cybersecurity risks in the SME sector. The NIST cybersecurity framework and risk management standards based on ISO 3100:2009 have informed the research recommendations. The recommendations also follow the study objectives and questions listed in the introductory chapter in section 1.3. It can be concluded that SMEs need a solid cybersecurity culture that transforms employees and their behaviour to reduce risk likelihood. The enforced cybersecurity culture will act as the human firewall against possible attacks and threats without pressure.

The study suggested implementing comprehensive, effective, and reasonable cybersecurity strategies to overcome cybersecurity challenges faced by SMEs. Small businesses invest in training on cybersecurity procedures, rules, standards, and guidelines. They should prioritise the safety and security of their private and sensitive information by protecting data and creating an effective policy that can directly and positively influence their reputation. All management and business owners should enforce the use of policies to be implemented in all aspects of the business. The small business sector should regularly back up their information or make use of cloud storage with adequate measures to protect their data. The SME sector should adopt any cybersecurity framework to help them manage, align and protect their business resources. Industry standards and frameworks benefit the sector in assessing and identifying risks to ensure alignment with security governance and implementing effective security policies. Frameworks, in general, are designed to help business sectors of all sizes to apply the security strategy for them. In addition, businesses should always conduct a risk assessment to determine the risk likelihood and implement proactive measures to reduce risks.

Businesses should prioritise the end device and technical systems security controls. Human factors are the leading source of cybersecurity risks. Therefore, businesses should keep their employees updated on the latest security measures. All employees should attend regular training and awareness workshops to equip them with adequate knowledge. Some security controls, such as the proper use of passwords, should be enforced to reduce

risks, especially for employees who have access to private and sensitive data. Employee behaviour should be governed by active policies, rules, and guidelines, which are regularly monitored and enforced. The government should collaborate and partner with businesses to strengthen and enforce the safety and security of information. There should also be a skilled and dedicated candidate who would be responsible for improving the state of cybersecurity by enforcing organisational compliance.

## **8.6 IDEAS FOR FUTURE RESEARCH**

The research was primarily concerned with the SMEs in six provinces in SA without including other African countries. The study only used NIST as the cybersecurity framework for managing cyberrisks. The study also used the only the ISO 31000:2018 standard in the risk assessment process. The study also used the AgenaRisk package with Bayesian Network tools as the technological instrument to predict the cybersecurity risk probability and the risk impact within the SME sector. This study has ideas which could be considered for future research.

So, in the future, it would be necessary to:

- To assess every NIST control on every sector in all the nine provinces of the country.
- To perform a comparative study of the different standards other than ISO 31000:2018
- Use Monte Carlo to predict cyberrisks and their likelihood.
- Perform the risk likelihood observations per sector and per province.
- Extend the scope by including the big organisations
- Use the posterior predictive densities like Expected log-predictive density (ELPD) or information criteria such as Akaike information criterion (AIC) and widely applicable information criterion (WAIC) to evaluate the Bayesian network algorithms.

## **8.7 SUMMARY**

The chapter aimed to perform the risk analysis to identify and evaluate the threats and risks relating to SMEs by looking at the major sources of risks, their consequences and risk likelihood. Through a thorough analysis of the main areas of the businesses, cyberthreats and risks were identified, exposed and analysed. The risk probability of individual attacks and their relative impact on the enterprise system were identified during the risk analysis process. The chapter presented the common cyberrisks, threats and attacks that businesses experiences. The study used risk management to analyse cyber-related risks to create a culture for decision-making based on data assessment. The assessment of cyberrisks maximises the opportunity and minimises the consequence of cyberthreats. The study analysed the collected data to identify the common cyberrisks and attacks with the main sources of threats to create the risk register for old and emerging cyberrisks.

The chapter discussed the qualitative and quantitative risk management techniques for cybersecurity and risk management at SMEs in SA. The information gathered from the selected sample of participants was used to establish the context of the study. The study explained potential, emerging and old risks with their sources in the context of cybersecurity at SMEs. The related risks were then identified, grouped and categorised according to themes to create the risk register. Identified risks were then analysed to determine the risk likelihood and impact. The overall risk value which is the results of the risk probability and the risk impact helped prioritise cyberrisks. The risk matrix was calculated as the risk likelihood multiplied by the risk impact to determine the risk scoring. The quantitative analysis determined the expected monetary value and used the quantitative analysis methods to perform sensitivity analysis, decision trees, and scenario analysis and used tornado graphs to analyse cyberrisks.

The study evaluated cyberrisks further by using probability estimation in various scenarios with different probabilities to meet the overall cost and schedule. Based on the experienced risks, the study presented the response treatment options with relevant and proactive plans guiding and monitoring the risk to enable the earliest possible warning. The last phase involved monitoring and reviewing the risks to identify abnormalities, which will be ongoing. With time, some risks can expire and be given a certain label such as 'the risk did not occur'. Similarly, some risk priorities may change based on the risk profile (*probability, impact*). With the ongoing pattern of risks and re-analysis, some risks could produce different priorities, influencing a revision of the response plan.

Based on the identified cyberrisks, threats, and attacks, the study recommended mitigation strategies that could be applied to reduce, avoid, separate, and mitigate cyberrisks at SMEs.

## **8.8 CONCLUSION OF THE STUDY**

This study designed, developed, and evaluated cybersecurity risk tools as a case for small to medium enterprises by following the research objectives and questions posed in Section 1 to support the main study aim. The relevant literature review was conducted, and the method of inquiry was selected and accounted for. This work combined the qualitative approach, risk management standard, cybersecurity framework, and the AgenaRisk package to achieve the study's main aim. The study used thematic analysis and risked analytical techniques to analyse data from the selected participants.

The NIST framework was used to align, manage, improve and mitigate cybersecurity risks experienced by the SMEs with the recognized cybersecurity standards and guidelines of the framework. Risk management processes helped to determine common cyberrisks experienced by the SMEs, their root causes and vulnerable assets, as well as their risk impact and likelihood. The study used quantitative techniques to determine expected monetary value, sensitivity analysis, expected maximum value (EMV), and use of decision trees and scenario analysis. For the model development, the study used the technological tool which is AgenaRisk package, to determine

the risk likelihood and the risk impact, illustrating the dependent and the dependent variables with their relationships.

It can be concluded that the South African country has become the victim of cybercrimes which trigger various risks to businesses. Cybercrimes are internally or externally generated and have hit different business sectors resulting in a negative impact. Regardless of the type and amount of security implemented in different organisations, businesses remain the target. The study discovered that cybercriminals are after what they can benefit than the size of the business. Businesses lose a range of items when they have become the targets of cybercrimes and risks. This includes the physical, digital, economic, psychological, reputational, social, and societal harm, which in turn delays the business growth. However, for cyber safety and security, businesses should always proactively implement mitigation measures that protect resources, people, data, and information to promote business continuity, confidentiality, integrity, and availability. Businesses should always align with the cybersecurity framework that promotes the safety and security of information and data.

## REFERENCES

- Abdullah, A., Thomas, B., Murphy, L. & Plant, E., 2018. An investigation of the benefits and barriers of e-business adoption activities in Yemeni SMEs. *Strategic Change*, 27(3): 195–208.
- Abdulrahim, N. 2019. *Managing cybersecurity as a business risk in information technology-based SMEs*. Doctoral dissertation: University of Nairobi, Kenya.
- Abomhara, M. 2015. Cybersecurity and the Internet of Things: Vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, 4(1): 65–88.
- Acuti, D., Pizzetti, M. and Dolnicar, S., 2022. When sustainability backfires: A review on the unintended negative side-effects of product and service sustainability on consumer behavior. *Psychology & Marketing*, 39(10),1933-1945.
- Adepetun, A. 2018. Africa: Cybercrime attacks rise by 30% in Africa. Available: <https://allafrica.com/stories/201811070596.html>. [Accessed: 13 November 2018].
- AgenaRisk. 2021. AgenaRisk. Available: <http://www.agenarisk.com>. [Accessed: 13 November 2020]
- Agrafiotis, I., Nurse, J.R., Goldsmith, M., Creese, S. & Upton, D. 2018. A taxonomy of cyber-harms: Defining the impacts of cyberattacks and understanding how they propagate. *Journal of Cybersecurity*, 4(1):tyy006.
- Aguessy, F.X., 2016. *Évaluation dynamique de risque et calcul de réponses basés sur des modèles d'attaques bayésiens* (Doctoral dissertation, Institut National des Télécommunications).
- Alahmari, A. & Duncan, B. 2020. 'Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence.' Conference Proceedings: International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA): 15).
- Alase, A., 2017. The interpretative phenomenological analysis (IPA): A guide to a good qualitative research approach. *International Journal of Education and Literacy Studies*, 5(2), pp.9-19.
- Aldhamari, R., Nor, M.N.M., Al Farooque, O. & Al-Sabri, H.M., 2022. Risk committee and stock price crash risk in the Malaysian financial sector: The moderating role of institutional ownership. *Journal of Accounting in Emerging Economies*, (ahead-of-print).Alexe, C.M., Alexe, C.G., Popescu, M.A.M. & Costinas, S. 2020. Software solutions for risk management within organizations. *International Scientific Conference eLearning and Software for Education*, 1:437–443.
- Alexei, L.A. & Alexei, A., 2021. Cyber security threat analysis in higher education institutions as a result of distance learning. *International Journal of Scientific & Technology Research*, 10(3): 129–133.
- Alkinani, H.H., Al-Hameedi, A.T.T. & Dunn-Norman, S. 2021, *Minimizing lost circulation non-productive time using expected monetary value and decision tree analysis*. Conference proceedings: SPE Western Regional Meeting. OnePetro. <https://doi.org/10.2118/200844-MS>.
- Almeida, F., Carvalho, I. & Cruz, F. 2018. Structure and challenges of a security policy on small and medium enterprises. *Ksii Transactions on Internet and Information Systems*, 12(2): 747–763.
- Almuhammadi, S. & Alsaleh, M. 2017. Information security maturity model for NIST cyber security framework. *Computer Science & Information Technology (CS & IT)*, 7(3): 51–62.
- Amankwa, E., Looock, M. & Kritzinger, E. 2015. *Enhancing information security education and awareness: proposed characteristics for a model*. Conference proceedings: International Conference on Information Security and Cyber Forensics, 2: 72–77.
- Amrin, N., 2014. 'The Impact of Cyber Security on SMEs.' Master's dissertation, Faculty of Electrical Engineering, Mathematics and Computer Science, Enschede, Netherlands: University of Twente.



- Anderson, M. 2020. Small businesses have a BIG impact on our economy. Available: <https://www.bizcommunity.com/Article/196/841/206855.html>. [Accessed: 13 November 2018].
- Anon. 2018. Cyber breaches cost Australian businesses more than \$600 million a year. Available: <https://nadic.com.au/cyber-risk-for-smes/> [Accessed 13 November 2020].
- Anon. 2019. Cybersecurity tops list of SMB priorities as attacks. Available: <https://smallbiztrends.com/2019/05/2019-small-business-cyber-attack-statistics.html>. [Accessed: 13 November 2018].
- Antunes, M., Maximiano, M., Gomes, R. & Pinto, D. 2021. Information security and cybersecurity management: A case study with SMEs in Portugal. *Journal of Cybersecurity and Privacy*, 1(2): 219–238.
- Anwar, M., He, W., Ash, I., Yuan, X., Li, L. & Xu, L., 2017. Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69: 437–443.
- Armenia, S., Angelini, M., Nonino, F., Palombi, G. & Schlitzer, M.F. 2021. A dynamic simulation approach supports the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems*: 113580.
- Armiger, S.B. 1977. Ethics of nursing research: profile, principles, perspective. *Nursing Research*, 26(5): 330–336.
- Atkins, L. & Wallace, S. 2012. *Qualitative education research*. London; Los Angeles: SAGE.
- Ayandibu, A.O. & Houghton, J. 2017. The role of small and medium scale enterprise in local economic development (LED). *Journal of Business and Retail Management Research*, 11(2): 133–139.
- Babbie, E. & Mouton, J. 2011. *The practice of social research*. Cape Town, South Africa: Oxford University Press.
- Bada, M., Sasse, A.M. & Nurse, J.R. 2019. Cybersecurity awareness campaigns: Why do they fail to change behavior? arXiv preprint arXiv:1901.02672.
- Balan, S., Otto, J., Minasian, E. & Aryal, A. 2017. Data analysis of cybercrimes in businesses. *Information Technology and Management Science*, 20(1): 64–68.
- Bali, S. 2018. Barriers to the development of telemedicine in developing countries. In Heston, TF (Ed.). *Telehealth*. Washington State: IntechOpen. (no pages: online chapter published). <http://www.doi.org/10.5772/intechopen.81723>.
- Barlette, Y., Gundolf, K. & Jaouen, A. 2017. CEOs' information security behavior in SMEs: Does ownership matter? *Systemes 'Information Management*, 22(3): 7–45.
- Barn, R. and Barn, B. 2016. 'An ontological representation of a taxonomy for cybercrime.' European Conference on Information Systems (ECIS), 45: 1–15.
- Beazley Group. 2019. Report on navigating change. Available: <https://investor.relations.beazley.com/reports-and-presentations/annual-reports>. [Accessed: 21 September 2021].
- Bell, S. 2017. Cybersecurity is not just a 'Big Business' issue. *Governance Directions*, 69(9): 536.
- Bendovschi, A. 2015. Cyber-Attacks – Trends, Patterns, and Security Countermeasures. *Procedia Economics and Finance*, 28: 24–31.
- Benz, M. & Chatterjee, D. 2020. Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons*, 63(4): 531–540.
- Berry, C. T. & Berry, R. L. 2018. An initial assessment of small business risk management approaches for cybersecurity threats. *International Journal of Business Continuity and Risk Management*, 8(1): 1.

- Biau, D.J., Boulezaz, S., Casabianca, L., Hamadouche, M., Anract, P. & Chevret, S. 2017. Using Bayesian statistics to estimate the likelihood that a new trial will demonstrate the efficacy of a new treatment. *BMC Medical Research Methodology*, 17(1): 1–10.
- Bisson, D. 2021. 6 Common phishing attacks and how to protect against them. Available: <https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/>. [Accessed: 29 November 2021].
- Blue Turtle Technologies, 2020. ‘Cyber Crime, a pandemic, is hitting the wallet of South African business.’ Available: <https://www.itweb.co.za/content/JN1gPvOYBWPMjL6m> [Accessed: 29 November 2021].
- BoE (Bank of England) 2019. Machine learning in UK financial services. Working Paper. Available: <https://www.bankofengland.co.uk/report/2019/machine-learning-in-uk-financial-services>. [Accessed: on 15th September 2021].
- Boukherouaa, E.B., AlAjmi, K., Deodoro, J., Farias, A. & Ravikumar, R. 2021. Powering the digital economy: Opportunities and risks of artificial intelligence in finance. *Departmental Papers*, 2021: (024).
- Broadhurst, R. & Chang, L.Y. 2013. *Cybercrime in Asia: Trends and challenges. Handbook of Asian Criminology*. Springer: online publication of a chapter: 49–63.
- Brown, A. & Dowling, P. 2001. *Doing Research/Reading Research*. London: Falmer Press.
- Brunner, M., Sauerwein, C., Felderer, M. & Breu, R. 2020. Risk management practices in information security: Exploring the status quo in the DACH region. *Computers & Security*, 92: 101776.
- Busetto, L., Wick, W. & Gumbinger, C. 2020. How to use and assess qualitative research methods. *Neurological Research and Practice*, 2(1): 1–10.
- Business Tech. 2019. These are the new definitions for micro, small and medium enterprises in South Africa. Available: <https://businesstech.co.za/news/business/305592/these-are-the-new-definitions-for-micro-small-and-medium-enterprises-in-south-africa/>. [Accessed: 21 December 2020].
- Cai, B., Huang, L. & Xie, M., 2017. Bayesian networks in fault diagnosis. *Transactions on industrial informatics*, 13(5): 2227–2240.
- Cai, B., Kong, X., Liu, Y., Lin, J., Yuan, X., Xu, H. and Ji, R. 2018. Application of Bayesian networks in reliability evaluation. *Transactions on Industrial Informatics*, 15(4): 2146–2157.
- Chak, S.K., 2015. *Managing Cybersecurity as a business risk for small and medium enterprises*. Doctoral dissertation: John Hopkins University, Baltimore, USA.
- Chang, L. 2013. Formal and informal modalities for policing cybercrime across the Taiwan Strait. *Policing and Society*, 23(4): 540–555.
- Chen, Z., Liu, J., Shen, Y., Simsek, M., Kantarci, B., Mouftah, H.T. and Djukic, P., 2022. Machine learning-enabled IoT security: Open issues and challenges under advanced persistent threats. *ACM Computing Surveys*, 55(5), 1-37.
- Choo, K.K.R. 2011. ‘The cyber threat landscape: Challenges and future research directions.’ *Computers & Security*, 30(8) 719–731.
- Chudasama, D. and Rajput, N., 2021. Protecting ourselves from digital crimes. *National Journal of Cyber Security Law*, 4(1), pp.1-6.
- Cisco Cyber Report. 2018. ‘Annual cybersecurity report.’ Available: <https://www.cisco.com/c/en/us/products/security-reports.html>. [Accessed: 11 May 2018].

- CISOMAG (Cybersecurity Magazine). 2020. 60% of small businesses do not have a cybersecurity policy: survey. Available: <https://cisomag.eccouncil.org/60-of-small-businesses-do-not-have-a-cybersecurity-policy-survey/>. [Accessed: 12 December 2021].
- Clarke J. 1991. Moral dilemmas in Nursing Research. *Nursing Practice*, 4(4): 22–25.
- Cockcroft, S., 2020. What is the NIST Framework? *IT NOW*, 62(4): 48–49.
- Coventry, L., Briggs, P., Blythe, J. & Tran, M. 2014. Using behavioral insights to improve the public’s use of cyber security best practices. *Government Office for Science Summary Report*. Northumbria: University of Northumbria.
- Cox, A. 2008. What's wrong with risk matrices? *Risk Analysis: An International Journal*, 28(2): 497–512.
- Creswell, J.W. & Guetterman, T.C. 2018. *Educational research: Planning, conducting, and evaluating quantitative and qualitative research*. 6th ed.
- Creswell, J.W. 2003. *Research design: Qualitative, quantitative, and mixed methods approach* 2nd ed. Thousand Oaks, CA: Sage.
- Creswell, J.W., 2002. *Educational research: Planning, conducting, and evaluating quantitative* (Vol. 7). Upper Saddle River, NJ: Prentice Hall.
- Crichton, D. 1999. The risk triangle. *Natural disaster management*, 102(3).
- Crichton, D. 2009. *The Risk Triangle*. Available on <http://www.ilankelman.org/crichton/1999risktriangle.pdf>. [Accessed: on 17 May 2021].
- Crovini, C., Santoro, G. and Ossola, G. 2021. Rethinking risk management in entrepreneurial SMEs: Towards the integration with the decision-making process. *Management Decision*, 59(5): 1085–1113.
- Dash, S. 2017. PMP Prep: Decision tree analysis in risk management. Available: <https://www.mpug.com/pmp-prep-decision-tree-analysis-in-risk-management/>. [Accessed: 12 December 2021].
- Davis, R. 2014. “10 Cyber Security Measures That Every Small Business Must Take” retrieved from <https://tech.co/news/10-cyber-security-measures-every-small-business-must-take-2014-11> [Accessed: 16 February 2019]
- de Araújo Lima, P.F., Crema, M. and Verbano, C., 2020. Risk management in SMEs: A systematic literature review and future directions. *European Management Journal*, 38(1), 78-94.
- De Vos, A.S. & Fouché, C.B. 1998. General introduction to research design, data collection methods, and data analysis. In De Vos (ed). *Research at the grassroots. A primer for the caring professions*. Pretoria: Van Schaik Publishers. [357-363].
- De Wilde, L. 2016. *A Bayesian network model for predicting data breaches*. Enschede, Netherlands: The University of Twente, in cooperation with the Delft University of Technology.
- Demirkan, S., Demirkan, I. & McKee, A. 2020. Blockchain technology in the future of business cyber security and accounting. *Journal of Management Analytics*, 7(2): 189–208.
- Department of Telecommunications and Postal Services (DTPS) 2017. Cyber-security, Briefing to the Portfolio Committee, 22 August 2017. Presentation to the Portfolio Committee on Telecommunications and Postal Services, Cape Town, Parliament of the Republic of South Africa [Accessed on 13 November 2018]
- Dilek, S., Çakır, H. & Aydın, M. 2015. Applications of artificial intelligence techniques to combating cyber crimes: A review. *arXiv preprint arXiv:1502.03552*.

- Dirgiatmo, Y., Abdullah, Z. and Ali, R.H.R.M., 2020. Social media practices in Indonesian SMEs. *International Journal of Business Information Systems*, 35(1), 3-26.
- Dlamini, W.M. 2011. Application of Bayesian networks for fire risk mapping using GIS and remote sensing data. *GeoJournal*, 76(3): 283–296.
- Doktoralina, C. & Apollo, A. 2019. The contribution of strategic management accounting in supply chain outcomes and logistic firm profitability. *Uncertain Supply Chain Management*, 7(2): 145–156.
- DTPS (Department of Telecommunications and Postal Services), 2017. Cyber-security, Briefing to the Portfolio Committee, 22 August 2017. Presentation to the Portfolio Committee on Telecommunications and Postal Services, Cape Town, Parliament of the Republic of South Africa [accessed on 13 November 2018]
- Durrheim, K., 2004. Research Design. In BlancheM.T. & Durrheim, K. (Eds). *Research in practice: Applied methods for the social science*. Cape Town: University of Cape Town Press. [29–53]
- Dwivedi, A.D., Srivastava, G., Dhar, S. and Singh, R., 2019. A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors*, 19(2), 326.
- Dzomira, S. 2014. Electronic fraud (cyber fraud) risk in the banking industry, Zimbabwe. *Risk Governance and Control: Financial Markets and Institutions*, 4(2):.16–26.
- Eboibi, F.E., 2021. Cybercriminals and Coronavirus cybercrimes in Nigeria, the United States of America and the United Kingdom: cyber hygiene and preventive enforcement measures. *Commonwealth Law Bulletin*, 47(1), pp.113-142.
- Eian, I.C., Yong, L.K., Li, M.Y.X., Qi, Y.H., & Zahra, F. 2020. Cyber Attacks in the Era of Covid-19 and Possible Solution Domains, Preprints. doi:10.20944/preprints202009.0630.v1
- Eiza, M., Okeke, R.I., Dempsey, J. & Ta, V.T. 2021. Keep calm and carry on with cybersecurity@ home: A framework for securing homeworking IT environment. *International Journal on Cyber Situational Awareness*, 5(1): 1–25.
- Elky, S. 2006. *An Introduction to Information System Risk Management*, SANS Institute InfoSec Reading Room SANS Institute, viewed 16 April 2011, from [http://www.sans.org/reading\\_room/whitepapers/auditing/introduction-information-system-risk-management\\_1204](http://www.sans.org/reading_room/whitepapers/auditing/introduction-information-system-risk-management_1204).
- Elmrabit, N., Yang, S.H., Yang, L. & Zhou, H. 2020. Insider threat risk prediction based on the Bayesian network. *Computers & Security*, 96: 101908.
- ENISA (The European Union Agency for Cybersecurity). 2019. Cybersecurity culture guidelines: behavioural aspects of cybersecurity. Available: [www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity/](http://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity/). (Accessed 31 January 2019).
- Eno-Akpa, R.N., 2016. The Case for an African Solution to Cybercrime-A Critical Assessment of the African Union Convention on Security in Cyberspace and Personal Data Protection. *Mtafiti Mwafrika (African Researcher)*, 31, pp.1-71.
- Ergen, A., Ünal, A.N. & Saygili, M.S., 2021. Is it possible to change the cyber security behaviours of employees? Barriers and promoters. *Academic Journal of Interdisciplinary Studies*, 10(4): 210.
- Eugen, P. & Petruț, D. 2018. Exploring the new era of cybersecurity governance. *Ovidius University Annals, Economic Sciences Series*: 18(1): 358–363.
- Eybers, S. and Mvundla, Z., 2022. Investigating cyber security awareness (CSA) amongst managers in small and medium enterprises (SMEs). In *Comprehensible Science: ICCS 2021*, 180-191. Springer International Publishing.
- Falcon Report, online 2020. “Data breach costs SA companies R40.2 million average in 2020,” available from <https://www.iol.co.za/business-report/companies/data-breach-costs-sa-companies-r402-million-average-in-2020-6649ae0a-b803-482c-978f-b395517c7fa7> [accessed on 17 December 2021].

- Falkner, E.M. & Hiebl, M.R. 2015. Risk management in SMEs: A systematic review of available evidence. *The Journal of Risk Finance*, 16(2): 122–144.
- Feng, N. and Li, M., 2011. An information systems security risk assessment model under an uncertain environment. *Applied Soft Computing*, 11(7), pp.4332-4340.
- Fenton, N. E. & Neil, M. 2014. Decision support software for probabilistic risk assessment using Bayesian Networks. *IEEE Software*, 31(2): 21–26.
- Fenton, N. E. & Neil, M. 2018. Risk assessment and decision analysis with Bayesian networks. Cleveland, Ohio: CRC Press (now part of Taylor and Francis Group).
- Fernandez de Arroyabe, I. & Fernandez de Arroyabe, J.C. 2021. The severity and effects of Cyber-breaches in SMEs: A machine learning approach. *Enterprise Information Systems*: 1–27.
- Fortuin, A., 2021. *The effects of mobile cloud accounting on the operations of small, medium and micro-enterprises in selected Cape Town markets* (Doctoral dissertation, Cape Peninsula University of Technology).
- Fripp, C. 2014. Cybercrime costs South Africa about R5.5 billion a year. Available: <https://www.htxt.co.za/2014/11/11/cybercrime-costs-south-africa-about-r5-8-billion-a-year/> [Accessed: 06 September 2018].
- Frosdick, S. 1997. The techniques of risk analysis are insufficient in themselves. *Disaster Prevention and Management: An International Journal*. 6(3): 165–177, MCB University Press.
- Gashami, J.P.G., Libaque-Saenz, C.F. and Chang, Y., 2020. Social-media-based risk communication for data co-security on the cloud. *Industrial Management & Data Systems*, 120(3), 442-463.
- Ghasemi, F., Sari, M.H.M., Yousefi, V., Falsafi, R. & Tamošaitienė, J. 2018. Project portfolio risks identification and analysis, considering project risk interactions and using Bayesian networks. *Sustainability*, 10(5): 1609.
- Gheorghică, D & Croitoru, V. 2016. *A new framework for enhanced measurable cybersecurity in computer networks*. Conference Proceedings: International Conference on Communications (COMM): 285–290).IEEE.
- Goldenson, J. and Goldenson, M.L. 2016. ‘Cyberrisk for small and medium-sized enterprises’. Available: <https://goldensoncenter.uconn.edu/wp-content/uploads/sites/912/2014/09/CyberRiskDraftReport-9-27-2016-Final-without-comments.pdf>. [Accessed: 11 June 2021].
- González-Manzano, L., & De Fuentes, J.M. 2019. Design recommendations for online cybersecurity courses. *Computers & Security*, 80: 238–256.
- Graham, J.D. and Wiener, J.W. 1995. *Risk versus risk: Tradeoffs in health and environmental protection*. Cambridge, MA: Harvard University Press.
- Grandell, J. 1991. *Aspects of risk theory*. Berlin: Springer.
- Gregoriades, A. & Karakostas, B. 2004. Unifying business objects and system dynamics as a paradigm for developing decision support systems. *Decision Support Systems*, 37(2): 307–311.
- Gundu, T. 2019. *Acknowledging and reducing the knowing and doing gap in employee cybersecurity compliance*. Conference Proceedings: International Conference on Cyber Warfare and Security, 14: 94–102.
- Gupta, R.P. 2017. *Remote sensing geology*. Berlin, Germany: Springer.
- Hadlington, L. 2017. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors. *Heliyon*, 3(7): e00346.
- Han, J., Kim, Y.J. & Kim, H., 2017. An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security*, 66: 52–65.

- Hans, S. 2016. Why artificial intelligence is a game-changer for risk management. Available: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/us-ai-risk-powers-performance.pdf> [Accessed: 31 May 2019].
- Hashedout Report. 2019. 15 small business cyber security statistics that you need to know. Available: <https://www.thesslstore.com/blog/15-small-business-cyber-security-statistics-that-you-need-to-know/>. [Accessed: 21 September 2021].
- Henson, J and Garfield, J. 2016. What attitude changes are needed to cause SMEs to take a strategic approach to information security? *Athens Journal of Business and Economics* 2(3): 303–318.
- Herath, T.B., Khanna, P. & Ahmed, M. 2022. Cybersecurity practices for social media users: A systematic literature review. *Journal of Cybersecurity and Privacy*, 2(1): 1–18.
- Herjavec Group, 2019. Official Annual Cybercrime Report. A report from Cybersecurity Ventures sponsored Herjavec Group. Available: <https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/>. [Accessed: 06 September 2021].
- Hertati, L., Widiyanti, M., Desfitriana, D., Syafarudin, A. and Safkaur, O., 2020. The effects of economic crisis on business finance. *International Journal of Economics and Financial Issues*, 10(3), p.236.
- Hoffmann, R., Napiórkowski, J., Protasowicki, T. & Stanik, J. 2020, Measurement models of information security based on the principles and practices for a risk-based approach. *Procedia Manufacturing*, 44: 647–654.
- Hoffower, H. 2018. There is a good chance you're a victim of credit card scams, and you do not even know it — here is what to do. Available: <https://www.businessinsider.com/credit-card-fraud-scam-what-to-do-2018-8?IR=T> [Accessed: 14 February 2019].
- Howard, L.S. 2018. SMEs underestimate cyber risks which could prove ‘fatal’: Allianz Report. Available: <https://www.insurancejournal.com/news/international/2018/02/21/481113.htm> [Accessed: 12 November 2018].
- Howard, L.S. 2018. SMEs Underestimate Cyber Risks Which Could Prove ‘Fatal’: Allianz Report. Available from <https://www.insurancejournal.com/news/international/2018/02/21/481113.htm> [Accessed on 12 November 2018]
- <https://businesstech.co.za/news/software/591486/small-businesses-in-south-africa-beware-cyber-criminals-are-coming-for-your-password/#:~:text=In%202022%2C%20the%20number%20of,to%2012%20344%20in%202021.> [Accessed: 13 May 2023].
- Huang, K., Siegel, M. and Madnick, S. 2018. ‘Systematically understanding the cyber-attack business: A survey.’ *ACM Computing Surveys (CSUR)*, 51(4): 1–36.
- Hubbard, J. 2019. SA business underplaying the danger of cybercrime. Available: <https://www.news24.com/fin24/finweek/business-and-economy/sa-business-underplaying-the-danger-of-cybercrime-20190313>. [Accessed: 14 February 2020].
- IBM (2018). “Managing Cybersecurity Risk in Government”: An Implementation Model. Available from <http://www.businessofgovernment.org/> [Accessed on 12 November 2018]
- Ifinedo, P. 2012. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1): 83–95.
- Iguer, H., Medromi, H., Sayouti, A., Elhasnaoui, S. & Faris, S. 2014. *The impact of cybersecurity issues on businesses and governments: A framework for implementing a cybersecurity plan*. Conference proceedings: International Conference on Future Internet of Things and Cloud: 316–321). IEEE.
- Iloiu, M. & Csimga, D. 2009. Project RISK evaluation methods - Sensitivity Analysis. Romania: the University of Petroșani, Department of Economics, 9(2): 33–38.



- Imgraben, J., Engelbrecht, A. & Choo, K.K.R. 2014. Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. *Behaviour & Information Technology*, 33(12): 1347–1360.
- IOL staff reporter (2017). “SA has the third highest number of cybercrime victims in the world” Available from <https://www.iol.co.za/capetimes/news/sa-has-third-highest-number-of-cybercrime-victims-in-world-11594553> [Accessed on 20 July 2018]
- ISO (International Organisation for Standardisation). 2002. Risk management vocabulary. ISO/IEC Guide 73. Geneva: ISO.
- ISO (International Organisation for Standardisation). 2018. ISO 31000:2018 (E) – Risk management – principles and guidelines. Available: <https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en> [Accessed 1 April 2023].
- IT News, Africa. Cybersecurity report 2017: Africa in Top 10 targeted regions. 2017. Available: <http://www.itnewsafrika.com/2017/12/cybersecurityreport-2017-africa-in-top-10-targeted-regions/>. [Accessed: 25 October 2018].
- Jain, A.K., Sahoo, S.R. and Kaubiyal, J., 2021. Online social networks security and privacy: comprehensive review and analysis. *Complex & Intelligent Systems*, 7(5), 2157-2177.
- Jain, A.K., Sahoo, S.R. and Kaubiyal, J., 2021. Online social networks security and privacy: comprehensive review and analysis. *Complex & Intelligent Systems*, 7(5), 2157-2177.
- Jensen, F.V. 1996. *An introduction to Bayesian networks*, 210: 1–178. London: UCL Press.
- Joint Research Centre 2019. A proposal for a European cybersecurity taxonomy. Publications Office of the European Union. Available: <https://publications.jrc.ec.europa.eu/repository/handle/JRC118089>. [Accessed: 18th June 2020].
- Jones, J.A. 2006. An introduction to Factor Analysis of Information Risk (FAIR). *Norwich Journal of Information Assurance*, 2(1): 67.
- Jordaan, P. 2014. Information security awareness in small information technology-dependent business organizations, Master’s dissertation, Department of Business Management, University of Johannesburg, South Africa.
- Kabanda, G. 2018. ‘A cybersecurity culture framework and its impact on Zimbabwean organizations.’ *Asian Journal of Management, Engineering & Computer Science*, 3(4): 17–34.
- Kabanda, G. 2020. *A Bayesian network model for machine learning and cybersecurity*. Conference Proceedings: 2nd Africa-Asia Dialogue Network (AADN). International Conference on Advances in Business Management and Electronic Commerce Research: 1–7).
- Kahle, J.H., Marcon, É, Ghezzi, A. & Frank, A.G. 2020. Smart products value creation in SMEs innovation ecosystems. *Technological Forecasting and Social Change*, 156: 120024.
- Kaigorodova, G.N., Mustafina, A.A., Pyrkova, G.K., Vyukov, M.G. & Davletshina, L.M. 2019. Cyber risks for insurance company. *Coastal Research Library*: 669–677. [https://doi.org/10.1007/978-3-030-11367-4\\_64](https://doi.org/10.1007/978-3-030-11367-4_64).
- Karabacak, B. & Sogukpinar, I. 2005. ISRAM: information security risk analysis method. *Computers & Security*, 24(2): 147–159.
- Karaci, A., Akyüz, H.İ. & Bilgici, G. 2017. Üniversite öğrencilerinin siber güvenlik davranışlarının incelenmesi. *Kastamonu Eğitim Dergisi*, 25(6): 2079–2094.
- Kaur, J. & Mustafa, N. 2013. Examining the effects of knowledge, attitude and behavior on information security awareness: A case on SME. Conference Proceedings: International Conference on Research and Innovation in Information Systems (ICRIIS): 286–290).IEEE.

- Kayumbe, A. & Michael, L., 2021. Cyber threats: Can small businesses in Tanzania outsmart Cybercriminals? *International Research Journal of Advanced Engineering and Science*, 6(1): 141–144.
- Khan, N.A., Brohi, S.N. & Zaman, N. 2020. Ten deadly cyber security threats amid COVID-19 pandemic. *TechRxiv Powered by IEEE*:394–399.
- Kirwan, G. & Power, A. 2012. Hacking: Legal and ethical aspects of an ambiguous activity. *Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices*: 21–36).
- Kite, M. J. S. 2009. *Information Security Policy*, viewed 17 May 2013, from <http://www.abdn.ac.uk/hr/uploads/files/information-security-policy.pdf>.
- Kjærulff, U.B. & Madsen, A.L. 2006. Probabilistic networks for practitioners: A guide to construction and analysis of Bayesian networks and influence diagrams. Department of Computer Science, Aalborg University, Denmark: HUGIN Expert A/S.
- Kobis, P. 2021. Human factor aspects in information security management in the traditional IT and cloud computing models. *Operations Research and Decisions*, 1: 61–76.
- Koeze, R. 2017. 'Designing A cyber risk assessment tool for small to medium enterprises.' The Delft University Of Technology, Faculty of Technology, Policy and Management Research conducted at KPMG Advisory NV November 2017 Electronic version. Available: <http://repository.tudelft.nl>. [Accessed: 15 June 2018]
- Kshetri, N. 2006. The simple economics of cybercrime. *IEEE Security and Privacy*, 4: 33–39.
- Kumar, T.V. 2019. Variation in the perception of desired qualities of police officers among trainees and senior police officers. Insights into the process and efficacy of police training. *International Journal of Comparative and Applied Criminal Justice*, 43(3): 241–262.
- Kumhar, D., Kewat, A. and Kumar, A., 2022. Internet Security: Threats and Its Preventive Measures. In *Advances in VLSI, Communication, and Signal Processing: Select Proceedings of VCAS 2021*, 753-766. Singapore: Springer Nature Singapore.
- Kupec, V. & Pisar, P. 2021. Auditing and controlling as a tool for SME marketing risk management. *Marketing and Management of Innovations*, 12(1): 225–235.
- Kure, H.I., Islam, S. & Razzaque, M.A. 2018. An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences*, 8(6): 898.
- Kurpjuhn, T. 2015. The SME security challenge. *Computer Fraud & Security*, 3(3): 5–7.
- Kwon, R., Ashley, T., Castleberry, J., Mckenzie, P. & Gourisetti, S.N.G. 2020. Cyber threat dictionary using MITRE ATT&CK matrix and NIST cybersecurity framework mapping.' *Resilience Week (RWS)*: 106–112). IEEE.
- Lallie, H.S., Shepherd, L.A., Nurse, J.R., Erola, A., Epiphaniou, G., Maple, C. & Bellekens, X. 2020. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, 105: 102248.
- Lee, J.W., 2019. Organizational usage of social media for corporate reputation management. *Becker, Kip*, 231-240.
- Leedy, P.D. 1997. *Practical research: Planning and design*. 6th ed.. New Jersey: Prentice-Hall.
- Lejaka, T.K., Da Veiga, A. & Loock, M. 2019. 'Cybersecurity awareness for small, medium and micro enterprises (SMMEs) in South Africa.' Conference Proceedings on ICTAS. <https://doi.org/10.1109/ictas.2019.8703609>.
- Levine, R. J. 1981. *Ethics and Regulation of Clinical Research*. Baltimore: Urban & Schwarzenberg.
- Li, L., He, W., Xu, L., Ash, I., Anwar, M. & Yuan, X. 2019. Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, 45: 13–24.



- Li, M., Hong, M. & Zhang, R. 2018. Improved Bayesian network-based risk model and its application in disaster risk assessment. *International Journal of Disaster Risk Science*, 9(2): 237–248.
- Linington, D. 2016. 8.8 million South Africans have fallen victim to cybercrime. Available: <http://www.itnewsafrica.com/tag/cybercrime-stats/> [Accessed: 15 May 2018].
- Liu, M., Wang, T., Skidmore, A.K., Liu, X. & Li, M., 2019. Identifying rice stress on a regional scale from multi-temporal satellite images using a Bayesian method. *Environmental Pollution*, 247: 488–498.
- Lloyd, G. 2020. The business benefits of cyber security for SMEs. *Computer Fraud & Security*, 2020(2): 14–17.
- Loonam, J., J. Zwiendelaar, V. Kumar & C. Booth. 2020. Cyber-resiliency for digital enterprises: A strategic leadership perspective. *IEEE Transactions on Engineering Management*: 1–14.
- Mahembe, E. 2011. Literature review on small and medium enterprises' access to credit and support in South Africa. National Credit Regulator. Available: [http://www.ncr.org.za/pdfs/Literature%20Review%20on%20SME%20Access%20to%20Credit%20in%20South%20Africa\\_Final%20Report\\_NCR\\_Dec%202011.pdf](http://www.ncr.org.za/pdfs/Literature%20Review%20on%20SME%20Access%20to%20Credit%20in%20South%20Africa_Final%20Report_NCR_Dec%202011.pdf). (Accessed: 28 December 2019).
- Mahn, A., Marron, J., Quinn, S. & Topper, D. 2021. Getting started with the NIST cybersecurity framework: A quick guide. NIST Special Publication 1271. <https://doi.org/10.6028/NIST.SP.1271>.
- Makina, D., Fanta, A.B., Mutsonziwa, K., Khumalo, J. & Maposa, O. 2015. Financial access and SME size in South Africa. Occasional Paper: 001–2015.
- Marais, J. 2018. SA ‘completely out of step’ with global SME growth trends. Available: <https://www.businesslive.co.za/bd/business-and-economy/2018-07-25-sa-completely-out-of-step-with-global-sme-growth-trends/>. [Accessed: 15 March 2019].
- Marzulina, L., Harto, L, Harto, K.H. & Erlina, D. 2022. Challenges and Strategies Used by English Teachers in Teaching English Language Skills to Young Learners. *Challenges and Strategies Used by English Teachers in Teaching English Language Skills to Young Learners*, 12(2): 382–387. <https://doi.org/10.17507/tpls.1202.22>.
- McGuire, M. & Dowling, S. 2013. Cybercrime: A review of the evidence: Summary of key findings and implications. Home Office Research Report 75. London: Home Office.
- McMahon, R., Bressler, M.S. and Bressler, L., 2016. New global cybercrime calls for high-tech cyber-cops *Journal of Legal, Ethical and Regulatory Issues*: 19(1):26.
- Metsänen, T. 2022. Application of decision tree analysis and expected monetary value technique in quantitative risk management: Evaluation of less risky investment strategy. Finland *OSUVA Open Science Emerald Publishers*, np.. Online PDF publication. <https://doi.org/10.1108/IJPSM-01-2022-0008>.
- Mierzwa, S. & Scott, J. 2017. *Cybersecurity in non-profit and non-governmental organizations. Results of a survey*. Washington DC: Institute for Critical Infrastructure Technology.
- Millaire, P., Sathe, A. & Thielen, P. 2015. What All cyber criminals know: Small & midsize businesses with little or no cybersecurity are ideal targets. Available: <https://www.chubb.com/my-en/articles/smes-with-little-or-no-cybersecurity-are-ideal-targets.aspx>. [Accessed: 15th of May 2019].
- Mo, S.Y.K., Beling, P.A. & Crowther, K.G. 2009. *Quantitative assessment of cybersecurity risk using Bayesian Network-based Model*. Conference Proceedings: Systems and Information Engineering Design Symposium: 183–187). IEEE.
- Moola, N. 2020. South Africa must support SMEs to save jobs. Available: <https://www.dailymaverick.co.za/article/2020-04-07-south-africa-must-support-smes-to-save-jobs/#gsc.tab=0>. [Accessed: 11 August 2020].
- Mottahedi, A., Sereshki, F., Ataei, M., Nouri Qarahasanlou, A. & Barabadi, A. 2021. The resilience of critical infrastructure systems: A systematic literature review. *Energies*, 14(6): 1571.

- Moyo, M., 2014. *Information Security Risk Management in Small-scale Organisations: A Case Study of Secondary Schools' Computerised Information Systems* (Doctoral dissertation, University of South Africa).
- Mugarura, N. & Ssali, E. 2020. Intricacies of anti-money laundering and cyber-crimes regulation in a global fluid system. *Journal of Money Laundering Control*, 24(1): 10–28.
- Mutia Sobihah, A.H., Ahmad Munir, M.S. and Mohamad Saladin, M., 2014. The relationship between e-commerce adoption and organization performance. *International Journal of Business and Management*, 9(1), pp.56-63.
- Nasir, A., Naderi, M.A. & Momeni, S.M. 2020. 'Risk management of information technology projects using Bayesian networks.' *Practical IT*, 1(5): 01–10.
- National Cyber Security Strategy (NCSS) 2016-2021 report online. Available from [https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national\\_cyber\\_security\\_strategy\\_2016.pdf](https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf) [Accessed on 13 November 2018].
- Ncubukezi, T. 2021. *An exploration of the malware impact on the end devices*. Conference Proceedings: CPUT Postgraduate Conference: 70.
- Ncubukezi, T. and Mwansa, L. 2021a. 'Best practices used by businesses to maintain good cyber hygiene during Covid-19 pandemic.' *Journal of Internet Technology and Secured Transactions*, 9 (1):.714–721.
- Ncubukezi, T. and Mwansa, L. 2021b. 'Security of the business activities in cyberspace: An Activity Theory Perspective.' *Information Society*, 16: 27–33.
- Ncubukezi, T., 2022a. Human Errors: A Cybersecurity Concern and the Weakest Link to Small Businesses. *Conference Proceedings: International Conference on Cyber Warfare and Security*, 17(1):395–403.
- Ncubukezi, T., 2022b. Impact of information security threats on small businesses during the Covid-19 pandemic. *Conference Proceedings: European Conference on Cyber Warfare and Security*, 21(1): 401–410.
- Ncubukezi, T., Mwansa, L. & Rocaries, F. 2020b. 'A review of the current cyber hygiene in small and medium-sized businesses.' Conference Proceedings: International Conference for Internet Technology and Secured Transactions (ICITST), 15: 1–6. IEEE.
- Ncubukezi, T., Mwansa, L. and Rocaries, F. 2021. Analysis and impact of the cybercrimes in the Western Cape small and medium-sized businesses. *Conference Proceedings: International Conference on Cyber Warfare and Security*, 16: 425–235.
- Ngugi, E.W. 2016. E-Commerce Security and Performance of SMEs in Nairobi, Kenya. Master's dissertation in Business Administration (MBA), School of Business, University of Nairobi, Kenya.
- Ngwenya, B. 2020. It's important to empower small businesses. Here's why. Available: <https://www.news24.com/citypress/voices/its-important-to-empower-small-businesses-heres-why-20181205>. [Accessed: 12 November 2018].
- Nicho, M. & Muumaar, S. 2016. Towards a taxonomy of challenges in an integrated IT governance framework implementation. *Journal of International Technology and Information Management*, 25(2): 2.
- Ning, H., Ye, X., Bouras, M.A., Wei, D. and Daneshmand, M. 2018. 'General cyberspace: Cyberspace and cyber-enabled spaces.' *IEEE Internet of Things Journal*, 5(3): 1843–1856.
- NIST (National Institute of Standards and Technology) Special Publication 800-181. 2017. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. National Institute of Standards and Technology (NIST). <https://doi.org/10.6028/NIST.SP.800-181>.
- NIST (National Institute of Standards and Technology). 2014. Framework for improving critical infrastructure cybersecurity: Version 1.0. Available from: <http://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>. [Accessed: 16 November 2020].

- NIST (National Institute of Standards and Technology). 2018. Framework Documents. Available from: <https://www.nist.gov/cyberframework/framework-documents> [Accessed: 16 November 2020].
- Nketekete, M., Emuze, F. & Smallwood, J. 2016. Risk management in public sector construction projects: Case studies in Lesotho, *Acta Structilia*, 23(2): 1–24.
- Nyanchama, M, 2005. Enterprise vulnerability management and its role in information security management. *Information Systems Security*, 14(3): 29–56.
- Osborn, E. 2015. Business versus technology: Sources of the perceived lack of cyber security in SMEs. *CDT Technical Paper* 01/15. Oxford: The University of Oxford.
- Osborn, E. and Simpson, A. 2018. ‘Risk and the small-scale cyber security decision making dialogue—a UK case study’. *The Computer Journal*, 61(4): 472–495.
- Parikh, A., 2019. *Cloud security and platform thinking: An analysis of Cisco Umbrella, cloud-delivered enterprise security*. Doctoral thesis: Massachusetts: Massachusetts Institute of Technology..
- Paté-Cornell, M.E., Kuypers, M., Smith, M. & Keller, P. 2018. Cyber risk management for critical infrastructure: A risk analysis model and three case studies. *Risk Analysis*, 38(2): 226–241.
- Patterson, J., 2017. *Cyber-security policy decisions in small businesses*. (Doctoral thesis: Minneapolis: Walden University).
- Paulsen, C. 2016. Cybersecurity in small businesses. *Computer*, 49(8): 92–97.
- Perez, C., 2020. *A Cybersecurity Strategy for the Small Business*. Doctoral thesis: New York: Utica University College.
- Peters, G., Shevchenko, P.V. and Cohen, R., 2018. *Understanding cyber-risk and cyber-insurance*. New South Wales, Australia: Macquarie University Faculty of Business & Economics Research Paper.
- Peyper, L. 2016. 32% of SMEs in SA are at risk of cyber-attacks – Cwele. Available: <https://www.fin24.com/Economy/32-of-smes-in-sa-at-risk-of-cyber-attacks-cwele-20160309>. [Accessed: 18 March 2019 ].
- PMI (Project Management Institute). 2008. A guide to the project management body of knowledge (PMBOK). PA: Project Management Institute.
- PMI (Project Management Institute). 2013. A guide to the project management body of knowledge (PMBOK® Guide). 5th Edition. Newtown Square, Pennsylvania: Project Management Institute, Inc.
- Ponemon Institute LLC. 2016. The state of cybersecurity in small & medium-sized businesses (SMB),’ Available: [https://keepersecurity.com/assets/pdf/The\\_2016\\_State\\_of\\_SMB\\_Cybersecurity\\_Research\\_by\\_Keeper\\_and\\_Ponemon.pdf](https://keepersecurity.com/assets/pdf/The_2016_State_of_SMB_Cybersecurity_Research_by_Keeper_and_Ponemon.pdf), [Accessed: 20 November 2018].
- Ponsard, C., Grandclaudon, J. & Dallons, G. 2018. *Towards a cyber security label for SMEs: A European perspective*. Conference proceedings: International Conference on Information Systems Security and Privacy, (ICISSP), 4: 426–431.
- Pritom, M.M.A., Schweitzer, K.M., Bateman, R.M., Xu, M. & Xu, S. 2020. *Characterizing the landscape of covid-19 themed cyberattacks and defenses*. Conference proceedings: IEEE International Conference on Intelligence and Security Informatics (ISI): 1–6. IEEE.
- Purnomo, I.D. & Wiguna, I.P.A. 2021. Risk evaluation of the use of the umbrella contract for the construction project for medium voltage distribution in South Surabaya Region using the Expected Monetary Value. *IPTEK Journal of Proceedings Series*, (3): 322–325.
- Quartey, P. 2015. Issues in SME Development in Ghana and South Africa. *International Research Journal of Finance and Economics*. 39: 218–228.

- Rahi, S. 2017. Research design and methods: A systematic review of research paradigms, sampling issues, and instruments development. *International Journal of Economics & Management Sciences*, 6(2): 1–5.
- Rashid, Y., Rashid, A., Warraich, M.A., Sabir, S.S. & Waseem, A. 2019. Case study method: A step-by-step guide for business researchers. *International Journal of Qualitative Methods*, 18: 1609406919862424.
- Rastenis, J., Ramanauskaitė, S., Janulevičius, J., Čenys, A., Slotkienė, A. & Pakrijauskas, K., 2020. E-mail-based phishing attack taxonomy. *Applied Sciences*, 10(7): 23–63.
- Reddy, K.S. 2016. Cybercrimes in India and the mechanism to prevent them. *International Journal of Innovative Research in Information Security (IJIRIS)*, (3)9: 29–32.
- Reguero, B.G., Beck, M.W., Schmid, D., Stadtmüller, D., Raeppe, J., Schüssele, S. & Pfliegner, K. 2020. Financing coastal resilience by combining nature-based risk reduction with insurance. *Ecological Economics*, 169: 106487.
- Remenyi, D., Williams, B., Money, A. & Swartz, E. 2003. *Doing research in business and management: An introduction to process and method*. London: SAGE Publications.
- Richards, K. 2017. Cost of cybercrime study: Insights on the security investments that make a difference. Michigan, USA: Ponemon Institute.
- Richardson, M.D., Lemoine, P.A., Stephens, W.E. & Waller, R.E. 2020. Planning for cyber security in schools: The human factor. *Educational Planning*, 27(2): 23–39.
- Richardson, V.J., Smith, R.E. & Watson, M.W. 2019. Much ado about nothing: The (lack of) economic impact of data privacy breaches. *Journal of Information Systems*, 33(3): 227–265.
- Rizvi, S., Orr, R.J., Cox, A., Ashokkumar, P. & Rizvi, M.R. 2020. Identifying the attack surface for IoT networks. *Internet of Things*, 9: 100162.
- Robson, C. 1993, *Real world research: A resource for social scientists and practitioner-researchers*. Oxford: Blackwell Publishers.
- Rusi, T. & Lehto, M. 2017. *Cyber threats megatrends in cyberspace*. Conference proceedings: International Conference on Management Leadership and Governance. Academic Conferences and Publishing Limited, 5<sup>th</sup>: 323.
- Russell, S. & Norvig, P. 2010. *Artificial intelligence: A modern approach*. 3rd ed. Upper Saddle River, New Jersey: Pearson Prentice Hall.
- Russell, S.J. & Norvig, P. 2003. *Artificial Intelligence: A modern approach*. 2nd ed.. Hoboken, New Jersey Prentice Hall.
- SABC News. 2017. Cyber attacks are reaching a critical point in SA. Available: <http://www.timenews.co.za/timenews-sabc-news-cyber-attacks-reaching-acritical-point-in-sawednesday-19-april-2017>. [Accessed: 09 November 2018].
- SABRIC (South African Banking Risk Information Centre), 2020, online. *Identity theft*, viewed n.d., from <https://www.sabric.co.za/stay-safe/identity-theft/>.
- SABRIC (South African Banking Risk Information Centre). 2014. Increase in card fraud – Sabric Report. Available: <https://www.fin24.com/Economy/Increase-in-card-fraud-Sabric-20141125>. [Accessed: 14 February 2019].
- Salam, M.T., Imtiaz, H. & Burhan, M., 2021. The perceptions of SME retailers towards the usage of social media marketing amid the COVID-19 crisis. *Journal of Entrepreneurship in Emerging Economies*, 13(4): 588–605.
- Salem, O., Hossain, A. & Kamala, M. 2010. *Awareness program and AI-based tool to reduce risk of phishing attacks*. Conference proceedings: International Conference on Computer and Information Technology, 10<sup>th</sup>: 1418–1423. IEEE.

- Santos-Olmo, A., Sánchez, L.E., Caballero, O.I., Camacho, S. & Fernandez-Medina, E. 2016, The importance of the security culture in SMEs as regards the correct management of the security of their assets, *Future Internet*, 8(4): 30.
- Saravanan, A. and Bama, S.S., 2019. A review on cyber security and the fifth generation cyberattacks. *Oriental Journal of computer science and Technology*, 12(2), 50-56.
- Sarre, R., Lau, L.Y.C. & Chang, L.Y. 2018. Responding to cybercrime: Current trends. *Police Practice and Research*, 19(6): 515–518.
- Sasse, M.A., Brostoff, S. & Weirich, D. 2001. Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *Technology Journal*, 19(3): 122–131.
- Saunders, M., Lewis, P. & Thornhill, A., 2009. Research methods for business students. 5th ed. Harlow, United Kingdom: Pearson Education
- SEDA (The Small Enterprise Development Agency). 2018. SMME Quarterly Update 1st Quarter 2018. Available: <http://www.seda.org.za/Publications/Publications/SMME%20Quarterly%202018-Q1.pdf>. [Accessed: 11 February 2019].
- Sen, P., Ahmed, A. & Islam, R. 2015. A study on e-commerce security issues and solutions. *International Journal of Computer and Communication Systems Engineering*, 2(3): 425–430.
- SenseOn. 2019. The state of cybersecurity SME report. Available: <https://www.senseon.io/sme-cybersecurity-report-2019>. [Accessed: 12 November 2018].
- Serianu Limited, 2017. Africa cybersecurity report 2017, demystifying Africa cybersecurity poverty line.
- Serrano, B.M., González-Cancelas, N., Soler-Flores, F. & Camarero-Orive, A. 2018. Classification and prediction of port variables using Bayesian Networks. *Transport Policy*, 67: 57–66.
- Sevinc, V., Kucuk, O. & Goltas, M., 2020. A Bayesian network model for prediction and analysis of possible forest fire causes. *Forest Ecology and Management*, 457: 117723.
- Shad, M.K., Lai, F.W., Fatt, C.L., Klemeš, J.J. & Bokhari, A. 2019. Integrating sustainability reporting into enterprise risk management and its relationship with business performance: A conceptual framework. *Journal of Cleaner Production*, 208: 415–425.
- Sheehan, B., Murphy, F., Kia, A.N. & Kiely, R. 2021. A quantitative bow-tie cyber risk classification and assessment framework. *Journal of Risk Research*: 1–20.
- Shevchenko, P.V., Jang, J., Malavasi, M., Peters, G.W., Sofronov, G. & Trück, S. 2021. Quantification of cyber risk–risk categories and business sectors. *Available at SSRN*  
Available: <https://ssrn.com/abstract=3858608> or <http://dx.doi.org/10.2139/ssrn.3858608>. [Accessed: 02 February 2022].
- Shukla, S., George, J.P., Tiwari, K. and Kureethara, J.V., 2022. Data Security. In *Data Ethics and Challenges*, 41-59. Singapore: Springer Singapore.
- Shuttleworth, M. 2017. Qualitative vs. quantitative risk analysis: What is the difference? Available: <https://www.project-risk-manager.com/blog/qualitative-and-quantitative-risk-analysis/> [Accessed: 09 November 2018].
- Smit, Y. & Watkins, J.A., 2012. A literature review of small and medium enterprises (SME) risk management practices in South Africa. *African journal of business management*.
- Smith, Y., and J. A. Watkins (2012). “A Literature Review of Small and Medium Enterprises (SME) Risk Management Practices in South Africa,” *African Journal of Business Management* 6(21), 6324– 6330.



- Soiferman, L.K. 2010. Compare and contrast inductive and deductive. Research approaches. Online PDF submission (Eric). Winiipeg, Canada: University of Manitoba. [1–23].
- Solvere, O. 2021. *Cyber Attacks on Small Businesses Increase*. Available from <https://www.solveone.com/pages/cyber-attacks-on-small-businesses-increasing-in-2021/> [accessed on 16 September 2021].
- Soomro, TR and Hussain, M. 2019. Social media-related cybercrimes and techniques for their prevention. *Applied Computer Systems*, 24(1): 9–17.
- Sovacool, B.K. & Del Rio, D.D.F. 2020. Smart home technologies in Europe: A critical review of concepts, benefits, risks, and policies. *Renewable and Sustainable Energy Reviews*, 120: 109663.
- Staff writer, 2022. Small businesses in South Africa beware, cyber criminals are coming for your password. Statistics in South Africa. ‘Quarterly financial statistics (QFS) December 2016’, 2017. Retrieved from <http://www.statssa.gov.za/publications/P0044/P0044December2016.pdf> [Accessed on 25 March 2018].
- Steve, M. 2017.” Cybercrime damages will cost the world \$6 trillion annually by 2021”. Cybercrime Report from Cybersecurity Ventures sponsored by Herjavec Group [Accessed: on the 23rd May 2018]
- Such, J.M., Ciholas, P., Rashid, A., Vidler, J. & Seabrook, T. 2019. Basic cyber hygiene: Does it work? *Computer*, 52(4): 21–31. <https://doi.org/10.1109/mc.2018.2888766>.
- Suh, B., & Han, I. 2003. The impact of customer trust and perception of security control on the acceptance of electronic commerce. *International Journal of Electronic Commerce*, 135-161.
- Sulistyowati, D., Handayani, F. & Suryanto, Y. 2020. Comparative analysis and design of cybersecurity maturity assessment methodology using NIST CSF, COBIT, ISO/IEC 27002, and PCI DSS. *International Journal on Informatics Visualization*, 4(4): 225–230.
- Sutherland, E., 2017. Governance of cybersecurity-the case of South Africa. *The African Journal of Information and Communication*, 20, pp.83-112.
- Sword, A. 2016. “SMEs hit with 7 million cybercrime attacks per year in £5.26 billion blow to UK economy,” *Computer Business Review*, 2018. Available in: <http://www.cbronline.com/news/cybersecurity/business/smes-hit-with-7-million-cyber-crime-attacks-per-year-in-526-billion-blow-to-uk-economy-4919992/> [accessed on 6th of September 2018]
- Tabassum, M., Kosinski, T. & Lipford, H.R. 2019. *I don't own the data: End-user perceptions of smart home device data practices and risks*. Conference proceedings: Symposium on Usable Privacy and Security (SOUPS), 15<sup>th</sup>: 435–450.
- Talwar, S., Dhir, A., Scuotto, V. and Kaur, P., 2021. Barriers and paradoxical recommendation behaviour in online to offline (O2O) services. A convergent mixed-method study. *Journal of Business Research*, 131, 25-39.
- Tam, T., Rao, A. & Hall, J. 2021. The good, the bad and the missing: A Narrative review of cyber-security implications for Australian small businesses. *Computers & Security*:102385.
- Teufel, S., Teufel, B., Aldabbas, M. & Nguyen, M. 2020. Cyber security canvas for SMEs. Conference Proceedings: International Information Security Conference: 20–33). Springer.
- Tiwari, A. 2010. *Information Security Risk Management: An Overview Risk Management: An Essential Guide to Protecting Critical Assets*, [Accessed on the 19<sup>th</sup> viewed 19 September 2012, from <http://www.suite101.com/profile.cfm>.
- Torres, M. & Thompson, N. 2020. Toward a cyber-security adoption framework for primary and secondary education providers. Conference proceedings: Australasian Conference on Information Systems.
- Totade, S., Kadu, V.S., Payghan, V.S. and Dhote, D.P., 2022. Study of Cyber Security. *International Research Journal of Innovations in Engineering and Technology*, 6(10), 122.

- Tranchard, S. 2018. Risk management: The new ISO 31000 keeps risk management simple. *Governance Directions*, 70(4): 180–182.
- Turk, R.W. 2013. Preparing a cyber-security workforce for the 21st Century. Carlisle Barracks Pa: Army War College.
- Twisdale, J.A., 2018. *Exploring SME Vulnerabilities to Cyber-criminal Activities Through Employee Behavior and Internet Access* (Doctoral dissertation, Walden University).
- Uma, M. & Padmavathi, G. 2013. A survey on various cyberattacks and their classification. *International Journal of Network Security*, 15(5): 390–396.
- Vakakis, N., Nikolis, O., Ioannidis, D., Votis, K. & Tzovaras, D. 2019. Cybersecurity in SMEs: The Smart-Home/Office Use Case. In IEEE 24th International Workshop on Computer-Aided Modeling and Design of Communication Links and Networks (CAMAD): 1–7).
- Van Haastreht, M., Sarhan, I., Shojaifar, A., Baumgartner, L., Mallouli, W. & Spruit, M. 2021. *A threat-based cybersecurity risk assessment approach addresses SME needs*. Conference proceedings: International Conference on Availability, Reliability, and Security: 16: 1–12.
- Van Niekerk, B. 2017. An analysis of cyber-incidents in South Africa. *The African Journal of Information and Communication (AJIC)*, 20: 113–132.
- Van Zyl, G. 2016. Anonymous 'hacks' Armscor website. Fin24. Available: <http://www.fin24.com/Tech/News/anonymous-hacks-armscor-website-20160712> [Accessed: 12 November 2018].
- Vaughan, E. & Vaughan, T. 2001. *Essentials of risk management and insurance*. 2nd ed. New York, NY: John Wiley & Sons.
- Venktes, K. 2016. eThekweni municipality website leaks user data – Expert. Fin24. Available: <http://www.fin24.com/Tech/News/ethekweni-municipalitywebsite-leaks-user-data-expert-20160908> [Accessed: 09 November 2018].
- Verizon Enterprise Solutions. 2019. Report on summary of findings. Available: <https://enterprise.verizon.com/resources/reports/dbir/2019/summary-of-findings/>. [Accessed: 12 November 2018].
- Vermeulen, J. (2016). Anonymous hacks SA government database, MyBroadband. Available: <http://mybroadband.co.za/news/security/155030-anonymous-hacks-sa-government-database.html>. [Accessed: 12 November 2019].
- Verzobio, A., El-Awady, A., Ponnambalam, K., Quigley, J. & Zonta, D. 2021. An elicitation process to quantify Bayesian networks for dam failure analysis. *Canadian Journal of Civil Engineering*, 48(10): 1235–1244.
- Vivian, R.W. 2013. “Ending the myth of the St Petersburg paradox” SA Journal of Economic
- Von Solms, R. & Van Niekerk, J. 2013. From information security to cyber security. *Computers & Security*, 38: 97–102.
- Von Solms, S., & Von Solms, R. 2014. Towards cyber safety education in primary schools in Africa. In *Proceedings of the eighth international symposium on human aspects of information security & assurance (HAISA 2014)*.
- Vuba, S. 2019. The missed opportunity: SMMEs in the South African economy. Available: <https://mg.co.za/article/2019-04-12-00-the-missed-opportunity-smmes-in-the-south-african-economy/>. [Accessed: 12 November 2019].
- Wallace, S., Green, K., Johnson, C., Cooper, J. & Gilstrap, C. 2021. An extended TOE Framework for cybersecurity adoption decisions. *Communications of the Association for Information Systems*, 47(2020): 51.
- Wang, J., Neil, M. & Fenton, N. 2020. A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. *Computers & Security*, 89: 101659.

- Watkins, J.A. 2012. A literature review of small and medium enterprises (SME) risk management practices in South Africa. *African journal of business management*, 6(21): 6324–6330.
- Wedawatta, G.S.D., Ingirige, M.J.B. & Amaratunga, R.D.G. 2011. Case study as a research strategy: Investigating extreme weather resilience of construction SMEs in the UK. Manchester, UK: University of Salford.
- Wen, C., Yang, J., Gan, L. & Pan, Y. 2021. Big data-driven internet of things for credit evaluation and early warning in finance. *Future Generation Computer Systems*, 124: 295–307.
- Williams, S. 2020. Cybercrime ranks highest on business concerns for 2020; research finds. Available: <https://itbrief.com.au/story/cyber-crime-ranks-highest-on-business-concerns-for-2020-research-finds> [Accessed: 12 November 2018].
- Wu, H., Dwivedi, A.D. and Srivastava, G., 2021. Security and privacy of patient information in medical systems based on blockchain technology. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, 17(2s), 1-17.
- Xero. 2018. 'The state of South African small business in 2017, a report produced in partnership with World Wide Worx'. Available: <https://www.xero.com/content/dam/xero/pdf/xero-south-africa-state-of-small-business-2017.pdf>. [Accessed: 5 September 2018].
- Xie, P., Li, JH, Ou, X., Liu, P. & Levy, R. 2010. *Using Bayesian networks for cyber security analysis*. Conference Proceedings: International Conference on Dependable Systems & Networks (DSN): 211–220.
- Yang, X.S. 2019. *Introduction to algorithms for data mining and machine learning*. London: Academic Press.
- Yanyan, D. (2018). "Cyber risk biggest headache for SA business – report" available from <https://www.fin24.com/Tech/News/cyber-risk-biggest-headache-for-sa-business-report-20180123> [Accessed: 16 November 2018]
- Yermalovich, P. & Mejri, M. 2020. *Information security risk assessment based on decomposition probability via a Bayesian network*. Conference proceedings: International Symposium on Networks, Computers and Communications (ISNCC): 1–8.
- Yin, R.K. 1994. Discovering the future of the case study. The method in evaluation research. *Evaluation Practice*, 15(3): 283–290.
- Zhang, R. 2013. *Climate change and national ocean strategy: Impact and risk assessment*. Beijing: Meteorological Press (in Chinese). Beijing: Beijing Meteorological Press.
- Zhang, R., Fang, L., He, X. and Wei, C., 2023. Controlling Network Risk in E-commerce. In *The Whole Process of E-commerce Security Management System: Design and Implementation* (121-179). Singapore: Springer Nature Singapore.
- Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F. and Choo, K.K.R. 2021. Artificial intelligence in cyber security: Research advances, challenges and opportunities. *Artificial Intelligence Review*: 1–25.
- Zio, E., 2018. The future of risk assessment. *Reliability Engineering & System Safety*, 177: 176–190.



## **APPENDIX A: Consent letter**

Department of Electrical, electronic, and computer  
Faculty of Engineering and building environment  
Bellville  
April 2021

Dear Sir/Madam

Re: Design, develop, and evaluate a cyber-security risk tool: a case of the small and medium-sized enterprises in South Africa.

I am a postgraduate student in Electrical, Electronic, and Computer Engineering at the Cape Peninsula University of Technology (CPUT), Bellville campus. I am conducting a research project on developing, developing, and evaluating a cyber-security risk tool: a case of small and medium-sized enterprises in South Africa.

Cyber risks within Small and Medium Enterprises (SMEs) are gradually increasing and have become a security concern. This is because; most SMEs entirely depend on Information Technologies and the Internet, which also opens lucrative opportunities to cyber criminals. These crimes leave SMEs vulnerable to cyber risks. The vulnerabilities open a door for information and computer security to be a critical issue for all SMEs. This study aims to analyse, design, develop and evaluate the cybersecurity risk assessment tool for SMEs in South Africa. To achieve this, the researcher must first gather information about the common cybersecurity risks or crimes that SMEs are experiencing. The information will help analyse the cyber risk cause, event, and impact to determine the risk likelihood and proximity to mitigate cybersecurity risks within the SME sector. This study focuses on SMEs from any sector within South Africa with at least a minimum of 1 to 150 employees, generating a turnover of R20 000 to R20 million a year.

I kindly request your participation in a short survey. The questionnaire will take between 30 to 45 minutes. For confidentiality of information, there will be no attempt will be made to identify you with the responses you make. So you are free to respond without any fear of victimization. Recommendations will be used only to inform improvements, with no reference to the identity of the sources. Finally, this research is authorized and complies with the CPUT HOC research ethics guidelines.

Your participation in this research project will be highly appreciated.

Yours Sincerely

Ms. Tabisa Ncubekezi

Cell: 078 155 6723

Email: tabisaphd@gmail.com or 208217673@cput.ac.za

## APPENDIX B: Ethical Clearance



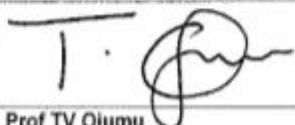
### FACULTY OF ENGINEERING & THE BUILT ENVIRONMENT

On 03 October 2019, the Engineering and Built Environment Ethics Committee of the Cape Peninsula University of Technology granted ethics approval to Ms TABISA NCUBUKEZI student number 208217673 for research activities related to her research proposal at the Cape Peninsula University of Technology.

<b>Title of Proposal</b>	Analysis of cyber security risks in small and medium enterprises in South Africa
--------------------------	--

**Comments:**

Data collection is required  
Permission to collect data obtained

	08/10/2019
Prof TV Ojumu Research and Innovation Coordinator – Faculty of Engineering and the Built Environment (Acting)	Date

2019FEREC-STD-93

## APPENDIX C: Questionnaire

In this section, the survey was shared with research participants that are IT managers, business owners, Chief information officers, or any other position from different business sectors. The participants came from different provinces in the South African country and consisted of four parts: the SME background; identified cyberattacks, cyberthreats and cyberrisks, cyberrisk likelihood and impact, monetary value, and mitigation strategies

Filling in the form costs at least 20 minutes, but spending more time answering the questions was appreciated.

Participation in this research is anonymous.

Thank you for participating!

### 1. Section 1: SME Background

This section of the survey focuses on profiling the SME. It is recommended that this questionnaire be completed by the owner of the business, IT manager, Chief information officer, or any other IT team member with extensive knowledge.

1.1 In which province does your SME operate in?

- Eastern Cape
- Western Cape
- KwaZulu Natal
- Free State
- Northern Cape
- Gauteng

1.2 In which sector does your SME operate in?

- ICT
- Transport and motor trade
- Mining and quarrying
- Manufacturing, retail and wholesale trade
- Electricity, gas, and water
- Accommodation and catering
- Retail estate and business businesses
- Construction and engineering
- Community, social and personal
- Media

1.3 How many employees does your business have?

.....

1.4 How long has your business existed

- 1 to 2 years
- 3 to 5 years
- 6 to 9 years
- More than 10 years

1.5 What is your current position?

- IT manager
- Business manager
- Chief Information Officer
- Other .....

1.6 What is your gender?

- Male
- Female
- They

1.7 What is your age?

.....

## 2 Section 2: Identified cyberattacks, cyber threats, cyber risks, their likelihood and risk impact

This section addresses vulnerabilities that weaken the business. The section looks at the policies, procedures, rules, guidelines, standards, and administration of hardware, software, data, facility, or personnel resources. The point is to identify cybersecurity weaknesses and test how far a potential exploit can compromise your network.

2.1 What are the common cyberattacks that your business experiences, especially during the COVID19 pandemic?

- Lack of computer hardware
- Lack of skilled personnel
- Malfunctioning of the system
- Lack of guidelines
- Unauthorised access
- Poor password criteria
- Data breach
- Viruses
- Worms
- Trojan
- Spyware
- Denial of service
- Phishing
- Human errors

Network failure

## 2.2 What are the common risks experienced by SMEs?

Bad reputation

Business destruction

Poor economic growth

Poor business growth

Lack of client trust

Loss of intellectual property

Malfunctioning of servers and other devices

Unexpected system failure

Limited access to resources

Compromised system

## 2.3 With a Lickert scale of 1 to 6. Rate the most likely risks of experience

1= Unlikely, 2= Unlikely to happen, 3= might happen, 4= likely to happen, 5= very likely to happen and 6= very likely to happen.

System failure

Email bombing

No backup system

Trojan Horse

Phishing

## 2.4 With a Lickert scale of 1 to 6. Rate the most likely risks of experience

1= Rare, 2= Unlikely to happen, 3= might happen, 4= likely to happen, 5= very likely to happen and 6= very likely to happen.

Fraud or theft

Lack of skilled personnel

Stress

Understaffing

Ignorance

Poor decision making

Lack of guidelines

Poor use of security measures

## 2.5 With the Lickert scale of 1 to 6. Rate the network and power risk likelihood

1= Rare, 2= Unlikely to happen, 3= might happen, 4= likely to happen, 5= very likely to happen and 6= very likely to happen.

- Malfunctioning firewalls
- Open wireless network
- Faulty network interfaces
- Poor electrical connections
- Outdated antiviruses and antispyware
- Equipment failure
- Faulty transmission media

2.6 With a Lickert scale of 1 to 6. Rate the device access and encryption risk likelihood

1= Rare, 2= Unlikely to happen, 3= might happen, 4= likely to happen, 5= very likely to happen and 6= very likely to happen.

- Unauthorised access to the software
- Unauthorised user registration
- Unauthorised access to physical facilities
- Unauthorised access to password files
- Unauthorised access to mobile devices, PCs, and laptops
- No device encryption

2.7 What are the impact of the common risk faced by the SMEs based on the risk likelihood and affecting the integrity, confidentiality, and availability of information. On a Lickert scale of 10 to 100, where Low (10) and High (100).

- Information disclosure
- Data modification
- No privacy
- Data and financial loss
- Lack of confidentiality
- Lack of integrity
- Denial of access
- Hardware failure
- Malware
- Phishing
- Lack of compliance
- Human errors
- Financial loss

2.8 What are the hardware, network and risk impact based on the common threats risk faced by the SMEs based on the risk likelihood and affecting the integrity, confidentiality, and availability of information? On a Lickert scale of 10 to 100, where Low (10) and High (100).

- Loss of hardware
- No skilled personnel
- No policy guidelines
- Unauthorised access
- Poor password criteria
- Data breach
- Viruses
- Malware
- Worms
- Trojan
- Phishing
- Spyware
- Insider attempts
- Criminals
- Denial of service

### **3 Section 3: Expected Monetary Values**

This section presents the range of monies SMEs use to recover from experienced risks.

- R601 000 to R1 000 000
- R301 000 to R600 000
- R101 000 to R300 000
- R51 000 to R100 000
- R10 000 to R50 000

### **4 Section 4: Risk mitigation**

This section addresses options used by SMEs to manage cyber risks.

- Share
- Transfer
- Accept
- Avoid

## APPENDIX D: Interview guide

This section presents the interview guide used to gather data from security experts. The data was used to design and develop cybersecurity models in this study. The guide addresses the common areas or sections affected in businesses, risk likelihood, and risk impact.

1. Do you think businesses are victims of cybercrimes?  
.....
2. What are the main cyberthreats or attacks which businesses encounter?  
.....
3. Do businesses mostly become victims on networked or standalone devices?  
.....
4. Which business areas need more protection measures? At least mention 5  
.....
5. What could determine the risk likelihood and impact of a data breach within the businesses?  
.....
6. What could improve the safety and security of the business?  
.....
7. What motivation do cybercriminals have?  
.....
8. What are employees' leading mistakes that can expose the business systems to cyberattackers?  
.....
9. Could you advise three or more common risk scenarios which can be simulated to demonstrate the risk likelihood and the risk impact that ultimately leads to a data breach?  
.....
10. What type of malware do businesses commonly experience?  
.....
11. Do you think adherence to cybersecurity policies, rules, and procedures is important for businesses? And why?  
.....