



Cape Peninsula  
University of Technology

**INFORMATION SECURITY ASPECTS SURROUNDING SMMEs IN CAPE TOWN,  
SOUTH AFRICA**

by

**SINOXOLO MOKOLO**

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

**Master of Technology: Business Information Systems**

**in the Faculty of Business and Management Sciences**

**at the Cape Peninsula University of Technology**

**Supervisor: Dr AC De la Harpe**

**Co-supervisor: Prof E Ruhode**

**District Six, Cape Town**

**November 2022**

**CPUT copyright information**

The thesis may not be published either in part (in scholarly, scientific or technical journals), or as a whole (as a monograph), unless permission has been obtained from the University

## **ABSTRACT**

Information security management is a crucial factor for all organisations under the current scenario of business globalisation. Businesses and organisations have availed huge amount of information on their databases, rendering it vulnerable to all types of cyber-attacks in the form of spams and malwares. Organisations, therefore, have to protect their databases to ensure privacy and confidentiality of data. Owing to the information security threats, this study evaluated information security aspects and how they can be included in the information security management framework for SMMEs in Cape Town. Semi-structured questionnaires were administered to 13 professionals in the IT Department of selected SMMEs in the tourism sector of Cape Town. The response rate was high (87%) and the respondent male-to-female ratio was almost equal. Findings from this study reveal that SMMEs are aware of the importance of information security for their businesses. How SMMEs perceive information security management is reflected in how they have established measures to protect their information as well as training and policy reviews that are conducted annually. Despite the theoretical policies that are in place for information security management, most respondents, however, highlighted lack of resources as a hindrance faced by SMMEs to invest in information security. Most SMMEs (92%) have information security policies in place, according to findings from this study, and 91% of the respondents highlighted that the SMMEs have a designated IT department responsible for information security management. In this study, all the respondents managed to describe the various measures that are in place when dealing with customers to protect both the SMMEs and their customers from cyber threats. Most respondents explained how installing anti-viruses on company laptops and computers manages their information security. The findings from this study provide a strong baseline for SMMEs to review their existing operating styles as well as to improve SMME data protection by applying adequate security measures.

## DECLARATION

I **Sinoxolo Mokolo**, declare that the contents of this thesis represent my own unaided work, and that the 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 \_\_\_\_\_

Date \_\_\_\_\_

## ACKNOWLEDGEMENTS

I wish to thank the following people:

**Zama Gregory Mokolo:** Mqwathi, I can't count the sacrifices you have made to continue to stand with me even when I needed to just be still. Tirelessly trying to do everything right by me, treating me like a winner even when I feel dejected. At my grouchiest and worst of times, you come to the rescue as my guardian angel to wipe away my frowns. I am forever grateful, Tata KaSgqebhezana.

**Ntombi Feya/Mokolo:** I may have stolen a few things from your wardrobe, but more importantly, I have inherited some of your amazing qualities too because I have always loved the way you approach life with grace and dignity. Thank you for showing me the way Mamntande, and FYI, I am your younger version. I love you Sapho "**Nxego**".

**Anele Gladile:** Thank you for being a bigger brother and a friend to me I know without a doubt that you will always be there to support me.

**Prof Ephias Ruhode & Dr Andre De La Harpe:** I will forever be grateful for your endless support throughout my studies without which my dream of completing my master's degree would not have been realised.

**Thulisa Ntshuntshe:** Thank you for being the sister I never had in my life. I appreciate you and I love you "**Manala**".

## DEDICATION

I dedicate this thesis entitled THE DESIGN OF AN INFORMATION SECURITY MANAGEMENT FRAMEWORK FOR CAPE TOWN ORGANISATIONS to my granny's only son who happens to be a father to me. I this moment to say thank you for believing in me even when I doubted my own capabilities; thank you for pushing me to greater heights because I pray to not disappoint you. You have been my strongest pillar and hope bringer. I have allowed too many years to pass without saying 'thank you' for believing in me unconditionally; for always giving me a shoulder to cry on. I always thought fathers were only needed by kids, but even in my adult life, you are still here with me. How blessed I am to have you. Even in my next life, I would still choose to be fathered by you **Mqwathi, Fola, Nomatyala, Bhulangwe**.

I also dedicate this thesis to my late Granny "**Nowayindishi Mokolo**". Thank you for all the good memories from my childhood till your last breath on earth. I vowed when I began tertiary life that I would only attend my academic graduation from the master's degree level, and with you by my side, driving my own car. But heaven couldn't wait for you. So I will take your sister Nongetheni Litholi on your behalf and my parents, Buntu and Sapho Mokolo, to graduation. Thank you for mothering my father so well, raising a man from a village boy whom I am proud to call a father. May your soul rest in peace **Majola, Mphankomo, Qengeba, Thole-lomthwakazi**.

I dedicate this thesis to **Thulisa Ntshuntsha**, my "sister from another mother". You took care of my heart since the first day we met 2018, sheltering me without accepting a cent for accommodation. On top of that you would buy me gifts every time your NSFAS bursary paid out. Thank you for your warm hugs, gifts, and above all, your endless support, "**Manala, Mpembe, Ndokose, Njiba**".

Lastly, I dedicate this thesis to **Alulamile Mngqete**. Thank you for all the endless support; your sacrifices do not go unnoticed, and I will forever be grateful to you **Khweba**.

## TABLE OF CONTENTS

ABSTRACT .....	ii
DECLARATION.....	iii
ACKNOWLEDGEMENTS .....	iv
DEDICATION .....	v
LIST OF FIGURES.....	xi
LIST OF TABLES.....	xii
LIST OF APPENDICES.....	xiii
ABBREVIATIONS .....	xiv
CHAPTER 1 .....	1
INTRODUCTION.....	1
1.1 Introduction .....	2
1.2 Background of the study .....	6
1.3 Background to the problem statement .....	8
1.4 Problem statement.....	11
1.5 Aim and objectives of research .....	13
1.5.1 Aim of research .....	13
1.5.2 Objectives of research.....	13
1.6 Research questions .....	13
1.6.1 Research question (RQ).....	13
1.6.2 Sub-research question (SRQ 1) .....	13
1.6.3 Sub-research question (SRQ 2) .....	13
1.7 Research methodology .....	13
1.7.1 Research philosophy .....	14
1.7.2 Research approach .....	14
1.7.3 Research strategy .....	14
1.7.4 Sampling .....	15
1.7.5 Data collection.....	15
1.7.6 Data analysis.....	15
1.8 Ethics .....	16
1.9 Headline findings .....	16

1.10	Contributions.....	16
1.11	Structure of the thesis .....	17
1.12	Chapter summary .....	18
CHAPTER 2 .....		19
LITERATURE REVIEW.....		19
2.1	Introduction .....	19
2.2	Security need.....	20
2.3	Overview of information security .....	22
2.3.1	Confidentiality.....	23
2.3.2	Integrity.....	23
2.3.3	Availability .....	24
2.4	Information security management practices (ISMP) .....	24
2.5	Security framework .....	25
2.5.1	Security framework definition .....	25
2.5.2	Framework core .....	26
2.5.3	Framework profile.....	26
2.5.4	Framework implementation tier .....	26
2.6	Risk management as a component of ISMS .....	27
2.6.1	Risk assessment .....	27
2.6.1.1	Threat identification .....	28
2.6.1.2	Vulnerability identification .....	28
2.6.1.3	Risk determination .....	28
2.6.1.4	Control recommendation.....	29
2.6.2	Risk mitigation .....	29
2.6.3	Risk evaluation .....	29
2.7	Dynamic information security risk management.....	30
2.7.1	Security property .....	33
2.8	SMMEs in South Africa .....	36
2.8.1	Factors affecting SMMEs in South Africa .....	38
2.9	How SMMEs in South Africa counter cyber threats .....	39
2.10	Overview of the target SMME for this study .....	41

2.11 Summary.....	41
CHAPTER 3 .....	43
RESEARCH METHODOLOGY .....	43
3.1 Introduction .....	43
3.2 Research philosophy .....	45
3.2.1 Ontology.....	45
3.2.2 Epistemology.....	46
3.2.3 Research philosophy for this study.....	48
3.3 Research approach.....	49
3.3.1 Inductive research approach .....	49
3.3.2 Deductive research approach.....	49
3.3.3 Abductive research approach.....	50
3.4 Research design .....	51
3.4.1 Quantitative research design.....	51
3.4.2 Qualitative research design .....	51
3.4.3 Mixed methods research design.....	51
3.4.4 Research design for this study .....	52
3.5 Sampling.....	52
3.6 Data collection .....	53
3.6.1 Interview guide .....	54
3.7 Data analysis .....	54
3.8 Delineation .....	55
3.9 Ethical considerations .....	55
3.9.1 Letter of consent.....	56
3.9.2 Anonymity and confidentiality .....	56
3.9.3 Voluntary participation.....	56
3.10 Reliability and Validity .....	57
3.10.1 Reliability .....	57
3.10.2 Validity .....	58
3.11 Summary.....	59
CHAPTER 4 .....	60



RESULTS.....	60
4.1 Introduction .....	60
4.2 The cases .....	61
4.3 Data analysis .....	61
4.4 Response rate.....	62
4.5 Section A results .....	63
4.5.1 Gender .....	63
4.5.2 Age.....	63
4.5.3 Position of the respondents.....	64
4.5.4 Work experience of respondents.....	65
4.5.5 Highest level of completed education.....	66
4.6 Section B results .....	66
4.6.1 Information management security issues faced by SMMEs .....	66
4.6.2 SMMEs with information security policies.....	67
4.6.3 Frequency of review of information security policy by SMMEs.....	68
4.6.4 SMME designation for information security management .....	69
4.6.5 Risk assessment of the SMMEs when interacting with outside individuals .	70
4.6.6 Measures and controls in place when dealing with customers.....	71
4.7 Section C results.....	72
4.7.1 Other security issues .....	73
4.8 Summary.....	74
CHAPTER 5 .....	75
DISCUSSION.....	75
5.1 Introduction .....	75
5.2 Response rate.....	75
5.3 Discussion based on Section A.....	76
5.3.1 Gender .....	76
5.3.2 Age group.....	77
5.3.3 Work experience .....	77
5.3.4 Highest level of qualification.....	77
5.4 Discussion based on Section B.....	78

5.4.1	Information management security issues faced by SMMEs .....	78
5.4.2	SMMEs with information security policies.....	79
5.4.3	Frequency of review of information security policy by SMMEs.....	79
5.4.4	SMME designation for information security management .....	80
5.4.5	Risk assessment of the SMMEs when interacting with outside individuals .	80
5.4.6	Measures and controls in place when dealing with customers .....	81
5.5	Summary.....	82
CHAPTER 6 .....		83
CONCLUSION AND RECOMMENDATIONS.....		83
6.1	Introduction .....	83
6.2	Objective-based conclusions .....	84
6.2.1	Importance of information security management in SMMEs in Cape Town	84
6.2.2	Hindrances faced by SMMEs to invest in information security management services.....	84
6.2.3	Information security policies in place for SMMEs in Cape Town .....	85
6.3	Overall conclusion.....	86
6.4	Recommendations.....	87
6.5	Limitations and future research.....	89
REFERENCES.....		90
APPENDICES .....		113

## LIST OF FIGURES

Figure 1.1: Layout of Chapter 1.....	1
Figure 1.2: The overall range of classification of small enterprises. Source: SEDA (2018).....	3
Figure 1.3: Trends in the number of SMMEs in South Africa from 2018 to 2019 (SEDA, 2022).....	5
Figure 2.1: Layout of Chapter 1.....	19
Figure 2.2: The CIA triad.....	23
Figure 2.4: Steps that can be followed by an SMME to counter cyber threats. Source: Malumo (2023).....	41
Figure 3.1: Layout of Chapter 3.....	44
Figure 3.2: The research onion.....	46
Figure 3.3: Summary of ethical considerations.....	57
Figure 4.1: Layout of Chapter 4.....	61
Figure 4.2: The response rate from the survey.....	63
Figure 4.3: Gender of participants.....	64
Figure 4.4: Age group of respondents.....	65
Figure 4.5: Position of respondents.....	66
Figure 4.6: Highest level of qualification of respondents.....	67
Figure 4.7: SMMEs with information security policies.....	68
Figure 4.8: Frequency of reviews of information security policy by SMMEs.....	70
Figure 4.9: SMME designation for information security management.....	71
Figure 4.10: Risk assessment of SMMEs when interacting with individuals outside the organisation.....	72
Figure 4.11: Summary of responses from Section C.....	74
Figure 5.1: Layout of Chapter 5.....	77
Figure 6.1: Layout of Chapter 6.....	85

## LIST OF TABLES

Table 3.1: Comparison of interpretive and positivist approaches .....	48
Table 3.2: Comparison of qualitative, quantitative and mixed methods designs .....	53
Table 4.1: Frequency and percentage age group of respondents .....	65
Table 4.2: Work experience of respondents .....	66
Table 4.3: Measures in place when dealing with customers .....	73
Table 4.4: Summary of other issues raised during questionnaire administration .....	75

## LIST OF APPENDICES

Appendix 1: Ethics Informed Consent Form.....	115
Appendix 2: Ethical Clearance from the University .....	.117
Appendix 3: Questionnaire .....	118

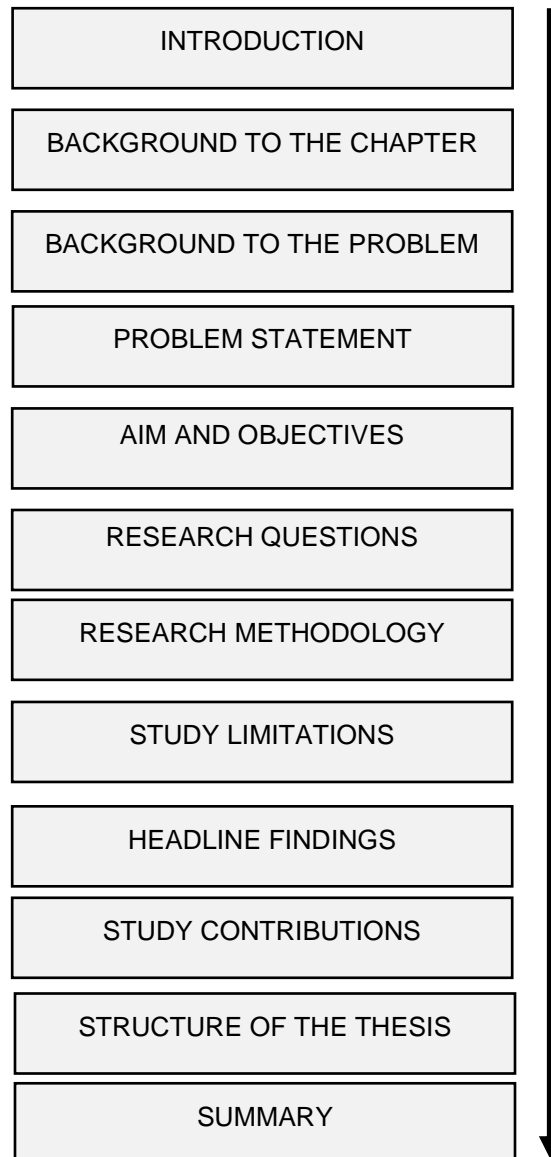
## **ABBREVIATIONS**

DDOS	Distributed Denial of Service
ICT	Information and Communication Technology
ISMP	Information Security Management Practices
IT	Information Technology
OECD	Organisation for Economic Co-operation and Development
RSA	Republic of South Africa
SA	South Africa
SMME	Small- Medium- and Macro Enterprise

# CHAPTER 1

## INTRODUCTION

The layout of Chapter 1 is illustrated in Fig. 1.1 below.



**Figure 1.1: Layout of Chapter 1**

## 1.1 Introduction

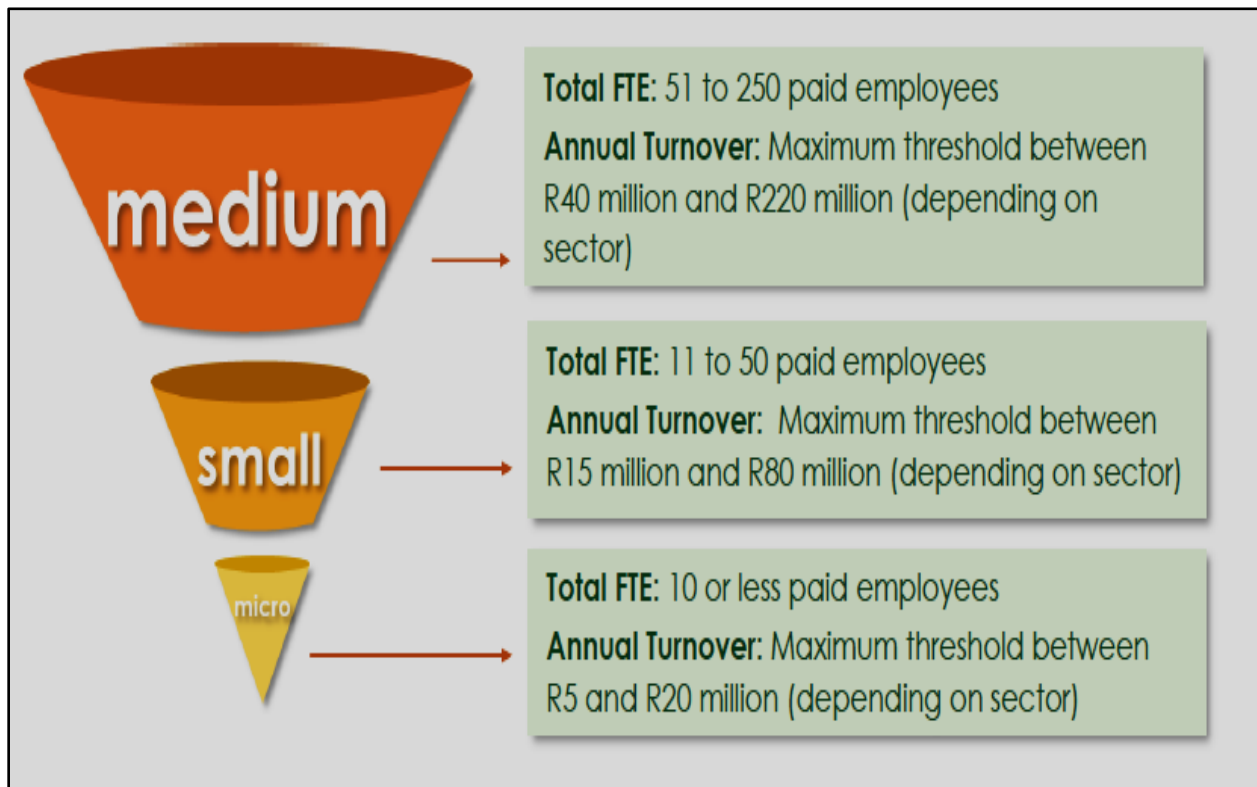
Information security development and implementation are important to small, micro medium and micro-enterprises (SMMEs). This research focuses on exploring information security aspects in order to propose an information security management framework for SMMEs in Cape Town, South Africa. This is done so that SMMEs are able to control and safeguard their information. SMMEs are suffering from information security breaches that not only affect the company but also its stakeholders (Wandera, 2018; Couce-Vieira et al., 2023). In 2020, SMMEs faced over 700,000 cyberattacks causing a total loss of US\$2.8 billion in damages (James, 2023). By 2025, cybercrime costs are predicted to reach US\$10.5 trillion (James, 2023). SMMEs are facing information security management issues that have been attributed to their limited information management systems and resources (Srinidhi et al., 2015). de Arroyabe and de Arroyabe (2021) suggest that SMMEs are typically prone to information security breaches because of the lack of simple control and planning systems and limited standardisation of information processes.

Similar to other businesses, asset information needs to be strategically protected and managed (Bland et al., 2021). Information security is defined by Alhassan and Adjei-Quaye (2017) as the “protection of information within a business, and the systems and hardware used to store, process and transmit this information.” Business management and leaders need to appreciate the value of information and develop frameworks in the organisation to implement information security. Though a number of approved information security frameworks are available, Whiteman and Mattord (2012) argue that these cannot be implemented by SMMEs as they are too complex and costly given the SMMEs limited resources. As a result, these frameworks are basically only adopted by large corporates.

SMMEs are defined in several ways, generally with reference to either turnover bands or the number of employees (or a combination of both) as prescribed by the National Small Business Act (NSB Act) of 1996. The Act allows for variations based on respective industry sectors (ILDPA, 2014). The South African DTI (2009-2019) defines and classifies



SMMES by size according to their annual turnover in terms of the National Small Business Amendment Bill (Republic of South Africa, 1996) depicted in Figure 1.2 below. In the NSB Act, micro enterprises are business entities which are operated by business owners and their families with fewer than five people employed and an annual turnover of less than R150 000. Very small enterprises are informal businesses with access to technology, employing fewer than 10 paid employees, except manufacturing, construction, electricity and mining sectors which have 20 employees. Small enterprises are the formally registered businesses which have fixed business premises and have a complex management employing up to 50 people. Medium enterprises are characterised by a decentralised management structure and employ up to 200 employees.

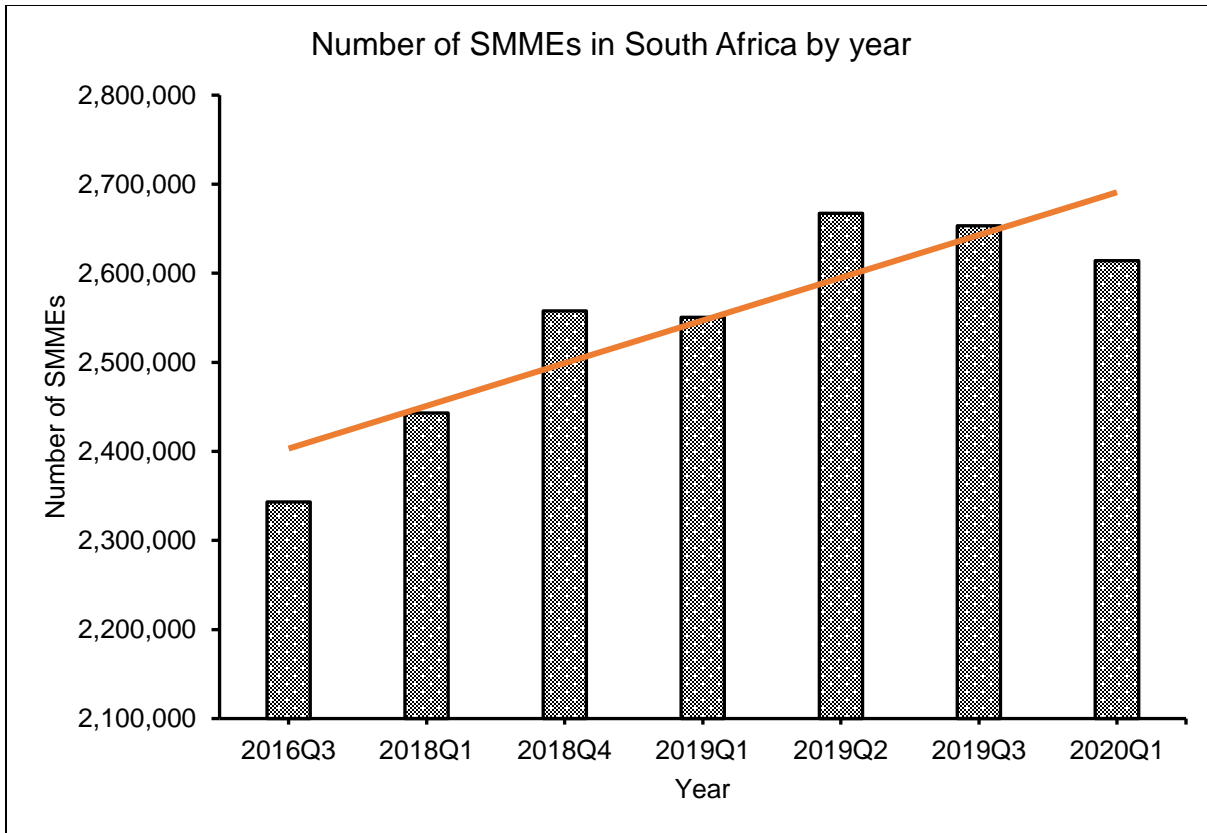


**Figure 1.2: The overall range of classification of small enterprises. Source: SEDA (2018)**

The South African government considers SMMEs a key priority area towards socio-economic development and growth. SMME's efficient and effective management is essential in creating employment and economic growth (George, 2022). Adomako and

Ahsan (2022) note that the majority of SMMEs form as a result of an entrepreneurial passion of founders with limited funding. This lack of funding hampers the ability for the SME to grow as they have limited access to formal sources of funding as compared to larger businesses (Adomako and Ahsan, 2022). This is further amplified by George (2022) who argues that SMME's understanding of information security risk is narrow and only limited to anti-virus software. Consequently, SMMEs are prone to information security risks, worsened by their lack of awareness and inadequate employee training programmes.

The number of SMMEs in South Africa has been increasing over the years from 2 343 058 in the 3<sup>rd</sup> quarter of 2016 to 2 614 063 in the 1<sup>st</sup> quarter of 2020, a growth of 10% over the period. This information is illustrated in Figure 1.3 below.



**Figure 1.3: Trends in the number of SMMEs in South Africa from 2018 to 2019 (SEDA, 2022)**

The number of SMMEs, however, declined in 2020 during the Covid-19 pandemic period to below 2.4 million SMMEs (SEDA, 2022). SMMEs provide a significant population of South Africa with employment opportunities. In 2019, the SMME sector employed 10.8 million people accounting for 66% of the South Africa's total employment (16.5 million) (SEDA, 2019). The number of jobs provided by SMMEs, however, declined drastically in 2020 also due to the Covid-19 pandemic (SEDA, 2022).

Owing to a number of definitions of SMMEs, this study focuses on the SMMEs in the Information and Communication Technology (ICT) sector that fell in the criterion of the SMME definition by the NSB Act of 1996. This study, therefore, adopts the NSB Act of 1996 definition with a particular focus on ICT SMMEs. SMMEs are defined as formal or informal small, medium and micro-enterprises focusing on ICT business and employing

fewer than 200 people including its subsidiaries or branches.

## **1.2 Background of the study**

According to the Eze et al. (2019), a significant percentage of SMMEs lack any formal data storage and backup facilities. The same research suggests that over 26% of SMMEs lack the capacity to restore information files following an email virus. Data corruption and incidental system failure are common amongst 25% of SMMEs. The report further confirms that employees are responsible for the majority of information security threats. The survey states that during the same period, there has been a lack of procedures and policies on information security despite technological evolutions which are opening up businesses to the public through connectivity by means of public networks and an increase in e-business.

Whiteman and Mattord (2012) argue that SMMEs should be aware of the fact that information security management is broad and extends to governance liability, regulatory and legal. But SMMEs do not have the knowledge and resources needed in managing changes that occur outside their key competence without help from outside (Devlin, 2021; Lejaka, 2021). Given their well-publicised limited knowledge and resources, the introduction of an information security management framework that can be implemented and managed without outside support will be ideal in improving business efficiencies and security.

The tenure of information security means the preservation of i) integrity; ii) availability; iii) confidentiality of data in the effort to guarantee information accountability; iv) authenticity, v) reliability; and vi) no repudiation (Moody et al., 2018). Cybersecurity is the safeguard of the cyber system that support cyberspace as well as the people using cyberspace in a societal, national and personal capacity. These societal, national and personal capacities include either “tangible or intangible interests which are exposed to the attacks that originate in cyberspace” (Kshetri, 2017). Cyber-attacks are a local and international reality that is essential to manage as it threatens actors (government, information security

agencies) and moves towards intentional disruptions, espionage, and crime of systems and networks (Hadlington & Chivers, 2020). To curb any attacks and threats, government and management leaders must acknowledge measures of weakness with an institution and the reality of attacks and threats.

In an ideal world, companies prefer to handle change in a strategic manner (Robbins & Judge, 2018) as this allows them to plan for goal-oriented activities as well as to implement their information security strategies. However, organisations still face difficulty in changing adaption mechanisms. Big data analytics, cloud computing, social media, new regulations and legislation present organisations and governments with new encounters with regard to threat and vulnerability management from both a human and technological perspective. The Verizon Data Breach Investigations Report indicates that whereas the majority of breaches arise from external causes, interior employees account for about 15%, with 14% arising specifically from employee errors (Verizon Enterprise, 2020).

The 2018 survey by PricewaterhouseCoopers (PwC) confirms that from a people perspective, the leading concern for information security is the human factor, with 29% (former) and 34% (current) personnel representing the major source of conciliation, followed by 22% (service providers), 19% (past service providers) and 16% (suppliers). From the perspective of technology, governments and organisations perceive phishing and malware as the leading threats relating to the human element. Organisations must focus on the application of planned change mechanisms to efficiently adapt to the changes and manage risks from the human perspective. The needed application must also apply to changes of the organisation's information security culture.

Information security includes people, technology and processes while confidentiality, availability and integrity are the three main elements of information security. According to the ISO/IEC 27000: Information Security Management Systems Standard, confidentiality

means undisclosed, unauthorised or unavailable information to processes, individuals or entities. Integrity means asset completeness and accuracy of property. Availability means an authorised entity's on-demand accessibility and usability. The standard maintains that authorised people must have limited and explicit access, trustworthy and accurate information. The prevailing technical actions in South African organisations such as "biometrics, firewalls, and passwords are insufficient in threat mitigation to the information." (Aldya et al., 2019). It is imperative to have measures to safeguard systems as well as defend data against damage. The deployment of information security requires the "consideration of processes like user de-registration and registration as well as people features like training, leading-by-example and compliance" (Åhlfeldt et al., 2018). The evolution of information security deployment has shifted the focus towards a governance-orientated and people-orientated approach.

### **1.3 Background to the problem statement**

A number of security frameworks are available for implementation by SMMEs to "enhance their information security management" (Lejaka, 2021). These frameworks, however, are more suitable for large corporates as SMMEs lack the technical competence and resources essential for implementing such frameworks (Lejaka, 2021). Magnusson (2022) elaborates this perspective, noting that for an enterprise to be ISO/IEC 27001 certified for a year it costs around \$5000 (roughly R80 000) and such amounts are significant for SMMEs to invest towards information security.

In South Africa, there is little development in information security notwithstanding the best efforts of the government (Kritzinger et al., 2017). South Africa's Auditor General has continuously reiterated in their investigations that there is concern of the current status of information technology controls. The Auditor General's audits identify that regardless of spending about R13.2 billion on information technologies, the current status of the information technology controls in SA is insufficient in the tough environments because 63% of the auditors indicate weak practices of information technology governance as well as an astounding 88% reporting weak general information technology controls (The

Auditor-General South Africa, 2020). According to this 2018/2019 report, SMMEs in South Africa struggle with effective implementation of the needed measures for improving ICT security (Kritzinger et al., 2017).

The losses in data confidentiality, integrity and privacy result in catastrophic consequences. For instance, in 2018, South Africa registered about 320 US million in costs of phishing attacks (Mimecast, 2019). The country accounts for 5% of global phishing attacks. The Federal Bureau of Investigation (FBI) states that with five hundred and thirty-four (534) complaints, South Africa ranks 11<sup>th</sup> out of the 50 countries which reported the highest internet-related concerns (FBI, 2018). From four years of historical information, the International Business Machines Corporation (IBM) indicates that R43.3 million is the average total expenses for data breach in 2019 for South African organisations, representing a 12.2% rise from 2018 (IBM, 2019). South Africa ranks as one of the nations with the highest possibility of a security breach in the following year (24 months) (Accenture, 2019). Even when researchers and organisations in South Africa rely on technologies and international and national cyber-crime information, there is no actual reflection of the security breach and incident dimensions. Dlamini et al. (2019:3) state that “the Directorate of Priority Crime of South Africa’s Police Service has made cyber-crime a vital crime, investing added resources into investigations of these crimes.”

The Mimecast Company maintains that organisations in South Africa must therefore remain conscious of information security, imminent attacks or threat from cyber-criminals who operate internationally and locally (Mimecast, 2019). Cyber-attackers possess sophisticated technologies, growing increasingly organised and prepared to initiate attacks. According to Patrick et al. (2018), because the South African government and organisations store, deal and collect enormous confidential and protected data daily, they have to continuously deliberate on ways to safeguard themselves against information security breaches and hacks as well as urgently improve and address information technology governance.

According to IoDSA (2020), the King III report contends that the company board is responsible for approval of the organisation's information security strategy and guaranteeing effective management of information assets. The Institute of Directors of Southern Africa states the company or organisation's board of directors has to delegate their obligation for information security implementation. The management of the company or organisation has to establish buy-in and commitment to information security (IoDSA, 2020). The Corporate Governance Code UK supports South Africa's King III report by stating that the directors of organisations and companies are responsible to ensure that they have conducted a vigorous evaluation of the leading risks affecting the organisation or company. The risks include the threats with the capacity to threaten the organisation's corporate model, liquidity or solvency and future performances (Financial Reporting Council, 2018). To effectively handle data assets, the organisation or company must conduct strong risk evaluations to detect risks that could be related to customer data or even data resulting from financial statements, databases and systems supporting the information, as well as workers with access to the data (Deloitte IAS Plus, 2020).

Studies such as Safa et al. (2016) as well as Hadlington and Parsons (2017) have identified "the human aspect" in information security as a fundamental aspect, alongside organisational and technical facets, which form part of the processes that guarantee information system protection and fidelity within the government or an organisation. The institutions have carefully deliberated and effectively addressed or managed organisational and technical issues regarding information security (Scholl et al., 2017). However, because it is an ever-changing and complex phenomenon, international organisations have effectively managed the human aspect because of the comparative ineptness of institutions as well as their management structures to control and identify the human aspect (Hina & Dominic, 2020). Within any organisation, the general organisational culture directs the human aspect, based on the individuals' attitudes, behaviours and norms, which comprise that organisation (Akhyari et al., 2018).



To resolve the human aspect, several preceding studies and research have focused on raising, managing and monitoring employee security awareness levels (Dhillon et al., 2016). While the desire to improve workers' mindfulness in line with security policy is overbearing for a culture of security policy compliance in institutions, Nasir et al. (2019) compared the culture of employees, concluding that there is significant improvement over the general information security culture if the workers read the institution's information security policy. Barzak et al. (2019) propose developing an effective information security culture framework that integrates responsibility, regulations, management, preparedness and society. Cuganesan et al. (2018) similarly proposes five variables which could impact information security culture: i) information security behaviours; ii) top management backing; iii) security awareness and education; iv) information security acceptance; and v) policy.

The non-expert information-security personnel in private businesses have therefore failed to monitor sustainably the existing company security situation. Information security is an exhaustive practice in need of serious workload which has proven insufficient in guaranteeing process excellence. While South Africa's companies and government have chosen to implement and combine numerous information security management frameworks, these frameworks lack the proper information security management framework tools, ignore the human aspect in developing solutions as well as the commendations to exiting information technology structures (IMF, 2022). There is an opening for an information security management framework with significant information safety administration elements and progressive measures for SMMEs.

#### **1.4 Problem statement**

Most countries around the world are still struggling to recover from the global financial crisis and economic backdrop caused by the Covid-19 pandemic in early 2020, which led to many economies shutting down (Saah, 2021). In these situations, SMMEs are thought to be the major drivers for triggering economic growth to revive the dwindling economies. But SMMEs are faced with information security management issues and have been

proven to have only limited information management systems and resources. The majority of SMMEs in South Africa continue to fail within a very short period, with high failure rates ascribed to the various challenges they face (Chimucheka & Mandipaka, 2015; Bruwer, 2020). The SMME sector, which is the economic backbone of South Africa, is dwindling, indicating a stagnating economy (Saah, 2021). The continuous dwindling of the SMMEs led to South Africa's growth rate of only 0.3% in 2016, which was an indication of a build-up to a constant economic slowdown because the country has been experiencing a per capita recession as population growth is exceeding that of the economy, thereby plunging South Africa into a technical recession (Sanele & David, 2021). The economic setback is affecting prices of commodities and the depreciation of the rand which is currently at 1:17.03 against the US dollar (Goko, 2022). This potentially results in an increase in capital costs for SMMEs.

Information security aspects have been shown to affect businesses. For instance, in 2018, the country registered about US \$320 million in costs of phishing attacks which represents 5% of the global phishing attacks (Mimecast, 2019). According to the Federal Bureau of Investigation (FBI), South Africa ranks 11<sup>th</sup> out of 50 countries which reported the highest internet related concerns (FBI, 2018). Most affected are the SMMEs as they lack any formal data storage and backup facilities (Brewerton, 2013; Yoshino & Taghizadeh-Hesary, 2016). Over 26% SMMEs lack the capacity to restore information files following an email virus. Data corruption and incidental system failure are common amongst SMMEs. While a number of security frameworks are available for implementation by SMMEs to enhance their information security management, most are more suitable for large corporates as SMMEs lack the technical competence and resources essential to implement such frameworks (Lejaka, 2021). Despite the large number of information security frameworks available to organisations, there is lack effective and efficient security frameworks for SMMEs.

## **1.5 Aim and objectives of research**

### **1.5.1 Aim of research**

The aim of the study is to explore information security aspects in order to propose an information security management framework for SMMEs in Cape Town, South Africa.

### **1.5.2 Objectives of research**

- i) To determine the importance of information security management in SMMEs in Cape Town;
- ii) To determine the hindrances faced by SMMEs to invest in information security management services in Cape Town;
- iii) To determine information security policies in place for SMMEs in Cape Town; and
- iv) To offer recommendations on the applicability of the proposed information security management framework to the human aspect in South Africa's SMME sector.

## **1.6 Research questions**

### **1.6.1 Research question (RQ)**

What information security aspects need to be considered for an information security framework for SMMEs?

### **1.6.2 Sub-research question (SRQ 1)**

What are the hindrances faced by SMMEs to invest in information security management services in Cape Town, South Africa?

### **1.6.3 Sub-research question (SRQ 2)**

What information security management measures are taken by SMMEs to protect their business from cyber threats in Cape Town?

## **1.7 Research methodology**

Research methodology is defined as a criterion in which data, facts and information are elicited and structured in a clear and meaningful manner that enables the researcher to

achieve the goal of the research (Neuman, 2014). The following sub-sections will give a snapshot of the research methodology which are fully described in Chapter 3.

### **1.7.1 Research philosophy**

Research philosophy refers to philosophical orientations about the world as well as the type of research being conducted (Adams et al., 2014). The choice of method to be used by a researcher is motivated by researcher's epistemology as well as theoretical position and how these shape and influence the research approach (Mertens, 2015). A research study can be conducted using either of the two philosophical positions namely: i) ontology or ii) epistemology (Saunders et al., 2019). For this research, an ontological position of subjectivism is used. This is for the researcher to be a real partner with the informants, and also to openly use her own experiences and reflections to uncover valuable meaning and find a different type of objectivity.

### **1.7.2 Research approach**

A research approach is a general plan and procedure for research or conducting a study (Saunders et al., 2019). Accordingly, research approaches can be divided into three categories – deductive, abductive and inductive approaches – which are discussed in detail in Chapter 3. This study follows the inductive approach. The logic that the researcher follows is inductive, from the bottom up, rather than handed down entirely from a theory or perspective of the researcher. Adopting an inductive approach means that the researcher decides to conduct the study on some individuals, in this case, those who are in SMMEs in the tourism sector, who are knowledgeable about the sector.

### **1.7.3 Research strategy**

The research design helps researchers pursue their journeys into the unknown but with systematic approaches to guide them. The research design is categorised into “quantitative, qualitative and mixed methods research designs” (Saunders et al., 2019). This current study uses a mixed methods research design which reflects the experiences

of participants (George, 2022).

#### **1.7.4 Sampling**

The study adopted purposeful sampling, which is a type of non-probability sampling (Saunders et al., 2019). The logic and power of purposeful sampling lies in selecting information rich cases for the study in depth. Information rich cases are those that one can learn a great deal about issues of central importance to the purpose of the inquiry, thus the term purposeful inquiry. For the current study, participants had to be employed by SMMEs operating in the tourism sector in Cape Town and working in the field of information technology and with an influence on organisational strategy. The sample defined by Creswell and Creswell (2018) as, “a small proportion of the population that is selected for observation and analysis”, for the current study were 13 IT experts (Unit of Observation) at management level within their organisations.

#### **1.7.5 Data collection**

The participants were selected based strictly on the official job position and functions at their workplace with regard to implementation of an information security framework. The research administered questionnaires to IT experts and data analysts within the case study organisations due to their knowledge about information security management framework implementation within their organisations. This study considered the primary method of data collection in choosing the method for obtaining data, with a decision on the study sample size, sampling technique as well as the data construction instrument. The semi-structured questionnaires were administered to 13 employees of SMMEs in the tourism industry in Cape Town. The study chose semi-structured questionnaires because they are simple to administer and have a higher response rate than other data collection methods.

#### **1.7.6 Data analysis**

The study used coding, summarising, categorising and then a thematic analysis for the

analysis. Each questionnaire was labelled 1-13 and corresponding responses were coded for Section A and C and entered into Microsoft Excel where figures, charts and tables were generated to allow easier comparison, presentation, validation and reliability of the findings.

## **1.8 Ethics**

The researcher applied for an ethical clearance from the Ethical Committee of the university before conducting the study to ensure the study was undertaken in an appropriate manner under the consideration of ethical values. It was important during the research process to make respondents understand that participation in this research was voluntary and that they were free to refuse to answer to any question and/or to withdraw from participation at any time. Other factors considered include informed consent, and anonymity and confidentiality which are further described in Chapter 3.

## **1.9 Headline findings**

From this chapter, it seems there are information gaps which warrants this study and are summarised below:

- A significant percentage of SMMEs lack the capacity to manage their information security following various threats and therefore, how SMMEs in Cape Town manage information security is unknown.
- There are various hindrances faced by SMMEs to invest in information security management services in Cape Town, South Africa. These need to be investigated in order to come up with solutions that can contribute to the growth of SMMEs.
- Addressing the challenge of information security management has the potential to promote SMME growth in Cape Town, and South Africa.

## **1.10 Contributions**

Owing to the contributions of SMMEs to the economy of South Africa (Bruwer, 2020), this

study is important as it aims to explore information security aspects in order to propose an information security management framework for SMMEs in Cape Town, South Africa. Addressing the information security aspects potentially improves the capacity to store data, restore information files following viral attacks and reduce data corruption and incidental system failures. The study may add knowledge on how SMMEs can positively maintain their information security and enhance their competitiveness. This knowledge can be used as a reference or baseline study for future references in theses and academic journals.

### **1.11 Structure of the thesis**

- Chapter 1:* This chapter introduced the thesis, giving the background of the study, problem statement, research aim and objectives, research questions, the significance of the study and the limitations.
- Chapter 2:* The chapter covers an evaluation of prevailing literature on the design of an information security management framework for South African organisations.
- Chapter 3:* This chapter discusses the research methodologies and design used in this research, including the research instrument employed for data collection.
- Chapter 4:* The chapter contains an examination of the collected data and uses figures and tables for the presentation of the collected information.
- Chapter 5:* The chapter covers a summary, recommendations and conclusion to the design of an information security management framework specific to South African organisations.

## 1.12 Chapter summary

This chapter introduced the research topic which is “*Information security aspects surrounding SMMEs in Cape Town, South Africa*”. In this chapter, issues regarding SMMEs were unpacked and narrowed to identify the problem being investigated with associated research objectives and questions. The problem that warranted development of this topic is the issue of SMMEs facing information security management problems which could be causing them to continue failing within a very short period of time. This study therefore evaluates the information security aspects and investigate how they can be included in the information security management framework for SMMEs in Cape Town, South Africa with 3 objectives linked to this aim. To achieve this, a mixed methods approach is taken using an interview guide administered to 13 respondents. The study uses coding, summarising, categorising and then content analysis for the analysis. Findings from this study may add knowledge on how SMMEs can positively maintain their information security and enhance their competitiveness. This knowledge can be used as a reference or baseline study for future references in theses and academic journals. The following chapter provides a literature review to explore the theoretical background for this research.



## CHAPTER 2

### LITERATURE REVIEW

The layout of Chapter 2 is illustrated in Fig. 2.1 below.

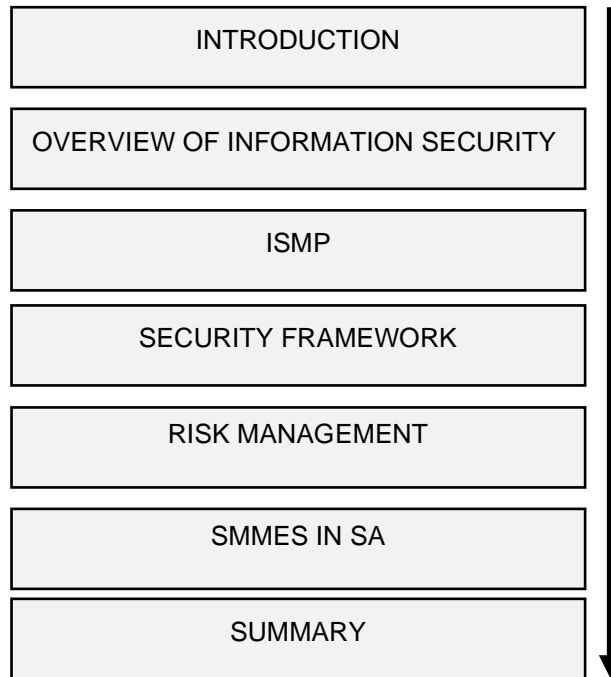


Figure 2.1: Layout of Chapter 2

#### 2.1 Introduction

The previous chapter introduced the research topic, the background and the study aim and objectives. The study explores information security aspects and how they can be included in the information security management framework for SMMEs in Cape Town. This chapter reviews the literature relevant to the research topic. Theoretical framing of this study draws from two streams of literature, namely SMMEs and the information security management framework. The researcher utilised multiple sources of information to conduct the literature review such as textbooks, journal articles, dissertations and website articles. These sources were obtained from Emerald, Google Scholar, the CPUT library and other databases. From the literature review, the researcher identified important

existing gaps in information security management in SMMEs. The chapter is presented as follows: i) Security need, ii) overview of information security, iii) the security framework, iv) risk management as component of ISMS, v) Dynamic information security risk management , vi) SMMEs in South Africa and vii) a summary.

## **2.2 Security need**

Kemp (2022) states that the amount of digital information that businesses now have access to and being shared continues to increase across the world. Kemp (2022) estimates that the information volume that we interact with will increase approximately ten times in a decade. The development of the internet heralded the impact of information systems on individual routine as it became a critical part of individual life. Pandey and Pal (2020) notes that despite offering huge benefits, the internet is also prone to dangers largely related to security issues. Security threats on the internet are described as catastrophic and even E-bay and Yahoo have experienced these security threats (De' et al., 2020: Somepalli et al., 2020).

In the information age, organisations are increasingly depending on information systems to outcompete their competitors. Balozian and Leidener (2017) postulate that information must be shared within the organisation as with all stakeholders including customers, employees and partners. As a result of the need to adopt new technologies and share organisational information with stakeholders, organisations are facing a mammoth task in security maintenance. Technology-based solutions are increasingly adopted by organisations to protect themselves from security breaches. According to Soomro et al. (2020), organisational use of technological control to security risks is inadequate to mitigate against risks, so as a result there has been an increase of security incidents. Soomro et al. (2020) conclude that technological controls are inadequate in risk prevention. As such, they elaborate that information security should not be perceived as a technological problem. Soomro et al. (2020) argue for comprehensive consideration of security problems within an organisation, suggesting that to solve the problem, technological control should be utilised. They further concur that exceptional

management practices are vital in providing an organisation with security protection to assets of the organisation.

Based on this background, security approaches by organisations have begun to be prioritised. However, predictions by specialists in the security sector are that not all security concerns can be eliminated (Karataş, 2021), with the further prediction that security concerns will gain prominence more than the expected internet growth. Karataş (2021) suggests that organisations should invest heavily to safeguard their information systems.

Taylor (2017) who notes that organisations have no choice but to be connected to the internet despite its shortcomings “As risky as the internet is, companies have no choice but to be there. The lure of new markets, new customers, new revenue sources and new business models are just great that companies will flock to the internet regardless of the risks”. This view is buttressed by Karataş (2021) further alludes to the point that despite the high risk involved in information technologies such as theft of data, data loss and security breaches, organisations are poised to be increasingly dependent on information technologies. Given the stiff competition among organisations on the internet to attract more customers and generate more sales, companies need to secure added advantage over their competitors. Taylor (2017) suggests that this occur by investing in software, information systems and secure website.

The internet is designed in such a manner that it is easy and convenient to reach fellow internet servers regardless of the distance and quite possible to launch network attacks. Misconfigured networks are easy target for hackers, and other malicious experts in security (Taylor, 2017). Hackers are motivated by different motives such as fame or financial gain. Huge sums of money can be lost by companies from malicious hacking and attacks on their security. Security incident impact on an organisation can be far reaching through company data loss, damaged reputation and money theft which can

lead to organisational bankruptcy. As such risks can be catastrophic, companies should rather invest in security (Taylor, 2017).

### **2.3 Overview of information security**

Baskerville (2018) explains that information security relates to the relationship that exists between three elements in information systems: organisational information resources, risk threats and risk controls. Any factor that has a negative effect on properties of information security is regarded as a threat. Guo (2018) classifies information threats into two categories: incidental and purposive. These threats are typically characterised by violation of integrity, service denial and disclosure of information (Dhillon et al., 2016). Protection strategies adopted to minimise the impact of threats are known as control measures. Formal controls are prescriptive as they are developed following findings on risk assessment and may include aspects like procedures and policies intended to provide advice to the personnel and provide noncompliance punitive measures. Dhillon et al. (2016) note that informal control involves elements such as education, training and development which are aimed at influencing the organisational culture. These measures are largely suggestive. Technological controls are considered restrictive and include elements such as the intrusion detection system, firewalls and other measures that restrict resources access.

Information resources relate to valuable assets that require protection. Baskerville (2018) further states that the aim of organisations is the preservation of integrity, confidentiality and availability of information resources – also known as the CIA triangle (Figure 2.2). The CIA triad highlights the three as the primary goals of data security (Covert et al., 2020; Palmieri et al., 2021). Other factors to consider besides the CIA triangle include accountability, reliability, authenticity and non-reputation (Whitman & Mattord, 2018; Dubojs et al., 2019; Covert et al., 2020).

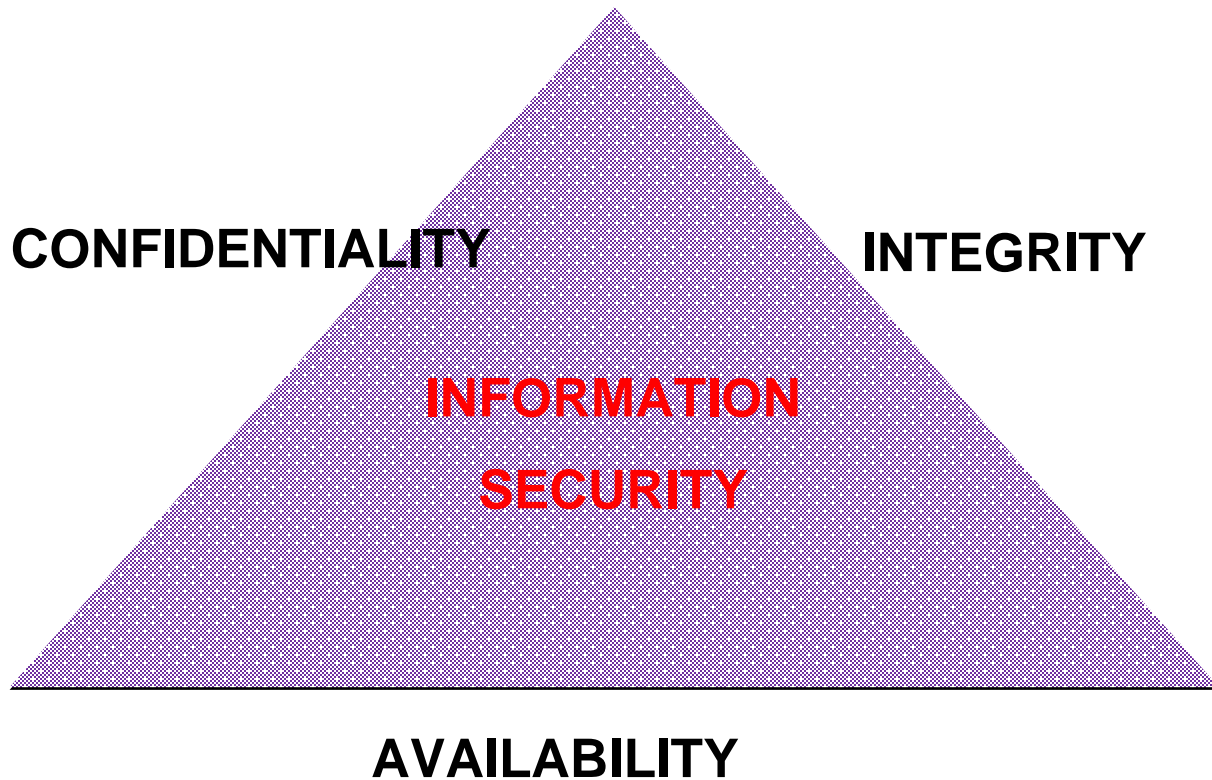


Figure 2.2: The CIA triad. Source: Baskerville (2018)

### 2.3.1 Confidentiality

Confidentiality, according to Amraoui et al. (2019), is an information property that protects it from being disclosed or made available to entities, individuals and processes that are not authorised to have access to such information. Confidentiality measures in a business organisation are specifically designed to prevent unauthorised information disclosure (Covert et al., 2020). The confidentiality principle keeps organisational information private and ensures that it is only accessible and visible to individuals who own and need it to perform organisational functions (Imperva n.d).

### 2.3.2 Integrity

Integrity is defined by Luo et al. (2019) as a property of information concerned with, “safeguarding the completeness and accuracy of assets”. The integrity principle ensures

that data is reliable, accurate and is not incorrectly modified, maliciously or accidentally (Li & Liu, 2021). Integrity is important for safety and financial data that is used for activities that include air traffic control, financial accounting and any electronic funds transfers (Imperva, n.d).

### **2.3.3 Availability**

Availability is defined as the protection of an organisation system's ability to make software systems as well as data fully available as per user's needs (Imperva, n.d). Availability as an information property relates to its potential of being usable and accessible upon request from authorised personnel or entity (Amraoui et al., 2019). The purpose of this availability principle is to make the ICT infrastructure, applications, software and the data available when required for organisational processes or for clients (Imperva, n.d). Availability is regarded as the most important principle in service-oriented businesses that mostly depend on information (Covert et al., 2020).

## **2.4 Information security management practices (ISMP)**

Information security management practices (ISMP), as noted by Somepalli et al. (2020), refers to "structured process for the implementation and continuous management of information security in organisations". The thrust of ISM is fostering the achievement and maintenance of high levels of integrity, confidentiality and information sources availability. ISM is considered as a process inclusive of organising, controlling, planning and commanding with the aim of establishing security levels that are satisfactory (Somepalli et al., 2020).

The turn of the new millennium has seen an increase in research focused on information security from a managerial perspective and its influence on organisational performance (Oyelami & Ithnin, 2019). The rise of incidents on information security led to academics realising that information security was broader than merely a technological problem but also involved a management dimension. Information control mechanisms implemented

continue to fail to eliminate risks, and Oyelami and Ithnin (2019) argue that technological control implementation within organisations is dependent on organisational strategies and security policy. This view is shared by Soomro et al. (2020) who note that programmes on security management that intend to offer comprehensive solutions should focus on practicing good management and technological controls. ISMPs have a significant role to play within organisations in terms of information source protection.

Despite having a significant amount of research focusing on managerial and technological aspects on ISM, there appears to be a gap on the three control types, and this leaves organisations with a need for coherent and detailed guidance on the types of practices that management can utilise in the process of information protection (Soomro et al., 2020). Management should be made aware of the range of technological practices available to them in their endeavour to protect organisational information resources. Literature on ISMPs can be classified into two categories – professional and academic – and this section will elaborate on these two schools of thought.

## **2.5 Security framework**

Originit (2017) suggests that an information security framework constitutes documents and policies that are pre-agreed and understood by stakeholders, detailed processes explaining how the business will manage information. The main thrust of the security framework is lowering of threat risk and other security vulnerabilities so as to enhance confidence within the organisation. A plethora of security frameworks exist across the world; each organisation as noted by Originit (2017) has the mandate of selecting the most appropriate security framework that addresses its particular situation.

### **2.5.1 Security framework definition**

The national Institute of Standards and Technology (NIST) (2018) describes a security framework as, “a risk-based approach to reduce cyber security risks. It is composed of following parts: the framework core, the framework profile and the framework implementation tiers”. The security framework, also referred to as the cyber security

framework, consists of several cyber security activities.

### **2.5.2 Framework core**

NIST (2018) states that the framework core is comprised of four elements: informative references, categories, functions and sub-categories. The purpose of the core is providing the practices and guidelines that align with industry standards and that do not hinder organisational communication across organisational boards. NIST (2018) explains that a thorough consideration of the aforementioned elements assists in providing the organisation with organisational direction in the management of cyber-security risk.

### **2.5.3 Framework profile**

This constitutes outcome from the subcategories and categories of the system selected by the organisation. According to NIST (2018), the framework profile can be characterised as the process of guidelines and standard alignment and practising implementation scenarios. To enhance the security posture of the organisation, NIST (2018) suggests a comparison of the prevailing state of the profile with the targeted profile. Development of a profile allows the organisation to review all categories and subcategories depending on the assessment of risk and available information on company business drivers. The addition of subcategories and categories capacitates the organisation in dealing with risk and the measurement and progress prioritisation in pursuit of the target profile. A company's current profile as noted by NIST (2018) can be utilised in supporting the business criteria planning, including elements like innovation and cost effectiveness.

### **2.5.4 Framework implementation tier**

This includes strategies used by a company in management and identification of risks. NIST (2014) points out that the management of cyber security practices by the organisation is expected to portray characteristics such as being adaptive, aware to risk and alert to threats. The tier selection initiative should be inclusive of prevailing management practices on prevailing risks, constraints faced by the organisation, regulatory and legal environment and also the prioritised organisational objectives (Taylor



2017). Implementation tiers, as noted by Taylor (2017), are expected to be critical in the provision of organisational guidance, specifically providing coordination and interaction on operational risk management and cyber risk management.

## **2.6 Risk management as a component of ISMS**

Murray and Enang (2022) define risk as an uncertainty that can impact the organisation. The risk management process is described as, “systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analysing, evaluating, treating, monitoring and reviewing risk” (Srinivas, 2019). Information security risk management, therefore, is concerned with management of risk within the digital environment concerning organisational data usage. Risks, having the potential to hamper information security, are supposed to be handled through three steppingstones: integrity, confidentiality and availability (NIST, 2018).

The purpose of risk management revolves around the ability to manage and control all risks and ensure that identified risks are harmonised with the risk level of the organisation (Alanen et al., 2022). ISO developed the ISO/IEC 27005:2018 as a component of the ISO 27000 series and as standard documentation to provide organisations with advice and guidance on aspects such as risk assessment, risk reporting, risk treatment, risk monitoring, risk acceptance and risk review in an endeavour to protect organisational information resources. According to Dhillon et al. (2016), three components are involved in information security risk management forming the basis of the aim of the current research model. These are risk assessment, risk mitigation and risk evaluation.

### **2.6.1 Risk assessment**

George (2020) describes risk assessment within an organisation as the process of risk identification. Risks are identified based on their potential to occur and their expected impact, so this assists in development of risk-reduction strategies (Akinrolabu et al., 2019). Murray and Enang (2022) state that risk assessment’s major hurdle is ensuring all

risks within a system are assessed, as this allows for appropriate mechanisms to control the risk by reducing or completely eliminating the risk. Dhillon et al. (2016) identify four methods utilised in risk assessment: the identification of potential threat, identification of potential vulnerability, determination of risk and recommendation of risk control which are discussed in the following sub-sections.

#### **2.6.1.1 Threat identification**

The aim of this step is to assess and identify the source of any potential threats to information security (NIST, 2014). A threat source is described as “any circumstance or event with the potential to cause harm to an IT system (Blišťanová et al., 2022; Alanen et al., 2022). There are different human threat types, emphasising that humans are more deadly as a source of threat because their motivation to conduct the threat could be dire (Dhillon et al., 2016). To control the impact, NIST (2014) suggests an estimation of an attacker’s resources, motivation and capabilities in carrying out the attack as this assists in the determination of threat being conducted.

#### **2.6.1.2 Vulnerability identification**

The aim of vulnerability identification as the third step creates a system that identifies potential risks that an attack could exploit (Abrahamsson & Tehler 2013). NIST (2014) further suggests that the development of a security requirement checklist, system security testing and use of vulnerability source should aid in identifying sources of the vulnerabilities on the system. Based on the IT system, a number of vulnerability identification methods can be utilised and system security testing is one such method to identify vulnerabilities of the system (Chandra et al., 2022).

#### **2.6.1.3 Risk determination**

Risk determination includes a set of processes and potential methods to reduce risks or reduce associated adverse effects (Kuzminykh et al., 2021). The risk determination step assesses risk level towards the IT system (Chandra et al., 2022). To achieve its goals, the risk matrix is implemented, taking into consideration the likelihood of the risk threats

and likelihood of impact (NIST, 2014). The results are then entered into the application for monitoring and evaluating risk management controls (Chandra et al., 2022). It then uses that data to calculate the impact of threat. It also estimates the relevant actions that should be taken by management in controlling the risk impact (NIST, 2014).

#### **2.6.1.4 Control recommendation**

The control recommendations, as the ultimate result of the risk assessment process, provide input to the risk mitigation process (Chandra et al., 2022). Business organisations must adopt strategies that control risks when securing their IT environment in order to identify and neutralise potential threats before breach incidents occur (RSI Security, 2021). The risk control strategies that are at the top in information security revolve around hunting for threats, patching potential vulnerabilities and rapid incident response when cyber-attacks breach perimeter defences (RSI Security, 2021).

#### **2.6.2 Risk mitigation**

Risk mitigation, as noted by Lundberg (2020:9), is the process of prioritisation of risks based on their likelihood and expected impact. Risks that are most likely to occur are prioritised as well as those risks that have a potential severe impact on the organisation (Kuzminykh & Carlsson, 2018). Measures to mitigate the risks are also implemented at this stage (Dorian, 2012). The focus at this level is ensuring that an adequate risk level is maintained within the organisation (Dhillon et al., 2016).

#### **2.6.3 Risk evaluation**

Risk evaluation is a continuous and on-going process to ascertain if the risk management process adopted by the organisation is effective, identifying if there are any adjustments needed to make it more effective (Lundberg, 2020). Its aim is to ensure that the risk management process is thorough and that all identified risks are mitigated against (Kuzminykh et al., 2021).

Dhillon et al. (2016) warns that information security risk management on its own cannot

provide a comprehensive solution to an organisation's security concerns. He further notes that the risk management process can only provide optimal results when it is implemented earlier and merges as part of the daily organisational activities. This is buttressed by Taylor (2018) who notes that if this is not implemented, the organisation can be exposed constantly to security threats.

The process of risk management, according to Srinivas (2019), involves four elements: i) risk analysis followed by ii) risk assessment then iii) risk reduction and finally iv) risk evaluation. The emphasis of risk management on information system security of an organisation is balancing the security cost measures with operational costs so as to ensure the business attains its objectives and goals without disruption. The risk management process is the responsibility of management that initiates the process and monitors its overall performance.

## **2.7 Dynamic information security risk management**

To control the impact of technical and social threats, Lundberg (2020) suggests that the dynamic information security risk model (DISRM) be responsible for tracking and monitoring threats to organisational information data. The purpose of the DISRM, as noted by Dhillon (2018) and Lundberg (2020), is the provision of counter-measures to cyber threats that have the potential to cause organisational damage. The model works alongside cyber experts in ensuring that routines for risk management are constantly updated accordingly. The model is supposed to have the capacity to monitor any security and technical threats that have the potential to damage an organisation's information assets. This will be through activities such as breaching information data integrity, availability and confidentiality and ensuring that such threats are automatically mitigated Lundberg (2020).

Dhillon et al. (2016) argues that the DISRM has further responsibilities such as, "to re-prioritise the organisation to protect sensitive information from getting compromised with as little effect on the organisational everyday work process as possible". When

implemented accurately, the DISRM approach can act as an efficient control for security of information which helps in achieving maximum security to organisational data. Lundberg (2020) explain DISRM as, “the coordinated activities to identify and mitigate socio-technical threats to information security in a continuous and adaptable manner”.

Both internal and external individuals can pose as an information security risk to an organisation (Metalidou et al., 2014; Shamsudin et al., 2019). Dlamini et al. (2019) affirm this perspective, noting that employees of an organisation can pose a threat to its information security; such inside threats are impossible to eliminate and so require constant monitoring and managing. Moustafa et al. (2021) agrees with this assertion, elaborating that the human factor to information security is more complicated to deal with than the technical element of security. In describing inside threats, Moustafa et al. (2021) explains that these could be employees within an organisation with direct access to information assets of the organisation who harbour the intention of damaging information assets.

Employees can also be unknowingly deceived to provide a third party with access to organisation information security data (OECD, 2019; Shamsudin et al., 2019). An insider threat can also be informed of an expelled employee whose motivation to access organisational information is to damage its reputation (Forrester, 2019). Employees within organisations are aware of the fact that while full security action towards organisational information is essential, their actions might not point to the same inclination (Alshare et al., 2018). They may evade certain security actions and are not aware of roles they can play in providing the organisation with information security (Forrester, 2019).

The research by Forrester (2019) establishes that human factor contributes significantly to organisational information security management and therefore should be prioritised. As technology continues to evolve over the years, the number of information system threats also continues to multiply (Li & Liu, 2021). This is because there is an accelerating

exchange and sharing of information intra-organisation across different departments while inter-organisations are expanding (Priyadarshini et al., 2021). Manipulation of organisational information security systems goes beyond only damaging organisational information data; it can bring serious economic consequences as third parties can access an organisation's productivity and operations and can taint its public image (Snehi & Bhandari, 2021; Li & Liu, 2021; Chandra et al., 2022). Economic impact of security breaches is therefore huge (Ford et al., 2021). Across the globe in recent years, financial fraud has been the major contributor to organisational financial loss; this is carried out through system manipulation and viruses gaining access from outside (van Driel, 2019). The challenge to data security and risk management is considered an issue that conglomerates and big corporates should be concerned with, because smaller organisations only have access to limited information system as their operations do not require confidential data (Ursillo, Jr. & Arnold, 2019; Jiang et al., 2022). Big institutions are supposed to prioritise information security management as breaches can threaten huge financial and credibility loss to an organisation (Ursillo, Jr. & Arnold, 2019).

According to ENISA (2021), regulatory and legal requirements also make it mandatory for organisations to prioritise the protection of organisational and personal data; hence, organisations have the responsibility to ensure that attention is devoted to information security risks. To deal with security threats and risks, ENISA (2021) suggests that organisation be compelled to consider the cost-effectiveness of control and mitigation measures with solutions adopted that are supposed to give the organisation a higher return on investment. Cost-effectiveness can be established by comparing the impact of business disruption of the security threat versus its solution cost to mitigate against the threat if it materialise. Through this analysis, Dubojs et al. (2019) suggest that risk management contributes to the alignment of the information technology strategy with the overall business strategy of the organisation. Risk management informs the organisation on which risk to prioritise and which risks to leave unattended because, as noted by Dubojs et al. (2019), "while focusing too much on security may cause the organisation unnecessary expenses, focusing too little will cause expenses because of disruption of business continuity or damage caused to the assets by threats which were not dealt with".

Anderson and Choobineh (2018) argue that several information specialists agree that organisations downplay the seriousness of information security threats as they fail to predict their impact on information assets of the enterprise.

Making use of an information system within a business enterprise is essential in its information risk management. Assets linked to information systems should be prioritised in seeking protection (Zhao et al., 2021). According to Hayati et al. (2021), information system is defined as a system within an organisation that compiles the day to day transactions in support of the operational activities, as part of strategic activities as well as managerial behaviours in order to provide reports in the form of activity information to related parties. Information system assets refer to aspects such as software, hardware, facilities, networks and people who manage such systems. An asset is described as any element with organisational value and essential to the attainment of organisational goals and values (Eroğlu et al., 2018). Assets can further be categorised as information system assets and business assets (Phil, 2020). Under information system (IS) assets, there are elements such as operating system, programmers, enterprise model, network and accessibility control to the organisation (Dubois et al., 2019). On the other hand, business assets include elements such as skills among the employees of the organisation, and information and processes that position the organisation to achieve its goals. It is imperative to note that all business elements of the assets are immaterial; examples include data management and enterprise model. IS assets, as noted by Li and Luo (2021) are critical to the achievement of organisational goals and bring value to the organisation and can thus be a component of the information technology system and may include the employees and individuals who are actively involved in information risk management. The assets of IS are primarily material except for software (Dubois et al., 2019).

### **2.7.1 Security property**

Taylor (2017) explains that security criterion can be categorised as a constraint within the organisation that reflects its security needs of its business assets. Its purpose is acting as an indicator in analysing the risk significance within the organisation. According to

Amraoui et al. (2019), as assets are prone to risks, these risks should be constantly analysed and evaluated as security properties to assess whether they have been damaged or not. Information security assets as alluded earlier include authenticity, integrity, non-repudiation, confidentiality, availability and accountability.

Risk impact is the overall consequences of the risk to the organisation; vulnerabilities and threats form part of the risk impact (Blišťanová, 2022). The use of a Distributed Denial of Service (DDOS) by a third party to attack an organisation's website due to its servers' insufficient filtering is an example of risk impact which may lead to huge loss to the organisation like losing access to its data base (Luo et al., 2019). Risk impact can also result from a thief gaining access into an organisation's premises and accessing its sensitive documents which impacts its confidentiality and integrity of the business strategies (Jang-Jaccard & Nepal., 2014). Impact therefore has a negative consequence from a risk and has capacity to harm an organisational system.

Risk impact can result in multiple reactions to the impact; for instance, as alluded to by Luo et al. (2019), when a business entity loses its confidentiality, this also impacts its competitiveness, whilst data inaccessibility can result in poor customer satisfaction and retention due to a loss of confidence in their privacy. A combination of vulnerabilities and threats is known as an event. Somepalli et al. (2020) state that threat targets are several to assets such as software, physical components, networks and data; these threats are classified as either human acts or natural disasters. Human acts, as the name suggests, result from deliberate or non-deliberate human actions (Shamsudin et al., 2019). Malicious human actions include theft, manipulation of information system fraud, and disclosure of sensitive individual information. The number of these cases, according to research, is increasing with regard to privacy and security cases (Somepalli et al., 2020).

A threat agent, as described by Sharma et al. (2021), triggers an information security threat and can therefore be categorised as a risk source characterised based on resources available, expertise and motivation. An example might include a third party



whose technical skills are limited but who has access to a bot network. Perhaps the competitor to the business has offered them huge profits. Or there may be an insider who has access to organisational premises and information data and has been offered huge monetary rewards by external individuals. The process of conducting a threat is known as an attack. This includes document theft or manipulation of organisational information security properties (Asgari et al., 2017). Risk treatment relates to dealing with an identified risk; its purpose is to enhance the organisational security needs. Risk treatment is a holistic approach that considers the relevant decisions, controls, actions and requirements in controlling the identified potential risk. Risk treatment is comprised of various components such as risk avoidance which, as noted by Luo et al. (2019), basically relates to refraining from getting involved with the risk, also referred to as risk withdrawal. Examples of risk avoidance include not storing sensitive documents within the office and not making use of web.

Risk reduction is another element of risk treatment which, as noted by Srinivas (2019), relates to initiatives taken by the organisation to minimise the negative consequences of the risk and to establish security requirements. Examples, as noted by Luo et al. (2019), include installing network traffic filters to eliminate DDOS attacks and making use of the safe to store confidential and sensitive documents so as to minimise information theft. Another element of risk treatment, risk transfer, involves making use of third parties to help mitigate against the impact of risk on the organisation. Initiatives of risk transfer, as noted by Srinivas (2019), include taking an insurance policy to cover information loss and other initiatives like information server outsourcing or licensing a third party to control the organisation's information data. The last component of risk treatment is known as risk retention which, according to Kuzminykh et al. (2021), relates to the acceptance of the consequences resulting from the risk. Examples include acceptance of sensitive information leakages and acceptance of server unavailability (Chandra et al., 2022:8). Security requirements are important in providing solutions to prevalent risks. Risk control, as noted by Taylor (2017), relates to designed tools whose focus is improving security so as to comply with the required needs. Security controls, according to Chandra et al. (2022) include elements such as policies, practices, procedures and devices that are utilised in

the reduction of risk. Examples include back-up servers and bio-keys.

## **2.8 SMMEs in South Africa**

South Africa has been facing economic challenges such as high poverty levels, inequality and high unemployment rates since the dawn of democracy in 1994 (World Bank, 2018). SMMEs are regarded as vital instruments for achieving set socioeconomic goals and innovation as set out in South Africa's National Development Plan (Bhorat et al., 2018; Lukhele & Soumonni, 2020). Leboea (2017) argues that SMME enterprises have some economic roles to fulfil, such as contributing to the country's gross national product. Ways in which SMMEs contribute to the country's gross national product include (1) manufacturing goods of value and (2) through the provision of services to both consumers and/or other enterprises. This exclusively encompasses the provision of products, and to a lesser extent, services to foreign clients, thereby contributing to overall export performance (Leboea, 2017). From an economic perspective, SMME enterprises are not just suppliers, but also consumers of the products and services of the bigger firms. Therefore, they have an important role to play if they are able to position themselves in a market with purchasing power. Their demand for industrial or consumer goods will improve the productive activity of their suppliers, just as their own productive activity is stimulated by the demands of their clients (DTI, 2019). The demand in the form of investment has a dual role to play, from the demand side (with regard to the suppliers of industrial goods) and on the supply side (through the potential for new production arising from upgraded equipment). Furthermore, demand is important to income-generation potential of SMMEs, and their ability to stimulate the demand for both consumption and capital goods.

Most importantly, and from a South African context, in theory, SMMEs have the potential to generate employment and upgrade human capital, due to their low capital and mechanisation levels. The nature of work in SMMEs is labour intensive. However, this is not always the case as the SMMEs usually struggle in business due to a number of factors: poor access to finance and credit, poor infrastructure, low levels of research and

development (R&D), onerous labour laws, an inadequately educated workforce, inefficient government bureaucracy, high levels of crime and lack of access to markets (Oyelana & Adu, 2015; Bureau for Economic Research, 2016). Economic historians have demonstrated the importance of this phenomenon in Europe's industrialisation and the subsequent development of other emerging economies (Zervoudi, 2020). As technological progress in agriculture liberated the agrarian labour force, this unskilled excess labour force was absorbed into small manufacturing industries and exposed to business experience, thereby encouraging a "learning-by-doing" effect (OECD, 2014). From the European industrial revolution we can therefore learn that the combination of job creation and skills upgrade which can be offered by SMMEs enhances the process of industrialisation, and social and economic development in a nation.

South Africa's current economic situation is comparable to the above scenario: the excess labour force is released, not so much from the agricultural sector, but rather from large enterprises in the secondary and tertiary sector (Bvuma & Marnewick, 2020). UNHCR Global Report (2020) states that enterprises are not necessarily facing economic recession, but they are rather growing and transforming themselves in such a way that their demand for unskilled labour is generally decreasing. This results in an abundant pool of unskilled labour, which SMMEs can possibly employ and upskill.

From a different viewpoint, it has been suggested that, in cases of jobless growth and a mismatch between the demand and supply of unskilled labour, a shift in both the sectorial composition of the economy and the occurrence of growth in different categories of firms may be an important avenue for the generation of both employment opportunities and growth (Oyelana & Adu, 2015). The question here is whether a more robust SMME growth strategy in South Africa will bring about such changes. This in turn depends on whether SMMEs are more labour-intensive and therefore likely to employ unskilled labour, and whether they can provide a process of skills upgrading. With these categories of functions defined from a theoretical perspective, the following section examines the structure of the South African economy to see whether SMMEs can, in their current position, fulfil these

roles.

### 2.8.1 Factors affecting SMMEs in South Africa

SMMEs, however, continue to be shadowed by their larger business counterparts with regards to GDP and innovation contribution. According to Bushe (2019), more than 70% of SMMEs fail in their first five to seven years of inception. There is an abundance of literature regarding the general and typical challenges faced by SMMEs in South Africa (Sitharam & Hoque, 2016; Leshilo & Lethoko, 2017). These challenges mostly relate to aspects such as access to capital, government regulations, education, which youth-owned SMMEs also experience. Findings from the literature on specific challenges faced by youth-owned SMMEs in South Africa are set out in Figure 2.3 below:

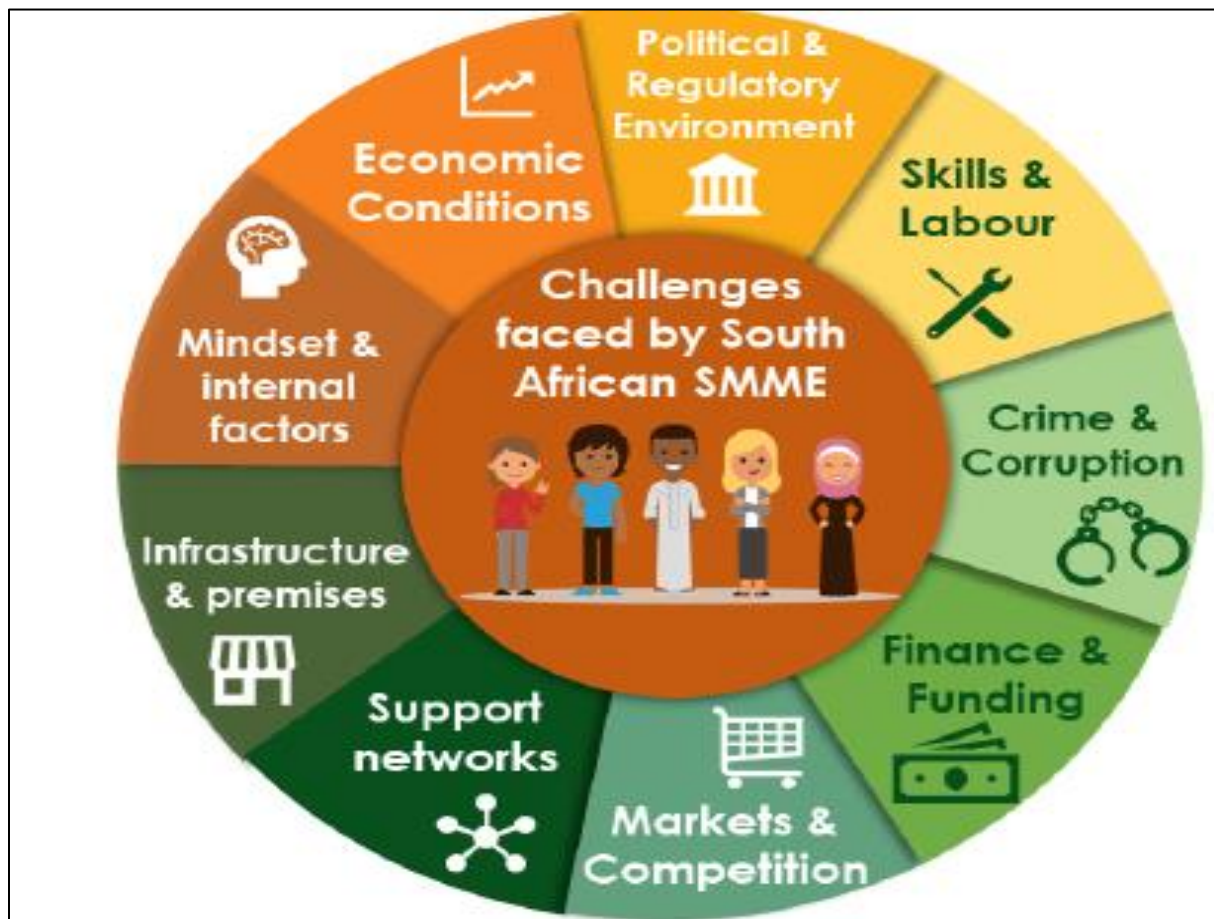


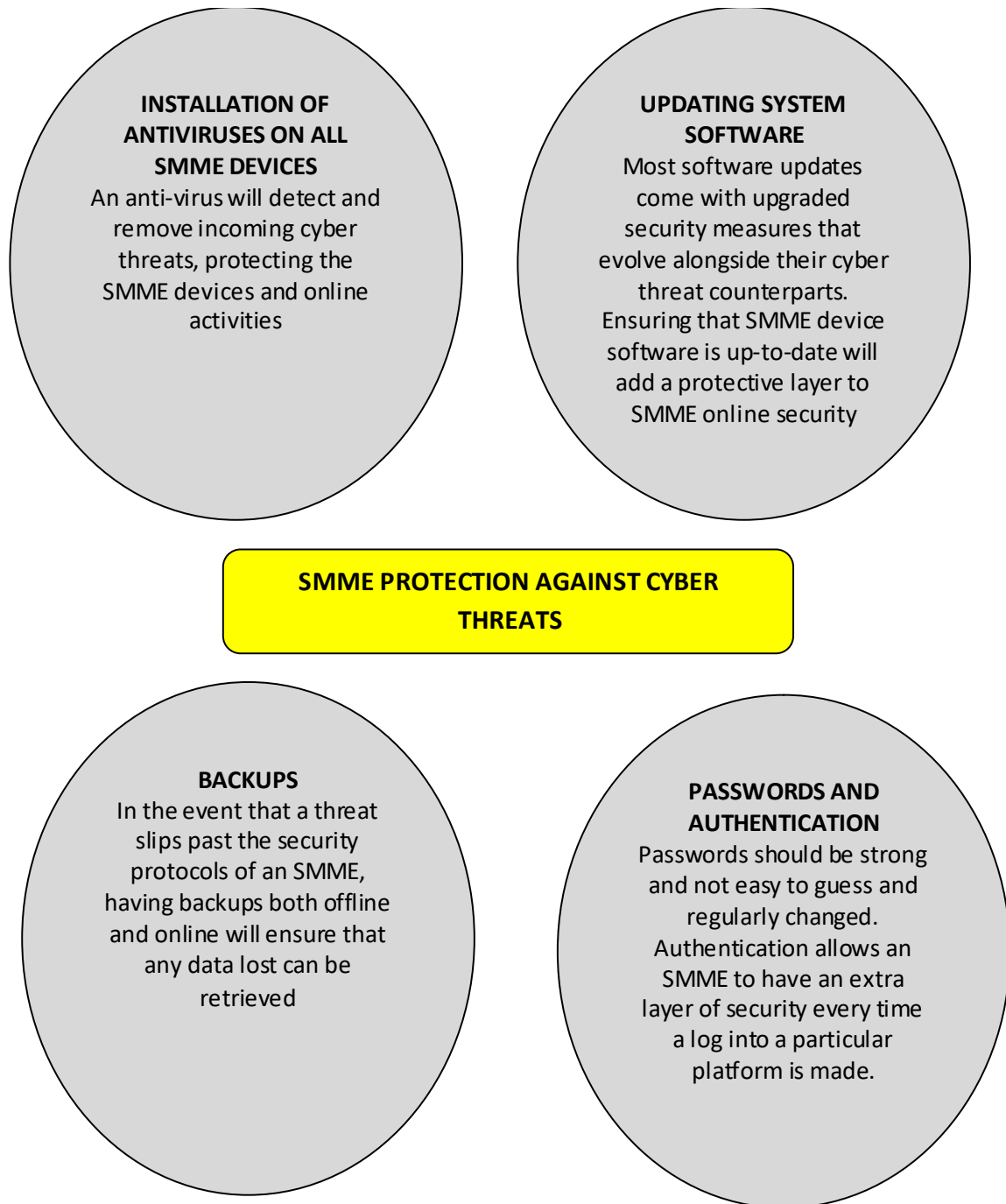
Figure 2.3: A summary of the challenges faced by South African entrepreneurs. Source: SEDA

(2019)

One reason why SMMEs in South Africa are not flourishing is because of information insecurity (Flynn, 2022) although this was not included in SEDA (2019)'s summary. SMMEs in South Africa are most vulnerable to cyber-attacks as they either do not invest in cyber security due to a lack of knowledge or inability to afford. Cyber-attacks lead to system damage, theft of vital confidential or financial information, and compromised data. The impact on SMMEs could be extremely detrimental as one may even incur legal fees if the virtual attack leads to the loss of third-party information. SMMEs are reluctant to take digital preventative measures to secure their resources or assets. Just like any other business that would not underinsure tangible business assets, South African SMMEs should not leave their digital assets unlocked in plain sight of criminals. In an SMME environment with a free flow of money, preventative measures must be weighed against the cost of not having security protection established as threats are becoming more prevalent (Flynn, 2022).

## **2.9 How SMMEs in South Africa counter cyber threats**

In South Africa, SMMEs are most vulnerable to cyber threats as they both do not invest in cyber security due to the expensive cost of adopting it as well as the general lack of knowledge (Devlin, 2021). Cyber threats lead to system damage, the theft of confidential information, and compromised data (Mimecast, 2019). This problem is more serious when the customers' data is compromised which should be protected at all times (Malumo, 2023). The impact on an SMME could be extremely detrimental as legal costs may be incurred (Accenture, 2019). It is therefore imperative that an SMME be protected so that attacks from cybercriminals can be prevented (Malumo, 2023). Illustrated in Fig. 2.4 are the steps an SMME could follow to ensure the safety of the business.



**Figure 2.4: Steps that can be followed by an SMME to counter cyber threats. Source: Malumo (2023).**

## **2.10 Overview of the target SMME for this study**

This study focuses on SMMEs in the tourism sector in Cape Town, South Africa. South Africa in recent decades, has positioned itself as one of the top tourism destinations in the world as tourists from across the world are attracted to its cultural and natural heritage. Tourism plays an important role in South Africa's economy. According to Stats Sa (2021), the sector contributed 3.7% to the national Gross Domestic Product (GDP) in 2019. Due to the Covid-19 pandemic, there was a drastic drop in tourist arrivals and the sector is recently showing improvement (Stats Sa, 2022).

SMMEs play a significant role across the South African tourism value chain: they play a key role in providing accommodation, tourism transport and tourism activity organisers, craft producers as well as souvenir shops (Hudson, 2023). The SMMEs in the tourism sector like any other SMMEs are prone to cyber threats which in total account for 43% of annual cyber attacks (James, 2023). With these concerning statistics, SMMEs must be conscious of the threats faced by their businesses and take precautionary measures. The increase in internet usage is a cause for alarm that all SMMEs should take into consideration. Unfortunately, SMMEs have limited resources to dedicate to cybersecurity which makes them vulnerable to cyberattacks (Brewerton, 2013; Yoshino & Taghizadeh-Hesary, 2016; James, 2023). As a step to counter the concerning statistics, this study evaluates the information security aspects and investigate how they can be included in the information security management framework for SMMEs in the tourism sector of South Africa.

## **2.11 Summary**

This chapter presented a detailed literature review concerned with aspects of information security. Discussed in this chapter is why security is needed, an overview of information security; the security framework; risk management as component of ISMS, dynamic information security risk management; and narrowing down to SMMEs in South Africa. From this chapter, SMMEs are generally prone to information security breaches because of the lack of simple control and planning systems and limited standardisation of

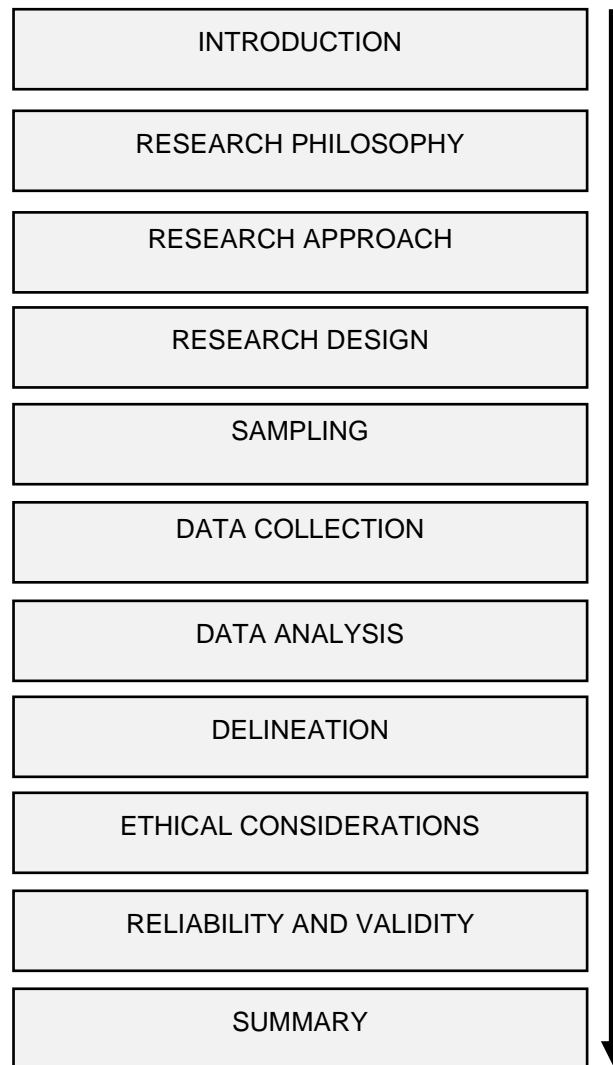
information processes as extensively described in this chapter. Despite having a significant amount of research focusing on managerial and technological aspects on ISM, there appears to be a gap on the three control types, and this leaves organisations with a need for coherent and detailed guidance on the types of practices that management can utilise in the process of information protection. Owing to this problem of security threats as a factor affecting SMMEs in South Africa, this study evaluates the information security aspects for SMMEs in Cape Town. Presented in the next chapter is the research methodology that was used to collect data for this study.



## CHAPTER 3

### RESEARCH METHODOLOGY

The layout of Chapter 3 is illustrated in Fig. 3.1 below.



**Figure 3.1: Layout of Chapter 3**

#### 3.1 Introduction

The previous chapter presented a detailed review of existing literature on information security aspects around businesses, particularly SMMEs. This chapter gives a clear and

detailed description of the research methodology in line with research aim and objectives. The research methodology chapter presents information on the research philosophy, nature of the present study, research instrument (questionnaire), data collection method, data analysis, reliability, validity and ethical considerations of the study, concluding with a summary relating to material covered in the chapter.

Research methodology is defined as “a systematic way of solving research problems comprising the theoretical analysis of a body of methods as well as principles associated with a branch of knowledge” (Igwenagu, 2016:4). Research methodology is defined as a field that assesses and explains the justification for appropriate research techniques and methodologies for a certain research topic (Bradshaw et al., 2017). Saunders et al. (2019:4) defines research methodology as a systematic way or method of solving research problems. It comprises of the theoretical analysis of a body of methods as well as principles associated with a branch of knowledge (Creswell & Creswell, 2018:309). The research onion as illustrated in Figure 3.2 below is a diagram that shows the various methodological choices that can be used, including research philosophies, research approaches, research strategies, research choices, and time horizons (Saunders et al., 2019:130). Components of the research onion are unpacked in the following sections which further narrows down to how this study fit in the onion.

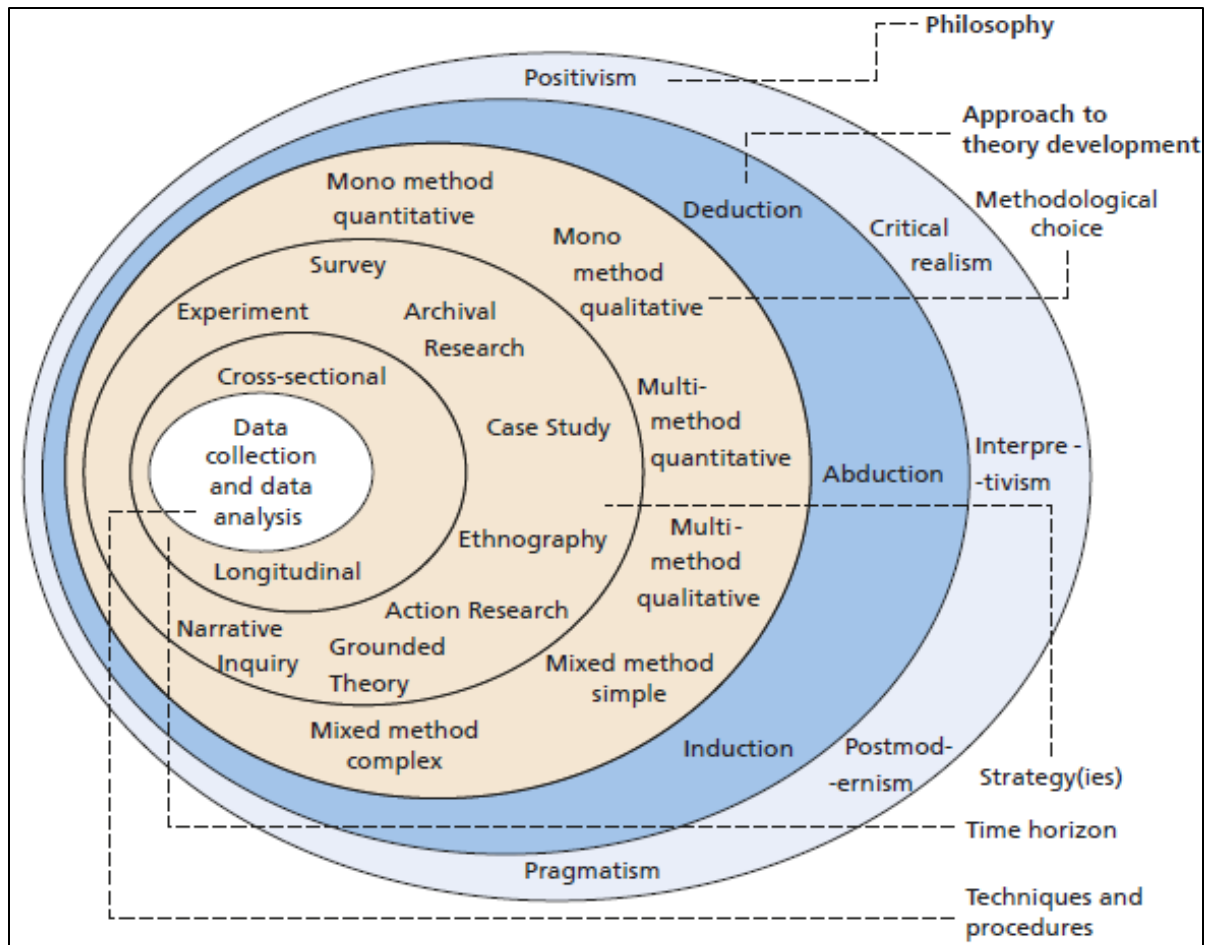


Figure 3.1: The research onion. Source: Saunders, Lewis and Thornhill (2019:130)

### 3.2 Research philosophy

Research philosophy, according to Adams et al. (2014), refers to philosophical orientations about the world as well as the type of research being conducted. The choice of method to be used by a researcher is motivated by researcher's epistemology as well as theoretical position and how these shape and influence the research approach (Mertens, 2015). A research study can be conducted using either of the two philosophical positions namely: i) ontology or ii) epistemology (Saunders et al., 2019:133). In the following sub-sections these positions are presented.

#### 3.2.1 Ontology

*Ontology* is more suitable for conducting quantitative research because it is used in describing facts as a nature of reality and nature of science. Ontology is a philosophy

branch concerned with assumptions we make so as to believe that a phenomenon makes sense or is real, or the very nature or essence of the social phenomenon being investigated (Kivunja & Kuyini, 2017). Ontology examines the researcher's underlying belief system about the nature of being and existence and helps conceptualise the form as well as nature of reality and what a researcher believes can be known about that reality. There two main ontological approaches, namely objectivist and subjectivist (Kivunja & Kuyini, 2017:27).

i) Objectivist

The thrust of objectivism is portraying that, "social entities exist in reality external to social actors concerned with their existence" (Creswell & Creswell, 2018:68). It illustrates that a research phenomenon can exist independent of the researcher and PIs who are classified as social actors.

ii) Subjectivist

Subjectivism holds that actions and perception of social actors contributes towards the construction of social phenomena; Creswell and Creswell (2018:69) notes that "ontological position which asserts those social phenomena and their meanings are continually accomplished by social actors".

### **3.2.2 Epistemology**

Epistemology is used to "describe how individuals come to know something, how the truth or reality is known, or what counts as knowledge within this world" (Kivunja & Kuyini, 2017). It is concerned with the bases of knowledge, its nature and forms and how it can be acquired, as well as how it can be communicated to other beings. Epistemology focuses on the "nature of human knowledge and comprehension that the researcher can possibly acquire so as to be able to broaden, extend and deepen an understanding in a particular field of research" (Kivunja & Kuyini, 2017:27). Within epistemology there are several branches and approaches, for example positivism and interpretivism among others.

i) Positivism

Within positivist research, the researcher and the research are independent from the physical and social reality and hence not influenced by it. A single truth is obtained from the research following objective testing. Positivist studies make use of experiments so quantifiable data is gathered and the findings are reported objectively.

ii) Interpretivism

The interpretive research approach emphasises the need for the research phenomena to be understood from the signs that the target population assign to the researcher. An interpretive researcher is focused on understanding, meanings, values and beliefs of the research phenomena so as to gain an in-depth understanding of the experiences and activities of the study population. Interpretive paradigms, as noted by Kivunja & Kuyini (2017), “emphasise the creativity aspects of science and how scientific knowledge is built through subjective interpretations of observations in the context of the researcher’s knowledge and mental models”.

Table 3.1 compares the interpretive and positivist approaches.

**Table 3.1: Comparison of interpretive and positivist approaches**

Interpretive approach	Positivist approach
Research is contextualised the researcher values the environment of the research setting	Makes use of quantifiable variables and thus is aimed at attaining an objective truth
Researchers are heavily immersed in the study as they actively participate in the selection of PIs, data collection and analysis; hence, the study is dependent on the researcher.	The research is independent from the researcher and thus the researcher cannot influence the outcome
Findings are not generalisable The study is flexible, and the researcher can adjust to cater for new developments in the study	Research findings can be generalised A structured approach is strictly adhered
Utilised in the collection of qualitative data Starts from data generation which is used to inform theory development	Used in the collection of quantitative approach Study is imbedded in theory, then data generation
Consider that the language, culture, values and religion or general context can influence the Ps	Assumes that social reality is independent from the research Ps; hence, context and research settings are not regarded as influencing the study

### **3.2.3 Research philosophy for this study**

For this research, a subjectivist and interpretivist philosophies were invoked to enable the researcher to explore the perceptions and experiences of the participants. This is for the researcher to be a real partner with the participants, and also to openly use own

experiences and reflections to uncover valuable meaning.

### **3.3 Research approach**

A research approach comprises “plans and procedures that consist of the steps of broad assumptions to the detailed methods of collecting data, analysis and interpretation” (Saunders et al., 2019). In some publications, a research approach may simply imply data collection and data analysis methods in general and the differences between quantitative and qualitative methods in particular. A research approach is, however, best seen as a general plan and procedure for research or conducting a study (Saunders et al., 2019). Accordingly, research approaches can be divided into three categories – deductive, abductive and inductive approaches – which are discussed in detail in the following sub-sections.

#### **3.3.1 Inductive research approach**

The aim of the inductive approach is to establish limited generalisations about distribution of patterns of association amongst measured or observed traits of individuals and social phenomena (Malhotra, 2017:172). In an inductive approach, there is a gap in the logic argument between the premises observed and the conclusion, with the latter being judged as supported by observations made (Woiceshyn & Daellenbach, 2018:3; Saunders et al., 2019). The inductive approach therefore assumes that all scientific work starts with observations which provide a secure basis from which information and knowledge can be derived and claims that reality impinges directly on senses; hence, there is correspondence between the sensory experiences, albeit extended by instrumentation, as well as the objects of those experiences (Malhotra, 2017:172).

#### **3.3.2 Deductive research approach**

The deductive approach is the reverse of the inductive approach (Nie & Wu, 2021:22). It begins with a “tentative hypothesis that forms a theory which could provide a possible explanation for a particular problem or phenomena, then proceeds using observations to rigorously test the hypothesis” (Malhotra, 2017:172). The deductive approach accepts

that an observation is guided by theory so this approach works from the more general to the more specific (informally called a 'top-down' approach) (Borgstede & Scholz, 2021:1). In this approach, one highlights an argument based on existing knowledge about the selected subject which is then researched to fill in the gaps (Malhotra, 2017).

### **3.3.3 Abductive research approach**

The abductive research approach involves constructing theories derived from social actors' language, meanings and accounts in the context of day-to-day activities (Żelechowska et al., 2020). Such research starts with a description of these activities; meanings then derives from the categories that form the basis of understanding the problem at hand (Awuzie & McDermott, 2017). This approach is used by interpretivism to produce scientific accounts of social life by drawing concepts and meanings used by social actors and the various activities in which they engage. Abductive approaches acknowledge that human behaviour depends on how individuals interpret the conditions in which they find themselves, thereby accepting the essentiality of having a description of the social world on its own terms (Malhotra, 2017).

This study follows the deductive approach. The logic that the researcher follows is inductive, from the bottom up, rather than handed down entirely from a theory or perspective of the researcher. This is useful because occasionally the research questions change in the middle of the research to better reflect the types of questions needed to grasp the research problem. Adopting an inductive approach means that the researcher decides to conduct the study on some individuals, in this case, those who are in SMMEs in the tourism sector, who are knowledgeable about the sector. The researcher is interested in their feelings about the SMMEs and situations they have experienced, how they coped with the problems their SMMEs encounter and their views about possible solutions. The data collection strategy, planned prior to the study, needs to be modified accordingly, to accompany the new questions. During the analysis of data, the researcher then followed a path of analysing the data to develop an increasingly detailed knowledge of the topic being studied.



### **3.4 Research design**

A research design is a structural framework of various research techniques and methods that are utilised by a researcher (Saunders et al., 2019). The research design helps researchers pursue their journeys into the unknown but with systematic approaches to guide them (Asenahabi, 2019:76). The research design is categorised into “quantitative and qualitative research design” (Creswell & Creswell, 2018:41; Saunders et al., 2019; Asenahabi, 2019:77).

#### **3.4.1 Quantitative research design**

In quantitative research design, researchers examine the variables while numbers as well as statistics are included in a project to analyse the findings (Allen, 2017). The use of figures, graphs, pie charts and frequency tables is the main form of data collection measurement in quantitative research design (Allen, 2017).

#### **3.4.2 Qualitative research design**

Qualitative research design, on the other hand, is contrary to quantitative research design (Saunders et al., 2019). Qualitative research design is explanatory in nature and is always seeking answers to “What is” and “How is” (Charmaz, 2015). Qualitative research design primarily focuses on why specific theories exist and how the respondent answers to it. This allows researchers to draw conclusions with proper findings (Charmaz, 2015).

#### **3.4.3 Mixed methods research design**

This is the branch of multiple methods research integrating the use of qualitative and quantitative data collection methods and data analytical procedures in the same research project (Creswell & Creswell, 2018:41; George, 2022). It is based on philosophical assumptions that guide data collection and analysis and the mixing of quantitative and qualitative collection techniques and analysis procedures (George, 2022). Researchers using mixed methods have a pluralist view of the research methodology as they believe

that flexibility in the selection of methods (both qualitative and quantitative approaches) is legitimate and that researchers should be tolerant of other researchers' preferred methods, even if they differ from their own (Saunders et al., 2019). These views can be contrasted with those researchers who believe that there should be a single legitimate method that should be followed (Saunders et al., 2019).

### 3.4.4 Research design for this study

The three research designs are summarised in Table 3.2 below.

**Table 3.2: Comparison of qualitative, quantitative and mixed methods designs**

Qualitative design	Quantitative design	Mixed methods design
Emerging methods	Pre-determined	Both emerging and pre-determined
Open-ended questions	Instrument based questions	Both open-ended and close-ended questions
Interview data, observational data, document data and audio-visual data	Performance data, attribute data, observational data, and census data	Multiple forms of data drawing on all possibilities
Text and image analysis	Statistical analysis	Statistical and text analysis
Themes, patterns interpretation	Statistical interpretation	Across databases interpretation

Source: Creswell (2014:45)

This study used the mixed methods research approach as it allowed the researcher to combine both inductive and deductive thinking to address the research problem (George, 2022).

### 3.5 Sampling

To address the problem of population size, a sample of the population was selected to

represent the whole population. A sample is defined by Creswell and Creswell (2018:212) as, “a small proportion of the population that is selected for observation and analysis”. The sample for the current study were 13 IT experts (Unit of Observation) at management level within their organisations.

By observing the sample characteristics, certain inferences can be made with regard the population’s characteristics. Saunders et al. (2019:297) and Palinkas et al. (2015) states that through probability sampling the researcher can generalise the findings results to represent the overall population from whom the participants were drawn. Saunders et al. (2019:315) explain that non-probability sampling includes snowball, convenience, purposeful and volunteer sampling. The study adopted purposeful sampling, “the logic and power of purposeful sampling lies in selecting information rich cases for the study in depth. Information rich cases are those that one can learn a great deal about issues of central importance to the purpose of the inquiry, thus the term purposeful inquiry”. Before initiating purposeful sampling, it is imperative to determine the criteria used in selecting a study site. For the current study, participants had to be employed by SMMEs operating in the tourism sector in Cape Town and working in the field of information technology and with an influence on organisational strategy.

### **3.6 Data collection**

The participants were selected based strictly on the official job position and functions at their workplace with regard to implementation of an information security framework. This is affirmed by Döringer (2021) who argue that “respondents should be experienced and knowledgeable in the area they are being investigated”. Research data can be more credible and convincing if informed by experienced and knowledgeable participants as they are positioned to provide quality information (Döringer, 2021). The research administered questionnaires to information technology experts and data analysts within the case study organisations due to their knowledge about information security management framework implementation within their organisations.

This study considered the primary method of data collection in choosing the method for obtaining data, with a decision on the study sample size, sampling technique as well as the data construction instrument. The semi-structured questionnaires were administered to 13 employees of SMMEs in the tourism industry in Cape Town. The study chose semi-structured questionnaires because they are simple to administer and have a higher response rate than other data collection methods.

### **3.6.1 Interview guide**

Saunders et al. (2019) state that based on the interpretivist approach, a small data sample is required for the collection of detailed and in-depth information. An interview undoubtedly performs a valuable function in obtaining comprehensive data that can be easily compared, say, by district or age and gender, and with other studies. As the focus of mixed methods incorporates both qualitative and quantitative approaches, to allow the researcher to experience the perspective of the interview guide, the researcher focused on developing semi-structured questions, allowing the participants to express themselves without restriction. In this study, data were collected by conducting interviews.

### **3.7 Data analysis**

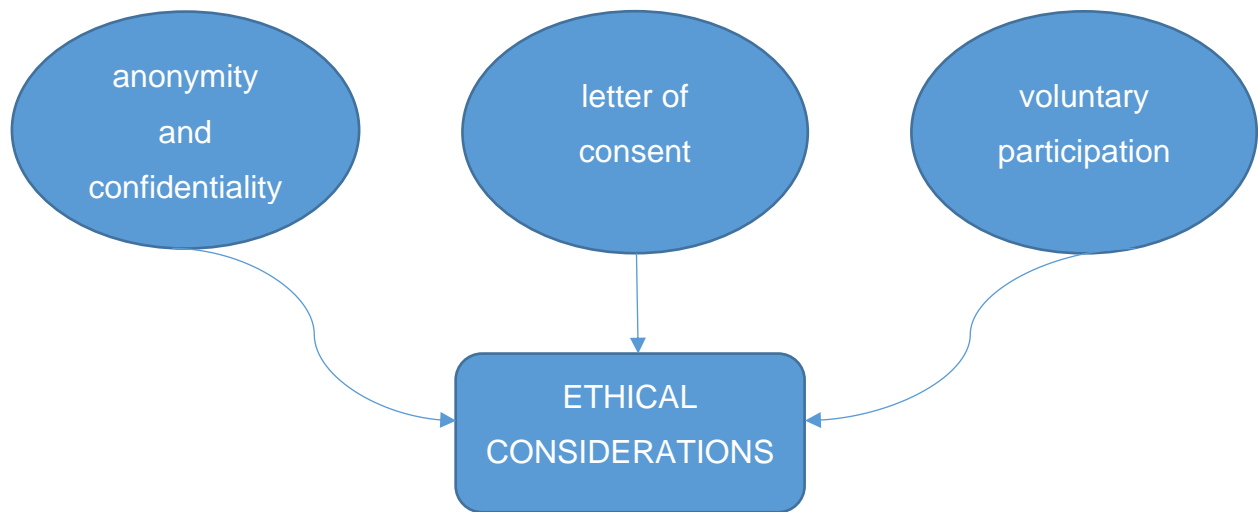
The data in this study was analysed using descriptive and interpretive analysis. Out of the 15 questionnaires emailed to the participants 13 responded. Each questionnaire was labelled 1-15 and corresponding responses were coded for Section A and C and entered into Microsoft Excel where figures, charts and tables were generated to allow easier comparison, presentation, validation and reliability of the findings. For the qualitative sections, a qualitative descriptive approach was utilised to provide straightforward descriptions of the experiences of the participants (Sandelowski, 2010; Doyle et al., 2020). A qualitative descriptive design was deemed most appropriate for the qualitative sections study as it recognises the subjective nature of the problem being investigated, the different experiences of the participants which are presented in a way that directly reflects the terminology used in the research questions (Doyle et al., 2020).

### **3.8 Delineation**

The study only focused on tourism SMMEs in Cape Town. As the research period is between 2022 and 2023, the study might not be applicable in different locations and in differing time periods.

### **3.9 Ethical considerations**

Creswell (2018) states that ethical considerations within research entail that the rights and welfare of Ps are protected throughout the research process. The researcher applied for an ethical clearance from the Ethical Committee of the university before conducting the study to ensure the study was undertaken in an appropriate manner under the consideration of ethical values. The ethical approval certificate is attached in Appendix 2. Figure 3.3 summarises the ethical considerations that were adhered to in this study which are described in the sub-sections that follow.



**Figure 3.3: Summary of ethical considerations**

### **3.9.1 Letter of consent**

Fleming and Zegwaard (2018:210) suggest that before participating in research, the participants must openly consent to participate. The letter of consent (Appendix 1) illustrates the research purpose and also highlights that the participants were informed of the research purpose, that it was for academic purposes only.

### **3.9.2 Anonymity and confidentiality**

The researcher assured the participants that their identity will be protected. The anonymity was assured by assigning the participant with codes such as participant 1. The researcher transcribed the data and had no vested interest in the organisations used as case studies and therefore participant anonymity remained high.

### **3.9.3 Voluntary participation**

The purpose and nature of the research was disclosed to all participants and the research was not conducted without formal consent of the participants. Participation was voluntary and the participants had the right to refuse to participate. The participants were given the

right to refuse to answer certain questions or to terminate their participation in the research at any point, without repercussion. In addition to verbally explaining the process to the participants, each participant was required to sign a consent form to participate in the research, as prescribed by the university. The consent form (Appendix1) explained the purpose, procedures, confidentiality and participants' rights. Participation in this study was not by coercion, as individuals participated of their own volition.

### **3.10 Reliability and Validity**

#### **3.10.1 Reliability**

Parnis et al. (2015) states that the reliability of the study is referred to as reliability, and this is decided by the dependability, consistency, predictability, stability, and honesty of the research instruments. Parnis et al. (2015) also mentions that reliability relates to the credibility of the research findings and the extent to which the research findings can be generalised and replicated. Parnis et al. (2015) further alludes that reliability is a criterion that observes the quality of research in reference to the measures used and data collected to provide consistent results and the concept of quality in qualitative research relates to generating an understanding of the topic.

Considering the issues around increasing reliability in qualitative research are critical. Parnis et al. (2015) emphasised that in order to ensure reliability, a researcher should consider the degree of bias in the sample design and selection, the consistency of the fieldwork, the systematic analysis of extensive data, the justification for the interpretation of data, and whether the design and conduct of the data collection accurately reflect the perspectives of all participants.

High-quality integration between the data-collection process, data analysis, and theory generation is required to assure the dependability and reliability of a research project (Cleary et al., 2014). It was essential to keep a thorough and accurate record of the data-gathering method so that other researchers may replicate it if necessary in order to ensure

high standards of dependability in this research investigation (Kumar, 2014).

Furthermore, Marshall and Rossman (2016) noted that in order to evaluate the reliability of qualitative research, the research questions should be clear, the researcher's role within the research site should be explicitly described, the findings should demonstrate significant parallelism across data sources, the fundamental paradigms and analytic constructs should be clearly specified, the data should be collected in conjunction with the research questions, proper data-collection protocols should be followed, and data quality should be combined.

In summary, reliability was evaluated by carefully documenting the methods used to produce and interpret data. Voice-recording equipment was used to record the interviews, which were then accurately presented along with a comprehensive transcription of the recordings and questions that elicited certain responses.

### **3.10.2 Validity**

Validity refers to the accuracy of the research findings in relation to the reality of the situation researched (Cleary et al., 2014). The validity, in its broadest sense, refers to the accuracy of the data collected from people close to the topic under study by the researcher (Kumar, 2014). In addition, validity is a construct referenced to the quality and ability of the research instrument to measure the research questions (Kumar, 2014).

In summary, validity is understood as the “correctness” or “precision” of the reading of the research (Lewis & Ritchie, 2013). Furthermore, Lewis and Ritchie (2013) asserted that when evaluating the validity, researchers must ask themselves a series of introspective questions: first, whether there was any bias in the sample design or selection; second, whether the questions' quality allowed participants to fully express their perspectives; third, whether the research questions had been identified, categorised, and labelled appropriately; and fourth, whether the respondents' feedback was accurately interpreted.



A fixed demonstration of abstracts and a standard assessment of variables are not necessary for the measurement of validity in qualitative investigations. So, in order to establish credibility by correctly interpreting the participant data, this research study first ensured validity. As a result, this research study ensured validity by first ensuring credibility through accurately interpreting data collected from participants (Koonin, 2014). In qualitative research, participants are the most important assessors of validity because the study focused on their experiences, perceptions, and beliefs; as a result, validation, confirmation, and approval would depend on how well the participants' concordance matched the finding (Kumar, 2014).

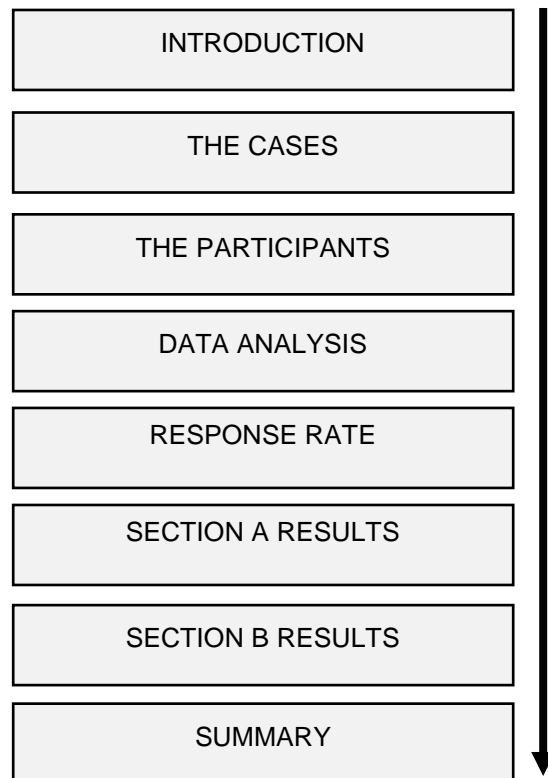
### **3.11 Summary**

This chapter described the detailed the research methodology for the execution of the research. This chapter first established the research philosophies as interpretivism, subjectivism, and pragmatism and elaborated on the subjectivist philosophical position which this study bases on. The mixed methods was then introduced as this study's research approach, backed by the inductive-theory-building method. Semi-structured interviews were administered to 13 participants in tourism SMMEs who have knowledge of information security aspects. These were sent via email or WhatsApp to respondents. The completed questionnaires were coded and analysed in MS Excel and SPSS. The ethical considerations of this research study underpinned this chapter, with detailed accounts of the processes related to informed consent, anonymity, confidentiality, and participants' protection during the data-collection processes. The next chapter presents the findings from this study.

## CHAPTER 4

### RESULTS

The layout of Chapter 4 is illustrated in Fig. 4.1 below.



**Figure 4.1: Layout of Chapter 4**

#### 4.1 Introduction

The preceding chapter reported on the research methodology adopted in this study. The chapter explores the theoretical aspects of the research approaches, rationale as well as the data collection and analysis process. This chapter presents the results from this study. The research findings are presented in frequency tables, graphs and charts. Figure 4.1 shows the outlay of Chapter 4. Firstly, the response rate of the survey is presented. This is then followed by three sections namely Section A showing the demographics of the

study and Section B and C presenting the results.

## **4.2 The cases**

This study targeted SMMEs in the tourism industry in Cape Town, Western Cape Province. The selection of the SMMEs were bound by the SA definition according to Section 1 of the NSB Act of 1996 as amended by the NSB Acts of 2003 which was described in Chapter 1. Therefore cases for this study, the following businesses were included:

- those operated by business owners and their families with less than five people employed and an annual turnover of less than R150 000
- those which are informal and employ less than ten employees who are paid
- those that are formally registered which have fixed business premises and have a complex management employing up to 50 people
- those characterised by a decentralised management structure and employs up to 200 employees.

Within the SMME, the IT department was specifically targeted as it met the scope of this study. Respondents from various IT departments made up the sample for this study and comprised of: IT Technicians, IT managers, web masters, web developers and software managers. Questionnaires were used for this study which were administered to 13 respondents. Further details of the respondents are presented in Section A and the questionnaire responses in Section B and C.

## **4.3 Data analysis**

The data in this study was analysed using descriptive and interpretive analysis. For the most part, the researcher was interested in using the data to evaluate information security aspects in SMMEs in Cape Town to articulate what it meant and to understand it. The study used thematic analysis for the categorisation, tabulation, classification, and

summarizing of all employee behavioural information as well as verbal information. Each questionnaire was labelled 1 – 15 and corresponding responses which were coded for Section A and C and entered into Microsoft Excel where figures, charts, and tables were generated to allow easier comparison, presentation, validation, and reliability of the study findings. The coded data was analysed using the COUNTIF function in Microsoft Excel and SPSS in order to produce meaningful explanations for the data.

#### 4.4 Response rate

The target research sample constituted 13 participants from three SMMEs purposively and conveniently selected (both participants and SMMEs) and operating in Cape Town. The sample translated into five participants from each organisation and the participants were drawn from the IT departments. The response rate was 87% (Figure 4.2). Unfortunately, two participants withdrew at the last minute, constituting the 13% no response category as shown in Figure 4.2.

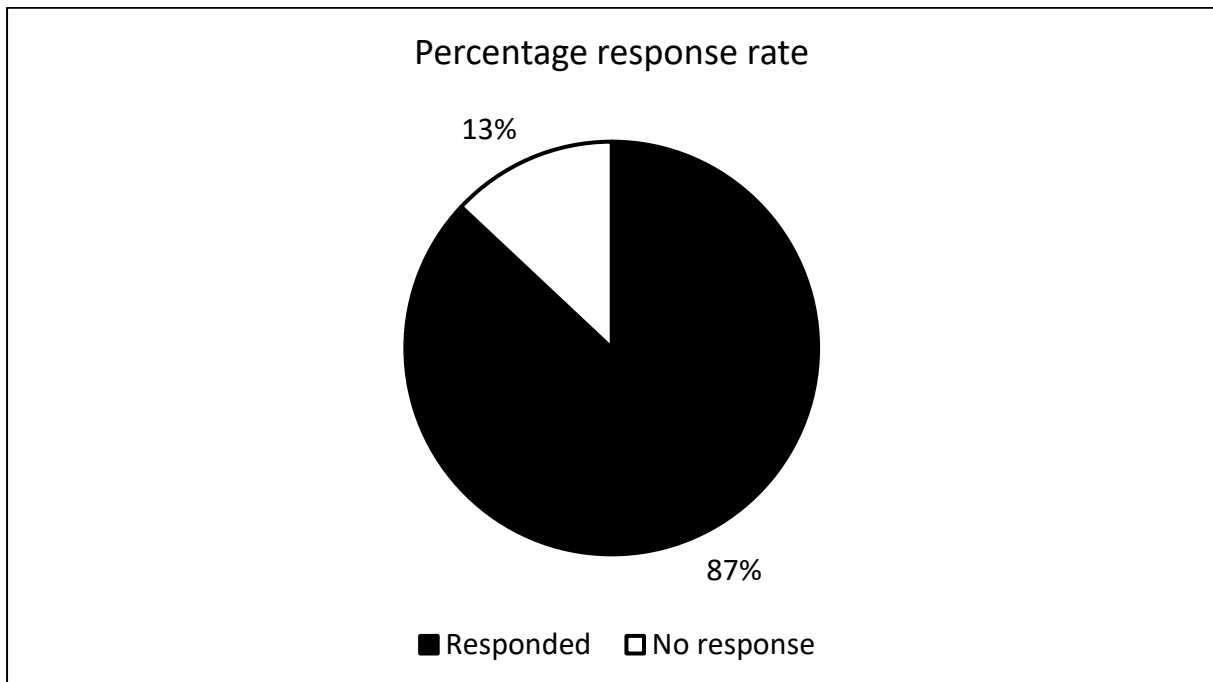


Figure 4.2: The response rate from the survey

## 4.5 Section A results

### 4.5.1 Gender

The gender of the respondents was females (n = 7) and males (n = 6), as illustrated in Figure 4.3.

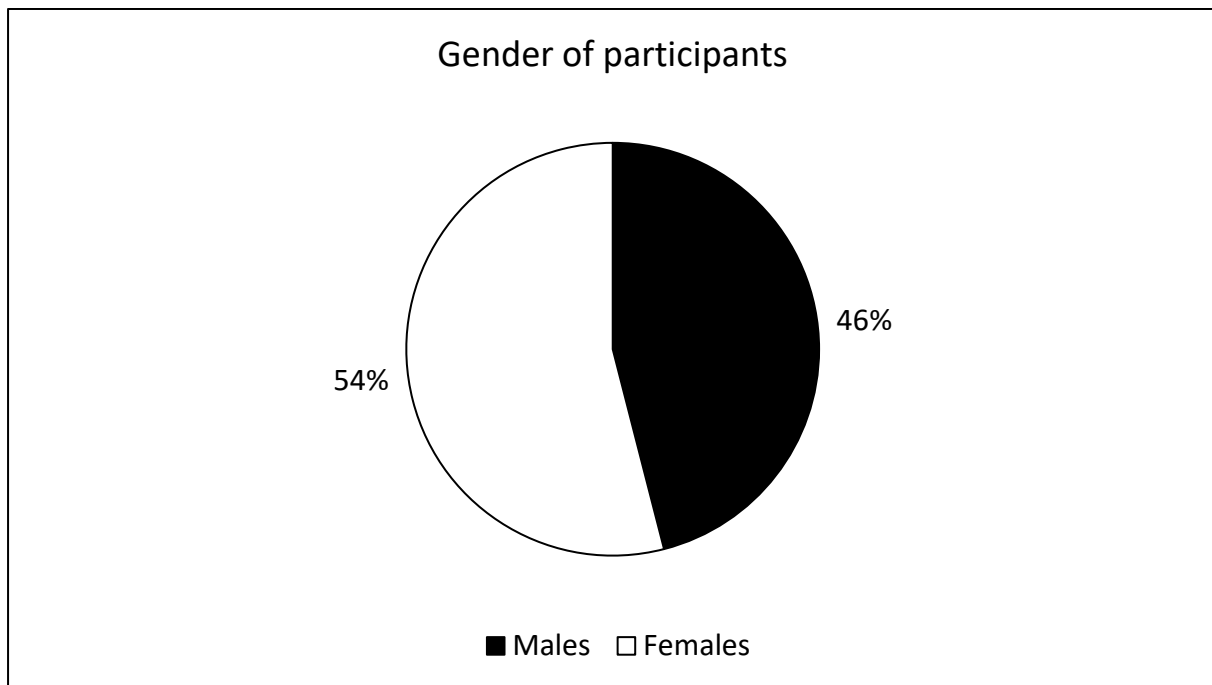


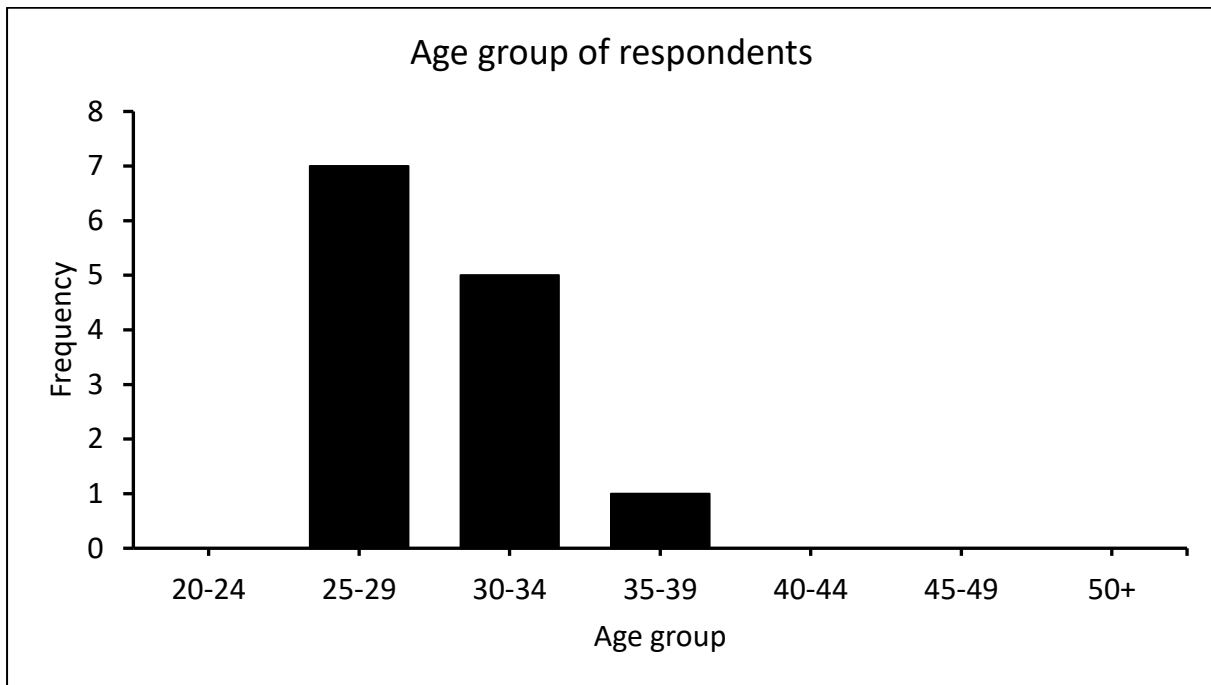
Figure 4.3: Gender of participants

### 4.5.2 Age

The age of the respondents ranged between 25 to 39 years (Table 4.1; Figure 4.4). The age modal group was 25-29 years which comprised 70% of the respondents (Table 4.1). No respondents were below 25 years or above 39 years old (Table 4.1; Figure 4.4).

**Table 4.1: Frequency and percentage age group of respondents**

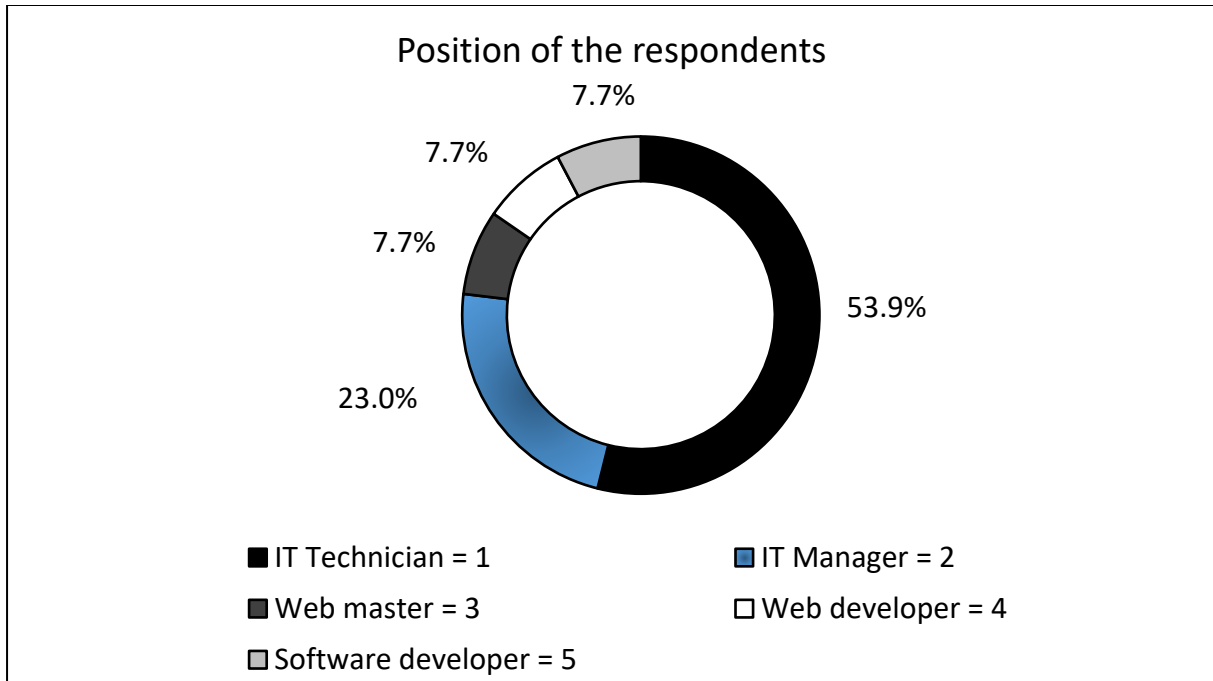
Age group	Frequency	Percentage (%)
20-24	0	0.00
25-29	7	53.85
30-34	5	38.46
35-39	1	7.69
40-44	0	0.00
45-49	0	0.00
50+	0	0.00



**Figure 4.4: Age group of respondents**

### 4.5.3 Position of the respondents

The respondents comprised out of IT Technicians (n = 7), IT managers (n = 3), web masters (n = 1), web developers (n = 1) and software managers (n = 1), corresponding to percentages of 53.4%, 23.0%, 7.7%, 7.7% and 7.7%, respectively (Figure 4.5).



**Figure 4.5: Position of respondents**

#### 4.5.4 Work experience of respondents

Respondents with less than six years' working experience represented a total of 84.7% of the respondents (Table 4.2). The sample did not include any respondents with more than 10 years' experience (Table 4.2).

**Table 4.2: Work experience of respondents**

Work experience	Frequency	Percentage (%)
1-3 years	6	46.2
4-6 years	5	38.5
7-9 years	2	15.4
10-14 years	0	0.0
15-19 years	0	0.0
20+ years	0	0.0

#### 4.5.5 Highest level of completed education

Out of the 13 respondents, 5 had a master's degree (representing 38.5%), followed by respondents who achieved a Diploma (4) and Degree (4) level (both representing 30.8%), while none of the respondents had attained a PhD (Figure 4.6).

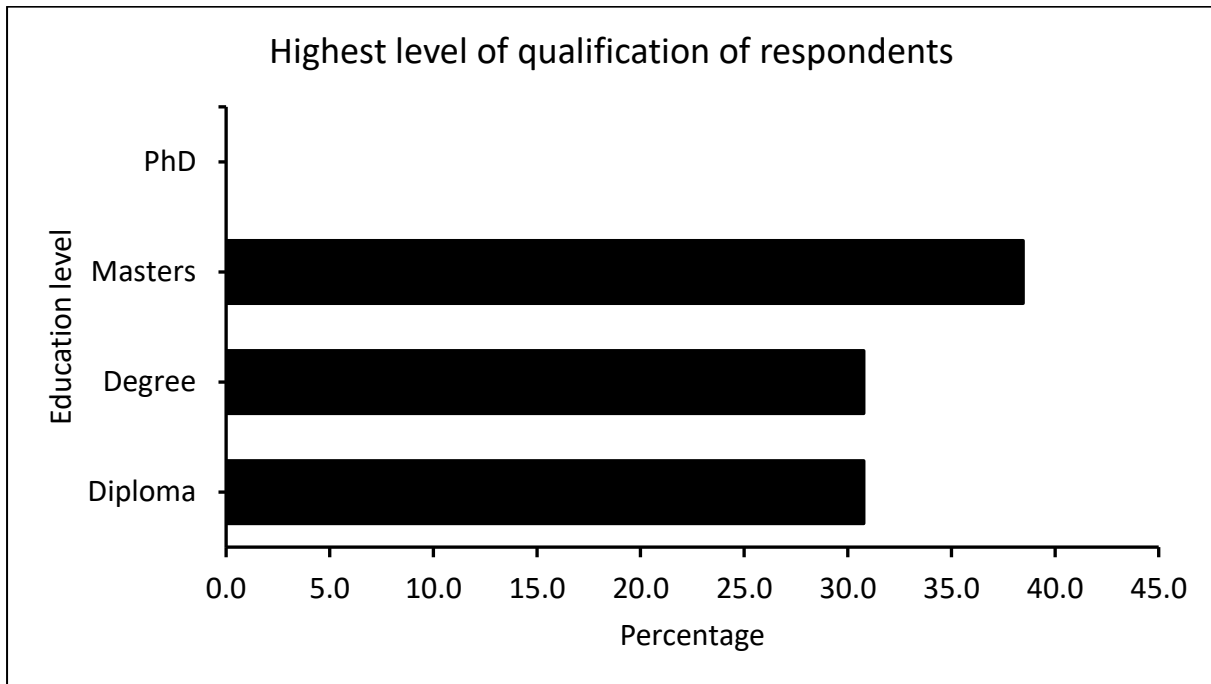


Figure 4.6: Highest level of qualification of respondents

#### 4.6 Section B results

##### 4.6.1 Information management security issues faced by SMMEs

From the respondents, it seems the main issue faced by SMMEs is their inability to acquire funding and resources to invest in information management security. This was mentioned by most respondents (respondent 4, 6, 7, 9, 11, 12, 13) and as explained by respondent as follows: "The SMMEs are faced with a lot of challenges when it comes to Information security as they do not have enough resources to mitigate all the possible risks in advance, they end up being victims of cyber-attacks". This was supported by respondent 7 who gave a similar response namely: "Budget constraints, limited



resources, and limited information expertise make it more probably difficult for SMMEs to achieve an adequate level of information security”.

The lack of resources is causing SMMEs to purchase third-party insurance which has security measures in place to counter information security threats. Respondent 12 stated that “ SMMEs are failing to get 3<sup>rd</sup> parties that they do business with which have security measures in place that they are in line with their information security requirements resulting in the risk of breaches or incurring expenses that could have been avoided”.

#### 4.6.2 SMMEs with information security policies

While the lack of resources affects the implementation of information security in SMMEs as described in the previous sub-section (4.3.1), 92% of the SMMEs have information security policies in place (Figure 4.7).

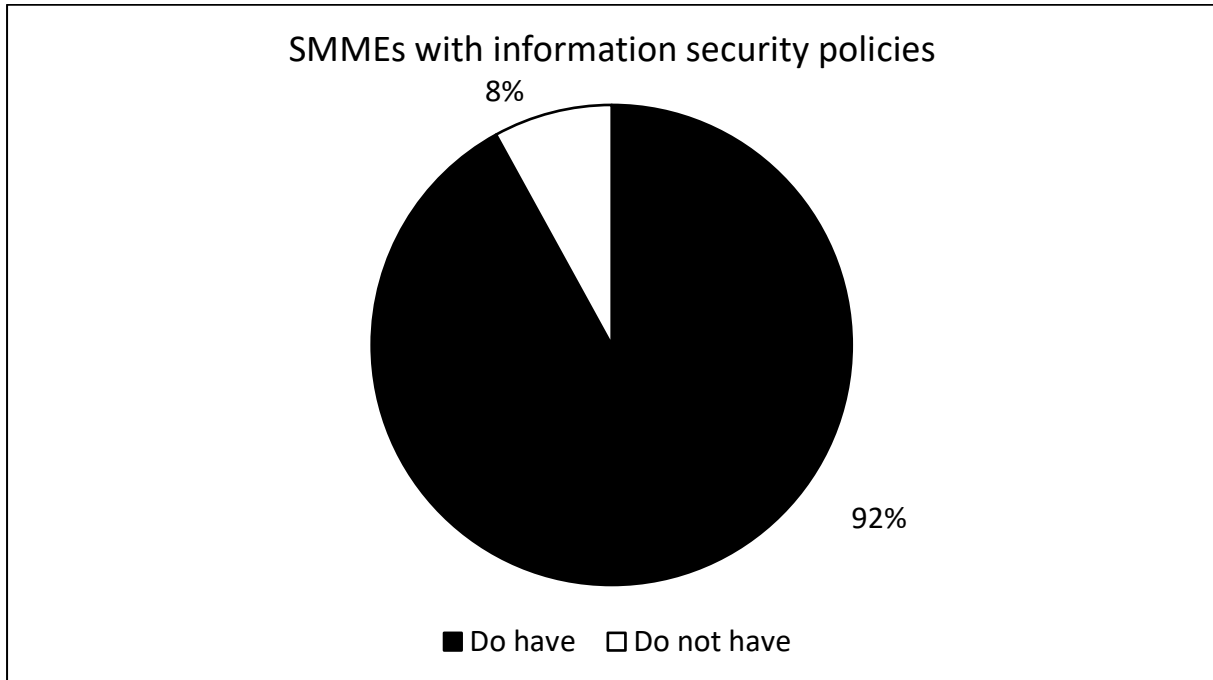


Figure 4.7: SMMEs with information security policies

On this question, only two respondents explained their responses as follow: Respondent

5 said “Yes, it does. For example, acceptable use policy, access control, cryptography and privilege access policy. Respondent 13 stated that “Yes, but it is not in detail as it more focuses on IT equipment usage”. 92%, of the respondents also highlighted that the present information security policies for SMMEs are conveyed to the employees. Most respondents, however, mentioned that these information security policies are only conveyed to employees upon joining the company. Respondent 2 said “Yes but only when they joined the company“. Respondent 5 stated that “Yes they are. When an employee is on board as part of annual compliance trainings”. Respondent 7 mentioned that “they periodically receive security training to keep employees abreast of emerging security threats”.

**4.6.3 Frequency of review of information security policy by SMMEs**

For this question, 50% of the respondents highlight that information security policies are reviewed every year (Figure 4.8). 34% of the respondents were not sure about the frequency of review of information and the responses “twice a year” and “when there is new information” both had 8% (Figure 4.8).

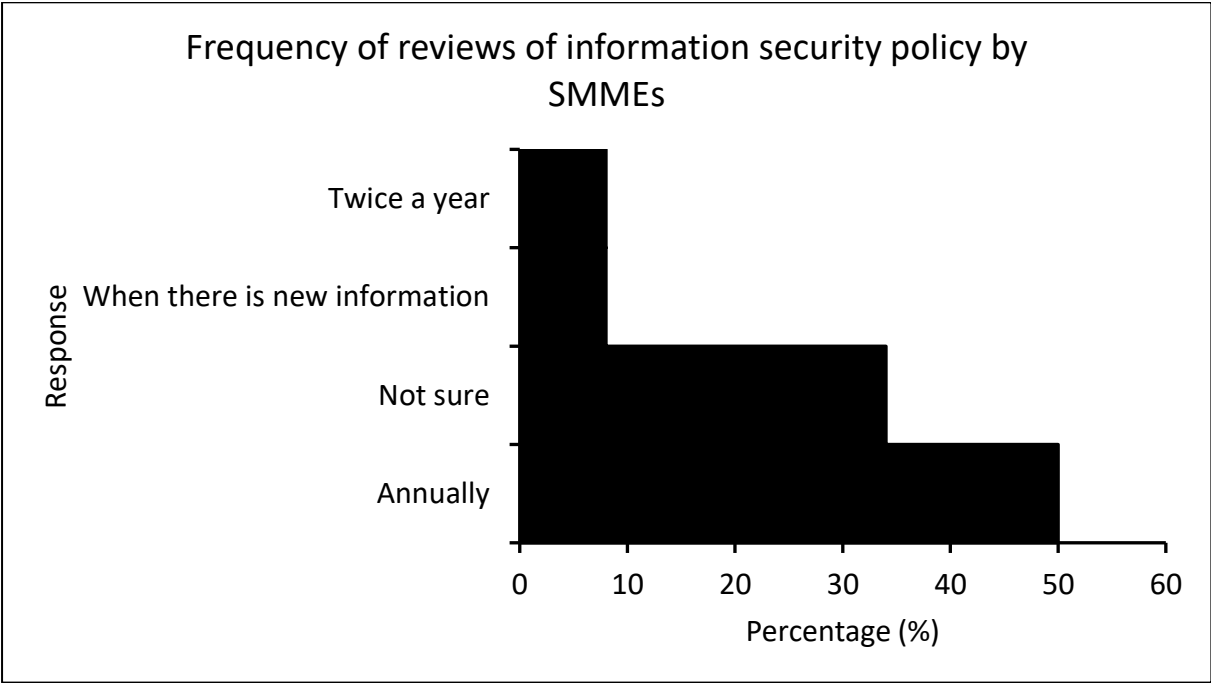


Figure 4.8: Frequency of reviews of information security policy by SMMEs

#### 4.6.4 SMME designation for information security management

91% of the respondents highlight that the SMMEs for which they work have a designated department and budget for information security management and 9% highlighted that the SMMEs that they work for does not have a designated department and budget for information security management (Figure 4.9).

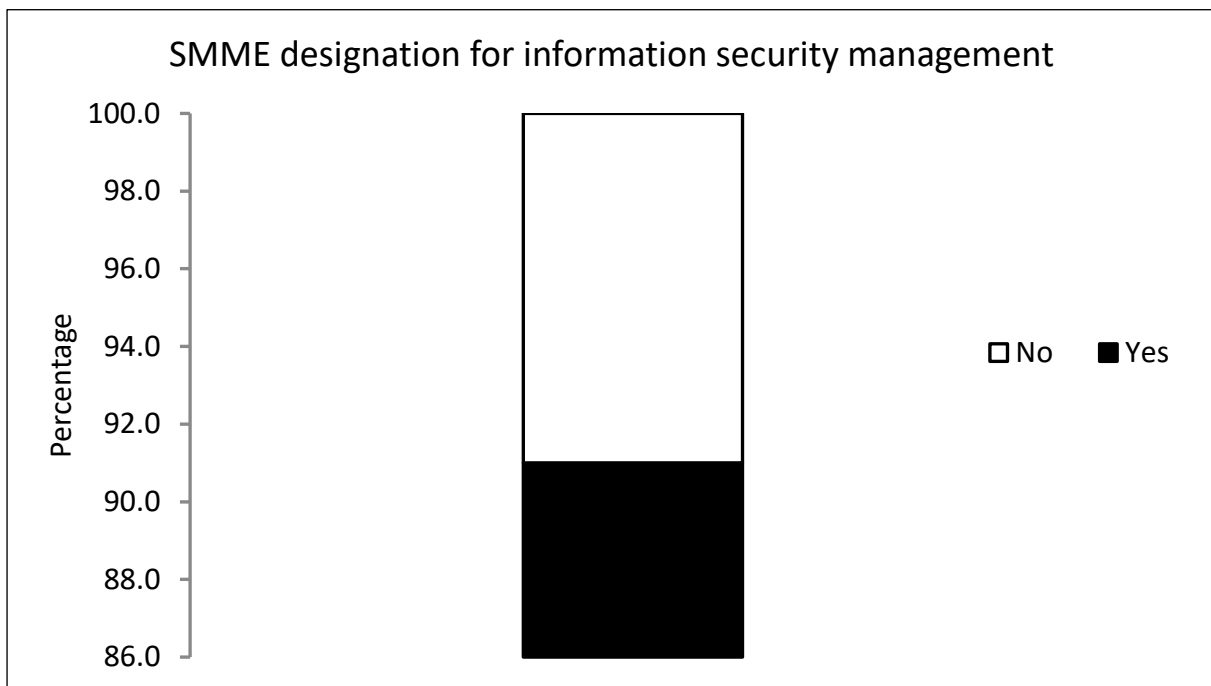


Figure 4.9: SMME designation for information security management

Four respondents confirmed that SMMEs have an IT department that handles the information security management, although full implementation is hampered by lack of resources. Respondent 5 mentioned that “Yes, it does. The information security and governance, risk and compliance team”. Respondent 7 also indicated that Yes, we have ICT and GRC departments sharing that responsibility.” Respondent 13 said that they do not have a specialised department as stated that “We do not have a designated department, only one IT department in my car, and it covers everything. There is an

allocated budget for this but only for antivirus software”.

#### 4.6.5 Risk assessment of the SMMEs when interacting with outside individuals

Risk assessments are conducted to minimise information security breaches, as highlighted by one respondent. From this study, 77% of the respondents confirmed that their SMME does a risk assessment when interacting with individuals outside of their business (Figure 4.10). This helps reduce information security threats as they engage or deal with people who are trustworthy as far as the business is concerned. Only 23% of the respondents confirmed that they do not necessarily do a risk assessment. One respondent (7) further explained that “risk assessments are conducted to minimise information security breaches”

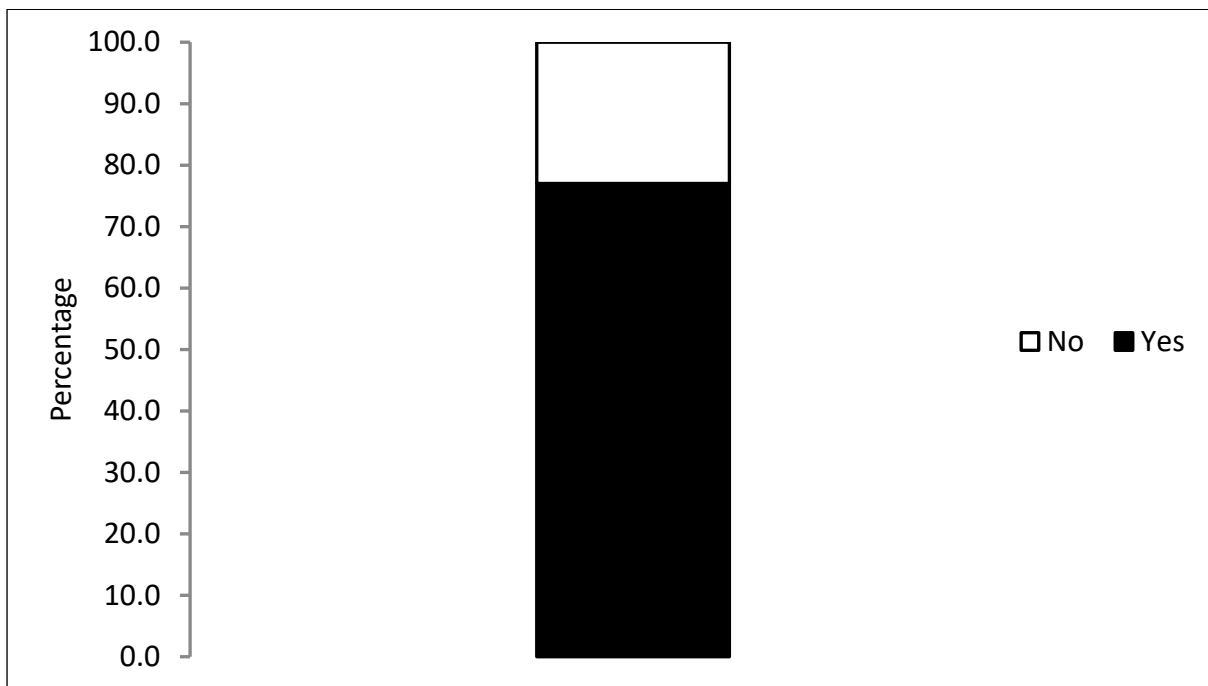


Figure 4.10: Risk assessment of SMMEs when interacting with individuals outside the organisation

92% respondents confirmed that they signed a non-disclosure agreement for their SMME.

Respondents specifically mentioned that signing a non-disclosure agreement is the only way to move forward and said that “it has to be signed and agreed before moving forward“. One respondent (1) admitted that it was not a requirement to sign the agreement for the SMME.

#### 4.6.6 Measures and controls in place when dealing with customers

From this study, all respondents described the various measures in place when dealing with customers to protect the SMME and customers from cyber threats. Most respondents explained how installing anti-viruses on company laptops and computers manages their information security. The responses from the respondents are summarised in Table 4.3.

**Table 4.3: Measures in place when dealing with customers**

<b>Respondent</b>	<b>Answer</b>
1	Encryption where needed on emails
2	Cloud firewalls put in place and antivirus installed in the machines
3	Vetting of customers if they are to access our information
4	Gate keeping and access control is taken seriously; every visitor signs a registry
5	Encryption where needed to access control and privacy policies
6	Security awareness training more often to keep staff updated with security trends
7	Control data & system access, strong passwords, two-factor authentication, monitor intrusion
8	Trainings are conducted once a month to minimise organisation risk to human error
9	Regular training to alert staff about the new threats targeted at them
10	Vetting of customers if they are to access our information
11	Cyber security training and user awareness conducted twice a year
12	No USB allowed; antivirus installed on company laptops; VPN available for employees machines

#### 4.7 Section C results

In this section, respondents were asked to answer either 'Yes' or 'No' for the four questions as described in Figure 4.11.

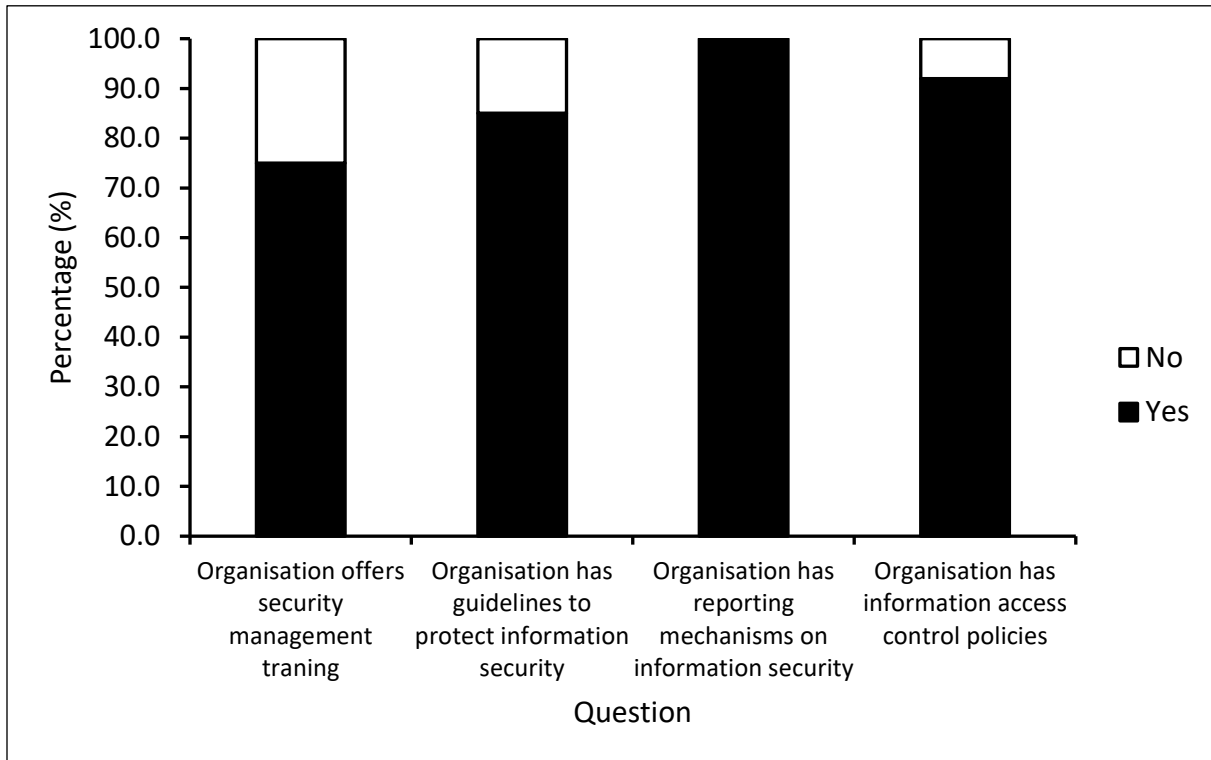


Figure 4.11: Summary of responses from Section C

From Figure 4.11, 75% of the respondents highlighted that their organisation offers security management training. The remaining 25% highlighted that their organisation do not offer security management training. Most respondents (85%) were aware of the organisational guidelines to protect intellectual property right (IPR) whilst 15% of the respondents were not aware of the organisational guidelines to protect IPR. All the respondents confirmed that their organisations have a reporting mechanism for information security incidents and 92% of the respondents confirmed that their organisations had information access control policies (Figure 4.9).

#### 4.7.1 Other security issues

Respondents were asked whether there were any other issues they wanted to raise. Only 31% of the respondents completed this section with additional information they wanted to give. The information was primarily directed towards issues that have to do with how SMMEs can protect themselves from security threats. The responses from the four respondents who made up the 31% are presented in Table 4.4.

**Table 4.4: Summary of other issues raised during questionnaire administration**

Respondent	Answer
2	When dealing with information security, you must always be updated about emerging security threats, vulnerabilities, controls and security topics. Information security awareness trainings must be conducted to keep employees updated and aware of emerging threats and possible attacks, and how they can protect themselves from being victimised.
5	Acknowledgement of policies failure of organisations to provide training and awareness around cyber security as this closely links with information security. Top management involvement in securing that information security controls are in place. Lack of internal audits that tests ISMS
7	When dealing with information security, an SMME must always be updated about any emerging security threats
13	When dealing with information security, an SMME must always be updated about any emerging security threats

## **4.8 Summary**

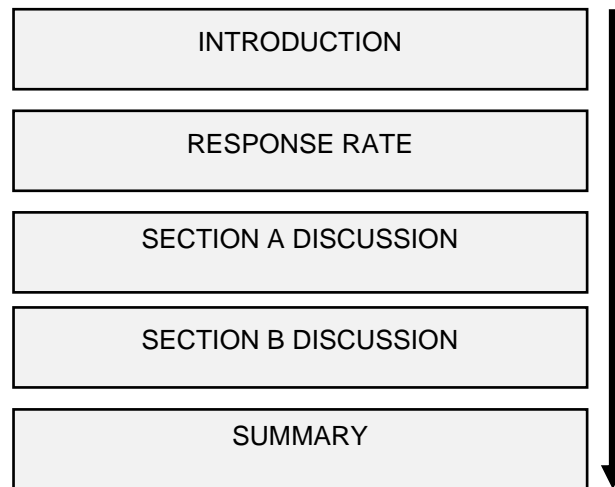
The chapter presented the research findings, discussing each response from the questionnaires. The findings illustrate that the majority of SMMEs are unable to implement information security management frameworks due to a lack of resources. An absence of information security management policies negatively impacts the performance of SMMEs as they are prone to cyber-attack and security breaches. Availability of an information security framework within the SMMEs will have the potential to improve accountability and performance. The next chapter will present the discussion of the research findings.



## CHAPTER 5

### DISCUSSION

The layout of Chapter 5 is illustrated in Fig. 5.1 below.



**Figure 5.1: Layout of Chapter 5**

#### 5.1 Introduction

The previous chapter presented the research findings under the three themes that were identified from the data and provided the discussion of the main findings and in relation to other situations and studies. The aim of this study was to evaluate the information security aspects and how they can be included in the information security management framework for SMMEs in Cape Town. Questionnaires were used as the data collection tool for this study and the previous chapter presented the research findings from this study. This chapter provides a discussion based on the research findings presented in Chapter 4.

#### 5.2 Response rate

Researches that use questionnaires have been popular in information systems for several reasons that include: the ease of questionnaire administration; how efficient they are in

gathering large amount of data at a low cost; how questionnaire respondents feel more comfortable in providing private or sensitive answers rather than when being interviewed face-to-face or by phone (Lindemann, 2021), and hence its adoption in this study. Recent studies have shown that surveys with a low response rate such as near 20% had more accurate results as compared to surveys with a high response rate such as between 60 - 70%. Nevertheless, despite these recent findings, a higher response rate of >80% from a small sample is preferable to a low response rate from a large sample (Lindemann, 2021). The response rate from this study as presented in Chapter 4 was high (87%). With this small sample a high response rate is essential in order to make some albeit low generalisation (Saunders et al., 2018). High response rates should be the goal of researchers and certainly is the standard expectation of editors of academic journals.

### **5.3 Discussion based on Section A**

#### **5.3.1 Gender**

The respondents were slightly biased towards females as females (7) were slightly more than males (6). Many factors contribute to gender inequality globally and gender bias in workplaces play an important role (Martínez et al., 2021:1). Due to well-known cognitive biases, many people often reach erroneous conclusions and develop stereotypes and prejudices. For example, in job applications, female applicants are assumed to be less likely to be committed, less self-confident and less likely to remain on a job than male applicants (Heilman, 2012). The International Labour Organisation indeed recognises gender bias as one of the leading causes of discrimination in hiring and promoting workers with the same qualifications and merits. The fact that a significant proportion of females is represented in the sample according to results from this study means that gender inequality is being addressed to some extent in this sector. However, these results cannot be generalised because this was a sample taken in Cape Town and specifically from the tourism sector. Gender inequalities could be characteristic of other sectors, or other regions, in South Africa.

### **5.3.2 Age group**

In this study, the age modal group was 25-29 years which comprised 70% of the respondents. Employing young people can bring all sorts of benefits to SMMEs, including growing their own workforce, increased competitiveness, a youthful employer brand and meeting the skills gaps (CIPD, 2015). As an SMME working innovatively, staying one step ahead of the business and competition is vital for success. Human resources will be conducting the business and therefore, recruiting and retaining the right talent is imperative. Finding employees with the right skills, expertise and attitudes can be a challenge with often limited material and financial resources. Bringing in youthful employees provides the solution, as they have much to offer SMMEs looking to grow and develop (CIPD, 2015). SMMEs are seen as a vital part of economies, contributing to youth employment and national development (Rotar et al., 2019).

### **5.3.3 Work experience**

Respondents with less < 6 years working experience represented a majority percentage of the respondents (84.7%). Interesting to note, is the absence of respondents that had more than 10 years' experience. SMMEs typically employ young people with less experience as compared to their bigger business counterparts who often require more substantive years of experience. This explains the fewer than six years' work experience of the majority of respondents. When these employees gain some experience, they are likely to be employed by the bigger companies which might explain why none of the respondents had more than 10 years' work. This could also be a result of the age of the SMME which could have been established not more than 10 years ago. All this however, requires further studies to validate these claim, investigating how the SMMEs link with bigger businesses with regards to the labour provision as employees gain experience at SMMEs for future employment in more established big businesses.

### **5.3.4 Highest level of qualification**

Out of the 13 respondents, 5 had a master's degree (representing 38.5%), followed by respondents who achieved a Diploma (4) and Degree (4) level (both representing 30.8%),

while none of the respondents had attained a PhD. This result supports various publications that regard SMMEs as vital sectors providing employment for younger graduates. As explained in section 5.3.3 above, the SMMEs could serve as a platform for youth with degrees and advanced degrees to gain work-related experience at SMMEs to then seek for new challenges in bigger businesses. This again, requires further studies to validate these claims.

## **5.4 Discussion based on Section B**

### **5.4.1 Information management security issues faced by SMMEs**

From this study, it seems the main issue faced by SMMEs is their inability to acquire funding and resources to invest in information management security which was mentioned by most respondents. Businesses of all sizes are continuously under information security threats, whether the company employs 10 or 200 000 employees (Manning, 2017). There is this notion that information security threats are only interested in large businesses, but data gathered in recent years disprove this belief. It seems that the lack of resources also affects the investment in information security management in other countries, as reported by Devlin (2021). SMMEs often have few resources to devote to information security management; in fact, a 2017 study found that 28% of SMMEs cited a lack of resources as the top obstacle to achieving information security management goals (Devlin, 2021). While large businesses often have vast resources to invest in robust information management security measures, SMMEs often lack the budget, and neither do they have the expertise. This can therefore be a daunting task. There are numerous threats to protect against in an SMME, and the cost of implementing robust information management security measures can be prohibitive.

Investing in information security resources will improve business processes or even enable new ones (Abazi, 2017). Information security processes are intended to protect any business and its associated resources because many information security process performances impact the performance of a business. The resource-based view, as a theory, applies in this situation as a firm's resources include all processes, assets,

information and knowledge. Information security is therefore tethered to the resource based-view theory of SMMEs because information security investments are a vital part of general IT investments (Abazi, 2017). SMMEs should invest in information security by applying for funding from the government or private organisations, or they may self-fund as it is predicted that these threats will unfortunately increase in upcoming years as more SMMEs go digital.

#### **5.4.2 SMMEs with information security policies**

While the lack of resources affects the implementation of information security in SMMEs as described in the previous sub-section (5.4.1), most of the SMMEs (92%) have information security policies in place. This is important as criminals are taking advantage of the uncertainty and fear that many citizens are experiencing because of pandemics and other uncertainties (ENISA, 2021). There has been a marked increase in phishing attacks, malicious emails, scams, malware and cyber attacks targeting specific businesses already under strain due to the Covid-19 pandemic. SMMEs have not been left out of these threats as some SMMEs have staff working remotely, and have deployed systems quickly rather than securely for them to continue to serve their customers (ENISA, 2021). In this regard, the findings that most SMMEs in this study have information security policies in place, reduces security concerns.

#### **5.4.3 Frequency of review of information security policy by SMMEs**

In this study, 50% of the respondents highlight that information security policies are reviewed every year, 34% of the respondents were not sure about the frequency of review of information and the responses “twice a year” and “when there is new information” both had 8%. It is important to review the information security policies of SMMEs annually, additional reviews should also be conducted whenever there are changes, amendments or new requirements, as reported by one respondent. This is important as cyber threats are constantly being unleashed by criminals (ENISA, 2021). These cyber threats are growing and predicted to continue to grow in the future as more and more businesses go digital.

Training of staff is also important in SMMEs in a digital world faced with these cyber threats. In this study, most respondents (75%) highlighted that their organisation offers security management training. Employee training is fundamental for employees to remain up to date with the recent security threats and innovative ways that promote the flourishing of SMMEs (European IPR, 2012). Training of employees is a human resource investment and gives the employer a guarantee that employees will be able to handle business secrets. Training on information security also creates a culture of information security within the business and is the most profitable aspect of confidentiality management (European IPR, 2012).

#### **5.4.4 SMME designation for information security management**

Most respondents (91%) highlight that the SMMEs that they work for have a designated department and budget for information security management and 9% highlighted that the SMMEs that they work for does not have a designated department and budget for information security management. It is important to have a separate department that budgets for information security management as itself it requires resources allocated to it so that sound information security management is in place. As an organisation has different departments, it is important to budget and plan well for each department so that all the goals and mandates of the business are fully accomplished.

#### **5.4.5 Risk assessment of the SMMEs when interacting with outside individuals**

Risk assessments are conducted to minimise information security breaches. From this study, most of the respondents (77%) confirmed that their SMME does a risk assessment when interacting with individuals outside of their business. This helps reduce information security threats as they engage or deal with people who are trustworthy as far as the business is concerned.

Security information sharing is a challenge for businesses. In most cases, they are reluctant to share their business information and report their incidents (Shojaifar & Fricker,

2020). This is likely due to fear of competitive disadvantage and negative publicity, believing that cyber threats are not severe enough to be reported, and generally, a lack of motivation and trust. Security information sharing is, however, a significant measure to reduce some risks of similar incidents as well as to develop a better understanding of the risk factors (Shojaifar & Fricker, 2020). Access control is an important security management policy for any business organisation. Sound policies prevent competitors and unauthorised individuals from accessing crucial information that might jeopardise the integrity of the SMME. In this study, 92% of the respondents confirmed that their organisations had information access control policies. Interestingly, all the respondents confirmed that their organisations have a reporting mechanism for information security incidents. This is important as these incidents should be reported and addressed to prevent future incidents. This keeps the business venture efficient in handling and addressing security incidents which would be based on previous encounters.

As information for an SMME is important, a non-disclosure agreement (NDA) should be signed by employees so that information is not lost to competitors and cyber criminals (European IPR, 2012). An NDA within a contract is an obligation of confidence which arises when parties reach an agreement to maintain the confidentiality of business information. The disclosure of business secrets would amount to a breach of confidentiality and therefore, a breach of contract (European IPR, 2012). Secrets in any business are confidential pieces information which provide a business or enterprise with an economic benefit that ultimately translates into competitive advantage (European IPR, 2012). This is derived directly from the fact that a business secret is generally not known to competitors due to the efforts of the SMME owner and employees to retain secrecy. In this sense, the protection of business secrets provides incentive to innovate by safeguarding substantial time, ideas and capital invested in efforts to innovate (European IPR, 2012).

#### **5.4.6 Measures and controls in place when dealing with customers**

As described in the previous sections, it is important for an SMME to have these security

measures in place so as to prevent threats of various levels. From this study, all the respondents described the various measures in place when dealing with customers to protect the SMME and customers from cyber threats. Most respondents explained how installing anti-viruses on company laptops and computers manages their information security. SMMEs face a major challenge in their business environment as they are not familiar with the best ways to manage their knowledge assets (Singh, 2014). SMMEs face different types of intellectual property right (IPR) challenges and need to evolve strategies that suit different conditions to remain competitive in the market (Singh, 2014). In this study, most respondents (85%) were aware of the organisational guidelines to protect IPR.

## **5.5 Summary**

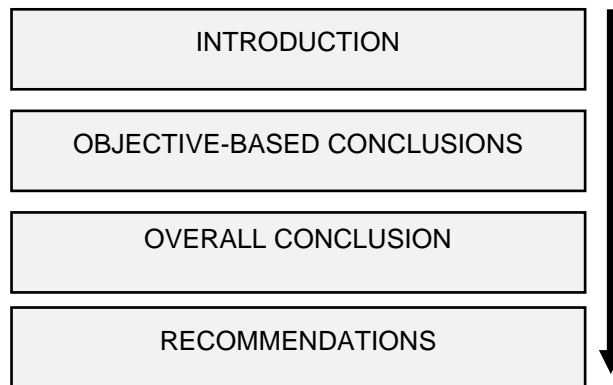
This chapter provided a discussion of the research findings of this study. Discussed in this chapter was issues that have to do with information security management in SMMEs in Cape Town. As highlighted in this chapter, most SMMEs are unable to implement information security management frameworks due to lack of resources. Lack of information security management policies negatively impacts the performance of the SMMEs as they become prone to cyber-attack and security breaches. The next chapter reflects on the research objectives and gives conclusions and recommendations for future studies.



## CHAPTER 6

### CONCLUSION AND RECOMMENDATIONS

The layout of Chapter 6 is illustrated in Fig. 6.1 below.



**Figure 6.1: Layout of Chapter 6**

#### 6.1 Introduction

The aim of this study was to evaluate the information security aspects and how they can be included in the information security management framework for SMMEs in Cape Town. Questionnaires were used as the data collection tool for this study. The response rate from this study was high and the gender of participants was almost balanced. The age modal group was between 25-29 years and most respondents were IT Technicians with less than 6 years working experience. Research findings and discussions presented in the previous chapter highlighted that most SMMEs are unable to implement information security management frameworks due to lack of resources. Lack of information security management policies negatively impacts the performance of the SMMEs as they become prone to cyber-attack and security breaches. This chapter provides a summary of the research findings and offers recommendations and a conclusion to the study. The conclusion will be discussed under the subheadings of the research objectives that were presented in Chapter 1.

## **6.2 Objective-based conclusions**

### **6.2.1 Importance of information security management in SMMEs in Cape Town**

Most SMMEs are aware of the importance of information security management. The importance is reflected in how the SMMEs offer information security management trainings to its employees, provision of guidelines to protect IPR, having reporting mechanisms for information security incidences and having access control policies. Most respondents confirmed that SMMEs had an IT department dedicated to handle cyber threats. SMMEs should generally be prepared to handle threats to their business and critical information through their IT departments and by having the right people and tools placed in the enterprise or business (Abbas et al., 2015). A well prepared SMME would be able to identify any information security breach and would first contain the damage being caused by the information security breach followed by its complete eradication. The recovery process would subsequently be initiated which would close or strengthen the weak links. Lessons learned from the information security breach would assist in fighting future similar breaches (Abbas et al., 2015) and in this study, most respondents highlighted that their organisations provide a platform for them to report security incidences. As described by Abbas et al. (2015), it is indeed these past incidences that help technicians to be well prepared for similar future attacks.

### **6.2.2 Hindrances faced by SMMEs to invest in information security management services**

Information security management is both complex and costly to implement and often requires expertise to manage the process (Ng et al., 2013). Identification of all the information assets in a business requires a dynamic inventory of the assets to be created so as to maintain a competent tracking system. Most SMMEs are not able to invest in information security management services because they do not have enough resources. SMEs form a large percentage of national economies globally and rely on information systems but relatively have fewer resources than their large business counterparts. Lack of funding creates an unfair competition from well established businesses which makes it so difficult for the SMMEs to establish and penetrate into the respective businesses or

markets.

Even when few resources are available, SMMEs generally invest them in establishing and maintaining IT security policies as well as strategies. This deficiency of information security investments and lack of proper information security policies by SMMEs predisposes them an easy target for the cyber criminals. Despite the challenges and threats that SMMEs face, their employment as well as reliance on ICT is rapidly increasing, and their business goals are directly being associated with the utilisation of ICT.

### **6.2.3 Information security policies in place for SMMEs in Cape Town**

The respondents from Cape Town SMMEs confirmed that their organisations have information security policies that are in place in their organisation. These are mostly reviewed annually in order to update the employees on the information security threats and related stuff that all have a resultant of protecting the integrity of the SMME. The implementation of information security policies is however complicated, costly and will not deliver immediate results. Prioritisation of information security policies could be low in SMMEs as business productivity could be highly prioritised than information security (Ng et al., 2013). Further, some SMMEs often believe that backing up their information and data is sufficient protection against most information security risks which is clearly a dangerous misperception, as most of the risks such as those that attack services may not be solved or addressed by backups (Ng et al., 2013).

Information security policies, strategies and plan outshines an SMME amongst its competitors and would obviously be chosen by customers to. Information security management will therefore, not only assist the SMMEs in having better and secure IT structures, it will yield in customer satisfaction as well as a good reputation which in turn will attract more business and maximise profits.

### **6.3 Overall conclusion**

The study revealed that the majority of SMMEs lacked investment into information security systems and as a result, they are prone to information security breaches. The study revealed that the SMMEs had measures aimed at reducing and mitigating against information security and these measures were part of the culture of such organisations and were not necessarily established by technical means. Information security management framework is aimed at achieving three key objectives which are technical countermeasures, policies, and programs.

The adoption of information security management frameworks by SMMEs is considered to provide them with strategic support that can enhance their operations and competitiveness. The business operating environment has largely evolved into digital with an increased use of electronic data interchange and electronic business and these require the SMMEs to improve their information security management to avoid being manipulated. The usage of the internet and online banking, shopping and other new technological innovations are allowing the SMMEs to connect with similar enterprises and also with large business entities and there is need to make use of firewalls and security control mechanism to control the organisational data from manipulation.

The study established that information security management issues were not being adequately dealt with within SMMEs with some of them having no information security policies that provide roadmap on the management of information. The general feeling within the majority of the SMEs was that information security was not a critical business area hence the organisations took a pedestrian approach. The management of SMMEs are aware of the security concerns and the need for adequate information security management framework though this awareness is displayed in a superficial manner like having a security policy stashed in the office and not implemented or educating the employees about such policies. The strategies used in dealing with viruses and other security intervention strategies amongst the SMMEs are largely ad-hoc and unplanned. The SMMEs management should invest in firewalls and training their employees on

utilising passwords and personal security measures on their gadgets to minimise the risk of security threats. Security standards must be adopted by the SMMEs to ensure information security are formalised within the organisations.

#### **6.4 Recommendations**

When one wants to start a digital transformation process for SMMEs, considering corporate cyber security as an element to invest in is crucial. This kind of investment often may seem superfluous, but protecting one's SMME and customers' data and information is necessary to avoid incurring huge costs in case of vulnerability. Ensuring absolute security also has great benefits for the perception of an SMME by customers. The SMMEs should consider developing succinct information security documents that captures critical issues such as acceptable usage of the information systems, backups, data and information security, employee training and education on information security and the protection of organisational assets. Through having documented policies on information security and processes the organisations will no-longer continue taking information security for granted but will revise and formalise their approach. The information security policies should not be imposed on the employees but rather they should be actively involved such that they are able to develop a buy-in to the security policies. As noted by Chidende (2018) SMMEs cannot claim that they have no access to knowledgeable employees due to their resources constraints because information on development of information security policies for SMMEs is easily accessible online and some free websites are dedicated to provide guidance and explanations in this regard and one such website is the Joint information systems committee.

The SMMEs do not need to assume that their external service provider are infallible with regard to information manipulation/hacking, prevention of virus and information theft hence they should be continuous questioning of the security systems and promote the usage of firewalls between the organisation and any external service provider and public network. Data backups are essential for the SMMEs as they provide the last solution when all other alternatives have failed hence the organisation should invest in data

backups. Another security measure that SMMEs should adopt is the use of a file saver operating system that offers a centralised user accounts that has policy controls and password management. The systems are no-longer complex and the internet has simplified templates that SMMEs can make use of. The use of wire walls and antivirus within the operations of SMMEs is non-negotiable as they provide essential protection for the organisation from manipulation.

The majority of the participants who are responsible for information security within their organisations indicated that they showed no consideration to social psychology during everyday management of risk. The security controls adopted by the organisations are only selected not because of their effectiveness but because of their costs. The challenge brought by this approach as alluded to by the participants is that the SMMEs adopted cheaper control access measures which did not protect the organisation from the potential risks. This view is shared by Julish (2013) who stated that through adopting weaker control access security measures the management negatively affected the attitude of the employees towards information security management which is then considered a less influential component in the management of the organisation.

When the person responsible for the management of information security does not consider issues with regard to employee perception into consideration this had a net impact of having inadequate control over information security because they are prone to over-estimate or underestimate the security risks. The study revealed that the SMMEs remain guilty of exhibiting this negative perception towards information security and this mentality was shared throughout the organisation. The study also revealed that internal threats to information security within the organisation did not result from malicious intent from the employees but was mostly a result of employee carelessness, ignorance or errors. The SMMEs should also invest in periodic training and educating their employee's mainly on issues of information security to avoid internal threats. SMMEs must develop policies that document measures to control information from being breached and these policies must be made aware to the employees.

Many business owners might not be aware of any funding opportunities for their SMMEs. Lack of funding was cited as the major issue that affects SMMEs from investing in information security management. This study therefore recommends the SMME owners to check the government website “<https://www.gov.za/about-government/small-business-development>” which has a list of funds that they can apply for. While the study has certainly made valuable contributions to the field of information security and SMMEs, there is scope for further enhancement.

### **6.5 Limitations and future research**

This study only focused on one SMME sector which is the tourism sector, let alone the focus on one province, Cape Town. Findings cannot be generalised to other SMMEs in South Africa. However, even though the results might not be generalised to other provinces, the study will still have relevance in terms of informing on the problems faced by SMMEs in South Africa to improve the country’s economy. For future research, a broader range of SMMEs may be considered so as to determine how they are being affected by security issues. Further studies could also explore SMMEs in different provinces so as to determine how geographical location affects security issues in SMMEs.

## REFERENCES

- Abazi, B. 2017. An approach to Information Security for SMEs based on the Resource-Based View theory. *International Conference on Information Systems and Security*: pp. 1-3.
- Abbas, J., Mahmood, H.K., & Hussain, F. 2015. Information security management for small and medium size. *Science International*, 27(3), pp. 2393-2398.
- Abdallah, N. & Abdullah, O.2019. Computer security behavior and awareness: An empirical case study. *International Journal on Perceptive and Cognitive Computing*, 5(1), pp. 8-14.
- Abel, J.P., Buff, C.L., & Burr, S.A.2016. Social media and the fear of missing out: Scale development and assessment. *Journal of Business & Economics Research (JBER)*, 14(1), pp. 33-44.
- Abidoeye, A.P., & Obagbuwa, I.C. 2017. DDoS attacks in WSNs: detection and countermeasures. *IET Wireless Sensor Systems*, 8(2), pp. 52-59.
- Abrahamsson, M., & Tehler, H. 2013. Evaluating risk and vulnerability assessments: A study of the regional level in Sweden. *International Journal of Emergency Management*, 9(1), pp. 76-92.
- Accenture. 2019. *2017 Cost of Cyber Crime Study* | Accenture. Available from: <https://www.accenture.com/us-en/insight-cost-of-cybercrime-2017>(Accessed 17/09/2022).
- Adams, J., Khan, H., & Raeside, R. 2014. *Research Methods for Business and Social Science Students* 2<sup>nd</sup> ed., London: Sage Publishers, pp. 271.



Adhabi, E.A.R., & Anozie, C.B. 2017. Literature review for the type of interview in qualitative research. *International Journal of Education*, 9(3), pp. 86-97.

Adomako, S., & Ahsan, M. 2022. Entrepreneurial passion and SMEs' performance: Moderating effects of financial resource availability and resource flexibility. *Journal of Business Research*, 144, pp. 122-135.

AGSA. 2017. *Information technology controls*. Available from: <https://www.agsa.co.za/Portals/0/Reports/PFMA/201617/GR/12%20information%20technology%20controls.pdf> (Accessed 17/09/2022).

Åhlfeldt, R.M., Nohlberg, M., Söderström, E., Lennerholt, C., & van Laere, J. 2018. Current Situation Analysis of Information Security Level in Municipalities. *Journal of Information System Security*, 14(1), pp. 3-19.

Ahmad, M. 2018. Review of the Technology Acceptance Model (TAM) in internet banking and mobile banking. *International Journal of Information Communication Technology and Digital Convergence*, 3(1), pp.23-41.

Al-Dhahri, S., Al-Sarti, M., & Aziz, A.A. 2017. Information security management system. *International Journal of Computer Applications*, 158(7), pp.29-33.

Aldya, A.P., Sutikno, S., & Rosmansyah, Y. 2019. Measuring effectiveness of control of information security management system based on SNI ISO/IEC 27004: 2013 standard. *In IOP Conference Series: Materials Science and Engineering*, 550(1), pp. 1-12.

Akhyari, N., Ruzaini, A.A., & Rashid, A.H. 2018. Information security culture guidelines to improve employee's security behavior: a review of empirical studies. *Journal of Fundamental and Applied Sciences*, 10(2S), pp. 258-283.

Akinrolabu, O., Nurse, J.R.C., Martin, A., & New, S. 2019. Cyber risk assessment in cloud

provider environments: Current models and future needs. *Computers & Security*, 87(101600), pp. 1-20.

Alanen, J., Linnosmaa, J., Malm, T., Papakonstantinou, N., Ahonen, T., Heikkilä, E., & Tiusanen, R. 2022. Hybrid ontology for safety, security, and dependability risk assessments and Security Threat Analysis (STA) method for industrial control systems. *Reliability Engineering & System Safety*, 220(108270), pp. 1-20.

Alshare, K., Lane, P.L., & Lane, M.R. 2018. Information security policy compliance: a higher education case study. *Information and Computer Security*, 26(1), pp. 91-108.

Allen, M. 2017. *The SAGE encyclopedia of communication research methods* (Vols. 1-4). Thousand Oaks, CA: SAGE Publications, Inc.

Alhassan, M.M., & Adjei-Quaye, A. 2017. Information Security in an Organization. *International Journal of Computer (IJC)*, 24(1), pp. 100-116.

Amraoui, S., Elmaallam, M., Bensaid, H., & Kriouile, A. 2019. Information systems risk management: Literature Review. *Computer and Information Science*, 12(3), pp. 1-20.

Anderson, B., Vance, A., Kirwan, C.B., Eargle, D., & Jenkins, J.L. 2016. How users perceive and respond to security messages: a NeuroIS research agenda and empirical study. *European Journal of Information Systems*, 25(4), pp. 364-390.

Asenahabi, B.M. 2018. Basics of research design: A guide to selecting appropriate research design. *International Journal of Contemporary Applied Researches*, 6(5), pp. 76-89.

Asgari, H., Haines, S., & Rysavy, O. 2017. Identification of threats and security risk assessments for recursive internet architecture. *IEEE Systems Journal*, 12, pp. 2437-2448.

Awuzie, B., & McDermott, P. 2017. An abductive approach to qualitative built environment research: A viable system methodological exposé. *Qualitative Research Journal*, 17(4), pp. 356-372.

Balozian, P & Leidner, D. 2017. Review of IS security policy compliance: Toward the building blocks of an IS asecurity theory. *Data Base for Advances in Information Systems*, 48(3), pp. 11-43.

Barnes, J., & Sanger, D. 2020. *U.S. Accuses Russian Military Hackers of Attack on Email Servers*. Available from: <https://www.nytimes.com/2020/05/28/us/politics/nsa-russian-hack.html> (Accessed 17/09/2022).

Barrett, D. 2017. *Websites of Ohio governor, Maryland county hacked with pro-Islamic state messages*. Available from: <https://www.latimes.com/nation/ct-ohio-government-websites-hacked-islamic-state-20170625-story.html>(Accessed 17/09/2022).

Barzak, O., Molok, N.N.A., Mahmud, M., & Talib, S. 2019. Incorporating Islamic principles in information security behaviour: a conceptual framework. *Journal of Information Systems and Digital Technologies*, 1(2), pp. 24-39.

Baskerville, R. 2018. *Information security: Going digital*. Proceedings of 47<sup>th</sup> Annual Conference of the South African Computer Lecturers' Association SACLA 2018, 18-20 June, Gordon's Bay South Africa.

Bauer, S., & Bernroider, E.W. 2017. From information security awareness to reasoned compliant action: analysing information security policy compliance in a large banking organization. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, 48(3), pp. 44-68.

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

887-901.

Bernstein, J., & Szuster, B.W. 2019. The new environmental paradigm scale: Reassessing the operationalization of contemporary environmentalism. *The Journal of Environmental Education*, 50(2), pp. 73-83.

Besser, L., Sturmer, J., & Sveen, B. 2016. *Chinese hackers behind Defence, Austrade security breaches*. Available from: <https://www.abc.net.au/news/2016-08-29/chinese-hackers-behind-defence-austrade-security-breaches/7790166> (Accessed 17/09/2022).

Bey, M. 2018. Great powers in cyberspace: The Strategic Drivers Behind US, Chinese and Russian Competition. *The Cyber Defense Review*, 3(3), pp. 31-36.

Bhorat, H., Buthelezi, M., Chipkin, I., Duma, S., Mondi, L., Peter, C., Qobo, M., Swilling, M., & Friedenstein, H. 2017. *Betrayal of the promise: How South Africa is being stolen, State Capacity Research Project*. Available from: <http://pari.org.za/wp-content/uploads/2017/05/Betrayal-of-the-Promise-25052017.pdf> (Accessed 24/10/2022).

Bland, J.A., Petty, M.D., Whitaker, T.S., Maxwell, K.P., & Cantrell, W.A. 2020. Machine Learning Cyberattack and Defense Strategies. *Computers & Security*, 92(101738), pp. 1-16.

Blišťanová, M., Tirpáková, M., & Galanda, J. 2022. Proposal of risk identification methodology using the prompt list on the example of an air carrier. *Sustainability*, 14(9225), pp. 1-20.

Borgstede, M., & Scholz, M. 2021. Quantitative and qualitative approaches to generalization and replication - A representationalist view. *Frontiers in psychology*, 12(605191), pp. 1-9.

Bradshaw, C., Atkinson, S., & Doody, O. 2017. Employing a Qualitative Description

Approach in Health Care Research. *Global Qualitative Nursing Research*, 4, pp. 1-8.

Brewerton, A. 2013. *Why SMEs should back up their data to the cloud*. Available from: <https://www.theguardian.com/small-business-network/2013/mar/11/back-data-to-cloud-small-business> (Accessed 24/10/2022).

Bruwer, J. 2020. Fortifying South African Small Medium and Micro Enterprise sustainability through a proposed internal control framework: The Sustenance Framework. *Expert Journal of Business and Management*, 8(2), pp. 147-158.

Bureau for Economic Research. 2016. *The small, medium and micro enterprise sector of South Africa*. Research Note 2016: No 1. Commissioned by the Small Enterprise Development Agency (SEDA).

Bushe, B. 2019. The causes and impact of business failure among Small to Micro and Medium Enterprises in South Africa. *Africa's Public Service Delivery and Performance Review*, 7, pp. 2310-2195.

Bvuma, S., & Marnewick, C. 2020. Sustainable livelihoods of township small, medium and micro enterprises towards growth and development. *Sustainability*, 12(8), pp. 3149-78.

Chandra, N.A, Kalamullah R., Ratna, A.A.P., & Gunawan, T.S. 2022. Information security risk assessment using situational awareness frameworks and application tools. *Risks*, 10(165), pp. 1-26.

Charmaz, K. 2015. Qualitative psychology: A Practical Guide to research Methods. In: K. Charmaz, J.A. Smith (eds). *Grounded Theory*. Sage Publications LTD, pp. 60-64.

Chimucheka, T., & Mandipaka, F. 2015. Challenges faced by small, medium and micro enterprises in the Nkonkobe municipality. *International Business and Economics Research Journal*, 14(2), pp. 309-316.

Chmura, J. 2017. Forming the awareness of employees in the field of information security. *Journal of Positive Management*, 8(1), pp.78-85.

Cindana, A., & Ruldeviyani, Y.2018. *Measuring information security awareness on employee using HAIS-Q: Case Study at XYZ Firm*. In 2018 International Conference on Advanced Computer Science and Information Systems (ICACSIS), pp. 289-294.

CIPD. 2015. *Employing young people A step-by-step guide for SMEs*. Available from: [https://www.cipd.co.uk/Images/employing-young-people-sme.guide\\_2015\\_tcm18-10262.pdf](https://www.cipd.co.uk/Images/employing-young-people-sme.guide_2015_tcm18-10262.pdf) (Accessed 24/09/2022).

Cleary, M., Horsfall, J., & Hayter, M. 2014. Data collection and sampling in qualitative research: does size matter? *Journal of Advanced Nursing*, 70(3), pp. 473-475.

Couce-Vieira, A., Insua, D.R., & Kosgodagan, A. 2020. Assessing and Forecasting Cybersecurity Impacts. *Decision Analysis*, 17(4), pp. 356-374.

Covert, Q., Steinhagen, D., Francis, M., Streff, K. 2020. Towards a triad for data privacy. *Hawaii International Conference on System Sciences*, pp. 4379-4387.

Creswell, J.W. 2014. *Research design qualitative, quantitative, and mixed methods approaches* 4<sup>th</sup>edition. Thousand Oaks, CA: SAGE Publications, pp. 304.

Creswell, J.W., & Creswell, J.D. 2018. *Research design: qualitative, quantitative, and mixed methods approaches* 5<sup>th</sup> edition. Los Angeles: SAGE Publications.

Cuganesan, S., Steele, C., & Hart, A. 2018. How senior management and workplace norms influence information security attitudes and self-efficacy. *Behaviour & Information Technology*, 37(1), pp. 50-65.

deArroyabe, F.I., & de Arroyabe, J.C. 2021. The severity and effects of Cyber-breaches in SMEs: a machine learning approach. *Enterprise Information Systems*, pp. 1-27.

Deloitte IAS Plus. 2020. *UK Corporate Governance Code*. Available from: <https://www.iasplus.com/en-gb/standards/corporate-governance/uk-corporate-governance-code> (Accessed 24/10/2022).

Department of Trade and Industry, DTI. 2009-2019. *The national youth economic empowerment strategy and implementation framework*. Mainstreaming Youth in the South African Economy 2009 – 2019. Available from: <https://static.pmg.org.za/docs/090901nyees.pdf> (Accessed 10/10/2022).

Devlin, C. (2021). *Small- and medium-sized businesses are vulnerable to cybercrime. Cincinnati*. Available from: <https://www.uc.edu/news/articles/2021/10/gc-small-and-medium-sized-businesses-are-vulnerable-to-cybercrime.html> (Accessed 24/10/2022).

Dhillon, G., Syed, R., & Pedron, C.D. 2016. Interpreting information security culture: An organizational transformation case study. *Computer Security*, 56, pp. 63-69.

Dhillon, G. 2018. *Information Security: Text & Case*. 2nd Edition. Prospect Press.

Dlamini, S., Mbambo, C. & Ma, W.W.I. 2019. Understanding policing of cyber-crime in South Africa: The phenomena, challenges and effective responses. *Cogent Social Sciences*, 5(1), pp.1-14.

Dorian, L. 2012. *Risk Management: Understanding industry insights*. Available online: <http://www.ica.bc.ca/ii/ii.php?catid=17> (Accessed 06/11/2022).

Döringer, S. 2021. The problem-centred expert interview. Combining qualitative interviewing approaches for investigating implicit expert knowledge. *International Journal of Social Research Methodology*, 24(3), pp. 265-278.

Doyle, L., McCabe, C., Keogh, B., Brady, A., & McCann, M. 2020. An overview of the qualitative descriptive design within nursing research. *Journal of research in nursing*, 25(5), pp. 443-455.

Eroğlu, Ş., & Çakmak, T. 2020. Information as an organizational asset: assessment of a public organization's capabilities in Turkey. *Information Development*, 36(1), pp. 58-77.

European IPR. 2012. *How to manage confidential business information*. Available from: [https://www.ipoi.gov.ie/en/commercialise-your-ip/using-ip-to-grow-your-business/what-is-intellectual-property-/how\\_to\\_manage\\_confidential\\_business\\_information.pdf](https://www.ipoi.gov.ie/en/commercialise-your-ip/using-ip-to-grow-your-business/what-is-intellectual-property-/how_to_manage_confidential_business_information.pdf) (Accessed 24/09/2022).

European Union Agency for Cybersecurity, ENISA. (2021). *Cybersecurity for SMES. Challenges and Recommendations*. European Union Agency for Cybersecurity (ENISA).

Eze, S.C., Chinedu-Eze, V.C., Bello, A.O., Adegun, A.A., & Alao, M.E. 2019. Challenges facing SMEs in emerging ICT adoption from diverse actors' perspective: A data driven approach. *International Journal of Mechanical Engineering and Technology*, 10(2), pp. 636-651.

FBI. 2018. *2017 Internet Crime Report Released* | Federal Bureau of Investigation. Available from: <https://www.fbi.gov/news/stories/2017-internet-crime-report-released-050718>(Accessed 17/09/2022).

Financial Reporting Council. 2018. *The UK corporate governance code*. Available from: <https://www.frc.org.uk/getattachment/88bd8c45-50ea-4841-95b0-d2f4f48069a2/2018-uk-corporate-governance-code-final.pdf> (Accessed 24/10/2022).

Fleming, J., & Zegwaard, J.E. 2018. Methodologies, methods and ethical considerations for conducting research in work-integrated learning. *International Journal of Work-Integrated Learning, Special Issue*, 19(3), pp. 205-213.



Ford, A., Al-Nemrat, A., Ghorashi, S.A., & Davidson, J. 2021. The impact of data breach announcements on company value in European markets. *WEIS*, pp. 1-8.

Forrester, V. 2019. *User information security behavior in professional virtual communities: A technology threat avoidance approach*. PhD Thesis, Nova Southeastern University, Florida, USA.

George, C. 2020. The Essence of Risk Identification in Project Risk Management: An Overview. *International Journal of Science and Research (IJSR)*, 9(2), pp. 1553-1557.

George, T. 2022. *Mixed methods research* | Definition, guide & examples. Scribbr. Available from:

<https://www.scribbr.com/methodology/mixed-methods-research/#:~:text=Advantages%20of%20mixed%20methods%20research,-%E2%80%9CBest%20of%20both&text=Combining%20the%20two%20types%20of,the%20weaknesses%20of%20the%20other> (Accessed 24/10/2022).

Goko, C. 2022. *Rand weakens past 17 per dollar as US recession fears mount*. Bloomberg Africa Edition.

Available online: <https://www.bloomberg.com/news/articles/2022-07-09/rand-s-resilience-tested-as-us-recession-fears-move-to-forefront?leadSource=verify%20wall> (Accessed 27/09/2022).

Guo, H., Liu, J., Qiu, Y., Menenti, M., Chen, F., Uhler, P.F., Zhang, L., van Genderen J., Liang, D., Natarajan, I., Zhu, L., & Liu, J. 2018. The Digital Belt and Road program in support of regional sustainability. *International Journal of Digital Earth*, 11(7), pp. 657-669.

Hadlington, L., & Parsons, K. 2017. Can cyberloafing and internet addiction affect organizational information security? *Cyberpsychology, behavior, and social networking*, 20(9), pp. 567-571

Hadlington, L., & Chivers, S. 2020. Segmentation analysis of susceptibility to cybercrime: exploring individual differences in information security awareness and personality factors. *Policing: A Journal of Policy and Practice*, 14, pp. 479-492.

Hayati, U., Mulyani, S., Sukarsa, D.E., & Winarningsih, S. 2021. Information system's implementation and its impact on university organization performance in west Java. *Utopía y Praxis Latinoamericana*, 26(1), pp. 343-358.

Heilman, M.E. 2012. Gender stereotypes and workplace bias. *Research in Organizational Behavior*, (32), pp. 113-135.

Hina, S., & Dominic, P.D.D. 2020. Information security policies' compliance: a perspective for higher education institutions. *Journal of Computer Information Systems*, 60(3), pp. 201-211.

Hudson, N. 2023. *Challenges and Opportunities for Small Tourism Businesses in South Africa Examining Pathways to a more Resilient System*. Available from: [https://www.ilo.org/wcmsp5/groups/public/---ed\\_emp/---emp\\_ent/---ifp\\_seed/documents/publication/wcms\\_866729.pdf](https://www.ilo.org/wcmsp5/groups/public/---ed_emp/---emp_ent/---ifp_seed/documents/publication/wcms_866729.pdf) (Accessed 27/08/2023).

Igwenagu, I. 2016. *Fundamentals of research methodology and data collection*. LAP Lambert Academic Publishing, Sunnyvale, USA, pp. 47.

ILDLP. 2014. *Informal Small Medium and Micro Enterprises (SMME) retailers in South Africa*. Available from: [https://www.wrseta.org.za/ILDLP/ILDLP\\_2014/Syndicate%201-%20Ratoon.pdf](https://www.wrseta.org.za/ILDLP/ILDLP_2014/Syndicate%201-%20Ratoon.pdf) (Accessed 24/10/2022).

Imperva. n.d. *Information security: The ultimate guide*. Available online: <https://www.imperva.com/learn/data-security/information-security-infosec/> (Accessed 10/11/2022).

IoDSA. 2020. *Integrated report 2020*. Available from: [https://cdn.ymaws.com/www.iodsa.co.za/resource/collection/E1C72386-2AEF-4AB7-9E54-6255E18806AE/IoDSA\\_Integrated\\_Report\\_2020.pdf](https://cdn.ymaws.com/www.iodsa.co.za/resource/collection/E1C72386-2AEF-4AB7-9E54-6255E18806AE/IoDSA_Integrated_Report_2020.pdf) (Accessed 24/10/2022).

James, N. 2023. *51 Small Business Cyber Attack Statistics 2023 (And What You Can Do About Them)*. Astra. Available from: <https://www.getastra.com/blog/security-audit/small-business-cyber-attack-statistics/#:~:text=Top%20Small%20Business%20Cyber%20Security%20Statistics%202023,-Here%20are%20the&text=Accenture's%20Cybercrime%20study%20reveals%20that,an d%20%24653%2C587%20on%20cybersecurity%20incidents> (Accessed 28/08/2023).

Jang-Jaccard, J., & Nepal. S. 2014. A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5), pp. 973-993.

Julisch, K. 2013. Understanding and overcoming cyber security anti-patterns. *Computer Networks*, 57, pp. 2206-2211.

Karataş, A. 2021. Evaluation of security management from the perspective of current management approaches and management models. *International Academic Social Resources Journal*, 6(31), pp. 1653-1670

Kemp, S. 2022. *Digital 2022: Global overview report*. Available from: <https://datareportal.com/reports/digital-2022-global-overview-report> (Accessed 24/10/2022).

Kivunja, C., & Kuyini, A.B. 2017. Understanding and applying research paradigms in educational contexts. *International Journal of Higher Education*, 6(5), pp. 26-41.

Koonin, M. 2014. Validity and reliability. In: Du Plooy-Cilliers, F., Davis, C. and

Bezuidenhout, R. (eds.) *Research matters*. Cape Town. Juta.

Kritzinger, E., Bada, M., & Nurse, J.R.C. 2017. A study into the cybersecurity awareness initiatives for school learners in South Africa and the UK. In: Bishop, M., Fitcher, L., Miloslavskaya, N., Theocharidou, M. (eds) *Information Security Education for a Global Digital Society*. WISE 2017. IFIP Advances in Information and Communication Technology, 503. Springer, Cham, pp. 110-120.

Kshetri, N. 2017. Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, 41(10), pp. 1027-1038.

Kumar, R. 2014. *Research methodology: A step-by-step guide for beginners*. Sage.

Kuzminykh, I., & Carlsson, A. 2018. Analysis of assets for threat risk model in Avatar-Oriented IoT architecture. In: O. Galinina, S. Andreev, S. Balandin, Y. Koucheryavy (eds) *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*. Springer: Cham, Switzerland, 11118: 52-63.

Kuzminykh, I., Ghita, B., Sokolov, V., & Bakhshi, T. 2021. Information security risk assessment. *Encyclopedia*, 1, 602-617.

Leboea, S.T. 2017. *Factors Influencing SMME Failure*. Unpublished Master's thesis, University of Cape Town, Cape Town.

Lejaka, T. 2021. *A framework for cyber security awareness in Small, Medium and Micro Enterprises (SMMEs) in South Africa*. MScThesis, University of South Africa, South Africa.

Leshilo, A., & Lethoko, M. 2017. The contribution of youth in Local Economic Development and entrepreneurship in Polokwane municipality, Limpopo Province. *Skills at Work: Theory and Practice Journal*, 8(1), pp. 45-58.

Lewis, J. & Ritchie, J. 2013. Generalizing from qualitative research. In: Ritchie, J., Lewis, J., Nicholls, C.M., Ormston, R. (eds.) *Qualitative research practice: A guide for social science students and researchers*. Sage Publications.

Li, Y., & Liu, Q. 2021. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, 7 pp. 8176-8186.

Lindemann, N. (2021). *What's the average survey response rate?* [2021 benchmark]. PointerPro. Available online: <https://pointerpro.com/blog/average-survey-response-rate/> (Accessed 0/11/2022).

Lukhele, N., & Soumonni, O. 2021. Modes of innovation used by SMMEs to tackle social challenges in South Africa. *African Journal of Science, Technology, Innovation and Development*, 13(7), pp. 829-837.

Luko, S.N. 2014. Risk assessment techniques. *Quality Engineering*, 26(3), pp. 379-38.

Luo, B., Yu, J., & Ji, H. 2012. Empirical analysis of interactive control's effectiveness: A parent-subsidiary company's interdependence perspective. *iBusiness*, 4, pp. 198-207.

Lundberg, J. 2020. *Dynamic risk management in information security: A socio-technical approach to mitigate cyber threats in the financial sector*. MSc Thesis, Örebro University, Örebro, Sweden.

Magnusson, A. 2022. *How much does ISO 27001 certification cost in 2022?* Available from: <https://www.strongdm.com/blog/iso-27001-certification-cost> (Accessed 24/10/2022).

Malhotra, G. 2017. Strategies in Research. *International Journal of Advance Research and Development*, 2(5), pp. 172-180.

Malumo, M. (2023). *Why SMEs in South Africa need cyber security*. Available from: <https://www.ikhokha.com/blog/why-smes-in-south-africa-need-cyber-security> (Accessed 29/08/2023).

Manning, K. 2017. *How and why small businesses are investing in cybersecurity*. The State of Security. Available from: <https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/small-businesses-investing-cybersecurity/> (Accessed 24/10/2022).

Marshall, C., & Rossman, G.B. 2016. *Designing qualitative research*. 6th ed.

Martínez, N., Vinas, A., & Matute, H. 2021. Examining potential gender bias in automated-job alerts in the Spanish market. *PLoS ONE*, 16(12), pp. 1-15.

Mertens, D. 2015. Mixed methods and wicked problems. *Journal of Mixed Methods Research*, 9(1), pp. 3-6.

Mesquida, A.L., Mas, A., Feliu, T.S., & Arcilla, M. 2014. MIN-ITs: a framework for integration of it management standards in mature environments. *International Journal of Software Engineering and Knowledge Engineering*, 24(6), pp. 887-908.

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas C., & Giannakopoulos, G. 2014. The human factor of information security: unintentional damage perspective. *Procedia - Social and Behavioral Sciences*, 147, pp. 424-428.

Mimecast, 2019. *The State Of Email Security Report 2019*. Retrieved from: <https://www.mimecast.com/resources/ebooks/the-state-of-email-security-report-2019/> (Accessed 23/10/2022).

Moody, G., Siponen, M., & Pahnla, S. 2018. Toward a unified model of information security policy compliance. *MIS Quarterly*, 42(1), pp. 285-311.

Moustafa, A.A., Bello, A., & Maurushat, A. 2021. The role of user behaviour in improving cyber security management. *Frontiers in Psychology*, 12(561011), pp. 1-9.

Murray, J., & Enang, I. 2022. *What is risk? Conceptualising Risk Assessment and Management across the Public Sector*. Emerald Publishing Limited, Bingley, pp. 1-16.

Nasir, A., Arshah, R.A., & Hamid, M.R.A. 2019. A dimension-based information security culture model and its relationship with employees' security behavior: A case study in Malaysian higher educational institutions. *Information Security Journal: A Global Perspective*, 28(3), pp. 55-80.

National Institute of Standards and Technology. 2014. *Framework for Improving Critical Infrastructure Cybersecurity*. Available from:  
<https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf> (Accessed 24/10/2022).

National Institute of Standards and Technology. 2018. *Framework for improving critical infrastructure cybersecurity*. Available from:  
<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>  
(Accessed 24/10/2022).

Neuman, W. L. 2014. *Social Research Methods: Qualitative and Quantitative Approaches*: Pearson New International Edition. Pearson Education Limited.

Ng, Z.X.H., Ahmad, A., & Maynard, S.B. 2013. Information security management: Factors that influence security investments in SMES. *11<sup>th</sup> Australian Information Security Management Conference*, pp.1-12.

Nie, Y., & Wu, X-L. 2021. Getting back to the nature of the microbial world: from the description and inductive reasoning to deductive study after 'meta-omics'. *Microbial Biotechnology*, 14(1), pp. 22-25.

Niemimaa, M., & Niemimaa, E. 2019. Abductive innovations in information security policy development: an ethnographic study. *European Journal of Information Systems*, pp. 1-24.

OECD. 2014. *Promoting better labour market outcomes for youth*. Melbourne. Available online: <https://www.oecd.org/g20/topics/employment-and-social-policy/OECD-ILO-Youth-Apprenticeships-G20.pdf> (Accessed 10/10/2022).

OECD. 2019. *Risks and challenges of data access and sharing*. Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, OECD Publishing, Paris. Available online: <https://doi.org/10.1787/15c62f9c-en> (Accessed 03/11/2022).

Originit. 2017. *Six most common security frameworks explained*. Available from <https://originit.co.nz/the-strongroom/six-most-common-securityframeworks-explained/> (Accessed 24/10/2022).

Oyelami, J.O., & Ithnin, N.B. 2015. Establishing a sustainable information security management policies in organization: A guide to information security management practice (ISMP). *International Journal of Computer and Information Technology*, 4(01), pp. 44-49.

Oyelana, A.A., & Adu, E.O. 2015. Small and medium enterprises (SMEs) as a means of creating employment and poverty reduction in Fort Beaufort. *Journal of Social Sciences*, pp. 8-15.

Palinkas, L.A., Horwitz, S.M., Green, C.A., Wisdom, J.P., Duan, N., & Hoagwood, K. 2015. Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and policy in mental health*, 42(5), pp. 533-544.



Pandey, N., & Pal, A. 2020. Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. *International journal of information management*, 55, 102171, pp. 1-5.

Parnis, D., Du Mont, J., & Gombay, B. 2015. Cooperation or co-optation? Assessing the methodological benefits and barriers involved in conducting qualitative research through medical institutional settings. *Qualitative Health Research*, 15(5), pp. 686-69.

Patrick, H., van Niekerk, B., & Fields, X. 2018. *Handbook of research on information and cyber security in the fourth industrial revolution*. IGI Global, Pennsylvania, United States.

Phil. 2020. What are Information Assets? Black Swan Security. Available online: <https://blog.blackswansecurity.com/2020/04/what-are-information-assets/> (Accessed 03/11/2022).

Priyadarshini, I., Kumar, R., Sharma, R., Singh, P. K., & Satapathy, S. C. 2021. Identifying cyber insecurities in trustworthy space and energy sector for smart grids. *Computers & Electrical Engineering*, 93(107204), pp. 1-15.

Robbins, S.P., & Judge, T.A. 2018. *Essentials of organizational behavior*. 14<sup>th</sup> Edition, Pearson Education, Inc., London, pp. 400.

Roller, M.R. 2020. *Strengths & limitations of the in-depth interview method: an overview*. Available from: <https://rollerresearch.com/MRR%20WORKING%20PAPERS/IDI%20Text%20April%202020.pdf> (Accessed 24/10/2022).

Rotar, L.J., Pamić, R.K., & Bojnec, S. 2019. Contributions of small and medium enterprises to employment in the European Union countries. *Economic Research-Ekonomska Istraživanja*, 32(1), pp. 3302-3314.

RSI Security. 2021. *Top risk control strategies in information security*. Available online:

<https://blog.rsisecurity.com/top-risk-control-strategies-in-information-security/> (Accessed 06/11/2022).

Saah, P. 2021. The impact of small and medium-sized enterprises on the economic development of South Africa. *Technium Social Sciences Journal*, 24, pp. 549-561.

Safa, N. S., Von Solms, R., & Fitcher, L. 2016. Human aspects of information security in organisations. *Computer Fraud & Security*, 2016(2), pp. 15-18.

Sandelowski, M. 2010. What's in a name? Qualitative description revisited. *Research in Nursing & Health*, 33, pp. 77-84.

Sanele, S., & David, D.O. 2021. Infrastructure development and population growth on economic growth in South Africa. *Munich Personal RePEc Archive*, 110884, pp. 1-11.

SANS. 2019. *The rising era of awareness training*. 2019 SANS Security Awareness Report, pp. 32.

Saunders, M., Lewis, P., & Thornhill, A. 2019. *Research Methods for Business Students*. 8<sup>th</sup> Edition. Harlow: Pearson.

Scholl, M., Leiner, K.M., & Fuhrmann, F. 2017. *Blind spot: Do you know the effectiveness of your information security awareness-raising program?* In: *Proceedings of the 21st World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2017)*, pp. 58-62.

SEDA. 2016. *BER Commissioned Research*. Stellenbosch University.

SEDA. 2018. *SEDA Integrated Business Report*. Pretoria: SEDA. Available online: [https://nationalgovernment.co.za/entity\\_annual/1487/2018-small-enterprise-development-agency-\(seda\)-annual-report.pdf](https://nationalgovernment.co.za/entity_annual/1487/2018-small-enterprise-development-agency-(seda)-annual-report.pdf) (Accessed 22/10/2022).

SEDA. 2019. *Women- and Youth owned SMMEs: the status, needs, challenges and opportunities in South Africa*. Integrated Report. Available online:

<http://www.seda.org.za/Publications/Publications/SEDA%20Integrated%20report%20-%20DSBD%2024%20Feb%2020.pdf> (Accessed 22/10/2022).

SEDA. 2022. *SMME Quarterly Update. 3rd Quarter 2021*. Available from: [http://www.seda.org.za/Publications/Publications/SMME%20Quarterly%202021Q3%20\(002\).pdf](http://www.seda.org.za/Publications/Publications/SMME%20Quarterly%202021Q3%20(002).pdf). (Accessed 24/10/2022).

Shamsudin, N.N.A., Yatin, S.F.M., Nazim, N.F.M., Talib, A.W., Sopiee, M.A.M., & Shaari, F.N. 2019. Information security behaviors among employees. *International Journal of Academic Research in Business and Social Sciences*, 9(6), pp. 560-571.

Sharma, G., Vidalis, S., Menon, C., Anand, N., & Kumar, S. 2021. Analysis and implementation of threat agents profiles in semi-automated manner for a network traffic in real-time information environment. *Electronics*, 10(1849), pp. 1-18.

Shojaifar, A., & Fricker, S.A. 2020. SMEs confidentiality concerns for security information sharing. Available from:

[https://www.researchgate.net/publication/342915920\\_SMEs\\_Confidentiality\\_Concerns\\_for\\_Security\\_Information\\_Sharing](https://www.researchgate.net/publication/342915920_SMEs_Confidentiality_Concerns_for_Security_Information_Sharing) (Accessed 24/10/2022).

Singh, R.K. 2014. Role of intellectual property rights for SMES: Need to manage knowledge. *DLR*, 6(1), pp. 25-40.

Sitharam, S., & Hoque, M. 2016. Factors affecting the performance of small and medium enterprises in KwaZulu-Natal, South Africa. *Problems and Perspectives in Management*, 14(2-2), pp. 277-300.

SME Climate Hub. 2022. *New data reveals two-thirds of surveyed small businesses*

*concerned over navigating climate action*. Available from:  
<https://smeclimatehub.org/new-survey-reveals-small-business-barriers-climate-action/>  
(Accessed 24/10/2022).

Somepalli, S.H., Tangella, S.K.R., & Yalamanchili, S. 2020. Information security management. *Holistica*, 11(2), pp. 1-16.

Snehi, M., & Bhandari A. 2021. Vulnerability retrospection of security solutions for software-defined cyber-Physical system against DDoS and IoT-DDoS attacks. *Computer Science Review*, 40(100371), pp. 1-23.

Soomro, K.A., Kale, U., Reagan, C., Akcaoglu, M., & Bernstein, M. 2020. Digital divide among higher education faculty. *The International Journal of Educational Technology in Higher Education*, 17(21), pp. 1-16.

Srinidhi, B., Yan, J., & Tayi, G.K. 2015. Allocation of Resources to Cyber-security: The Effect of Misalignment of Interest between Managers and Investors. *Decision Support Systems*, 75, pp. 49-62.

Srinivas, K. 2019. Process of Risk Management. In: A.G. Hessami (ed). Perspectives on Risk, Assessment and Management Paradigms. *IntechOpen*, pp. 1-42.

Statistics South Africa (Stats SA). 2021. *Tourism in South Africa: a pre-COVID-19 benchmark*. Available from: <https://www.statssa.gov.za/?p=14992> (Accessed 25/09/2023)

Taylor, L. 2017. What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society*, 4(2), pp. 1-14.

The Auditor-General South Africa. 2020. *Integrated 2020-21 annual report*. The increased relevance in a changing world, pp. 178.

UNHCR Global Report. 2020. Available from: [https://reporting.unhcr.org/sites/default/files/gr2020/pdf/GR2020\\_English\\_Full\\_lowres.pdf](https://reporting.unhcr.org/sites/default/files/gr2020/pdf/GR2020_English_Full_lowres.pdf) (Accessed 10/10/2022).

Ursillo, Jr., S., & Arnold, C. 2019. *Cybersecurity is critical for all organizations – Large and Small*. Preparing future-ready professionals. Available online: <https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/cybersecurity-critical-all-organizations-large-and-small> (Accessed 06/11/2022).

vanDriel, H. 2019. Financial fraud, scandals, and regulation: A conceptual framework and literature review. *Business History*, 61(8), pp. 1259-1299.

Verizon Enterprise. 2020. *Data breach investigations report*. Available from: <https://www.verizon.com/business/resources/reports/2020/2020-data-breach-investigations-report.pdf> (Accessed 24/10/2022).

Wandera. 2018. Understanding the mobile threat landscape in 2018. Available from: [http://staxxsolutions.com/wp-content/uploads/2018/05/Understanding\\_the\\_mobile\\_threat\\_landscape.pdf](http://staxxsolutions.com/wp-content/uploads/2018/05/Understanding_the_mobile_threat_landscape.pdf) (Accessed 24/10/2022).

Whitman, M.E., & Mattord, H.J. 2012. *Principle of information security*, 4<sup>th</sup> Edition. Thomson Course Technology, Boston, pp. 658.

Woiceshyn, J., & Daellenbach, U.S. 2018. Evaluating inductive versus deductive research in management studies: Implications for authors, editors, and reviewers. *Qualitative Research in Organizations and Management an International Journal*, 13(1), pp. 1-28.

World Bank. 2018. *The World Bank Annual Report 2018*. Washington, DC: World Bank.

World Bank. Available from: <https://openknowledge.worldbank.org/handle/10986/30326> (Accessed 24/10/2022).

Yoshino, N., & Taghizadeh-Hesary, F. 2016. Major challenges facing small and medium sized enterprises in Asia and solutions for mitigating them. *ADB Working Paper 564*. Tokyo: Asian Development Bank Institute. Available from: <http://www.adb.org/publications/majorchallenges-facing-small-and-medium-sized-enterprises-asia-and-solutions/> (Accessed 24/10/2022).

Żelechowska, D., Żyluk, N., & Urbański, M. 2020. Find out a new method to study abductive reasoning in empirical research. *International Journal of Qualitative Methods*, 19, pp. 1-11.

Zervoudi, E.K., 2020. Fourth industrial revolution: opportunities, challenges, and proposed policies. In: *Industrial Robotics-New Paradigms* [Working Title]. Available online: <https://www.intechopen.com/chapters/70877> (Accessed 09/09/2022).

Zhao, Z., Ye, R., Zhou, C., Wang, D., & Shi, T. 2021. Control-theory based security control of cyber-physical power system under multiple cyber-attacks within unified model framework. *Cognitive Robotics*, 1, pp. 41–57.

## APPENDICES

### Appendix 1: Ethics informed consent form

#### ETHICS INFORMED CONSENT FORM Faculty of Business and Management Sciences

##### CONSENT TO PARTICIPATE IN A STUDY

You are kindly invited to participate in an Information Security on SMMEs study being conducted by Sinxolo Mokolo from Cape Peninsula University of Technology. The findings of this study will contribute towards (tick as appropriate):

<i>An undergraduate project</i>		<i>A conference paper</i>	
<i>An Honours project</i>		<i>A published journal article</i>	
<i>A Masters/doctoral thesis</i>	✓	<i>A published report</i>	

The research is entitled “**Identifying Information Security aspects that can be included in the Information Security Management Framework for SMMEs in South Africa**” The aim of this study is to evaluate the information security aspects and how they can be included in the information security management framework for SMMEs in Cape Town.

Information security development and implementation are important to Small, Macro, and Medium enterprises (SMMEs). SMMEs are faced with information security management issues and have been credited to their limited information management systems and resources. SMMEs are usually prone to information security breaches because of the lack of simple control and planning systems and limited standardization of information processes. Similar to other business, asset information need to be protected and managed strategically. The research focuses on individuals in the SMME sector to determine knowledge on information security and how they protect their SMMEs from security breaches.

##### Selection criteria

You were selected as a possible participant in this study because you are:

- You are in the SMMEs sector and understand issues surrounding SMMEs, particularly with regard to Information Security aspects

Your participation in this project is voluntary. You may refuse to participate or withdraw from the project at any time with no negative consequence. There will be no monetary gain from participating in this research project. Confidentiality and anonymity of records will be maintained by the researcher and the Department of Business and Administration, Cape Peninsula University of Technology. This study has been ethically reviewed and approved by the Department of Business and Management Sciences Research Ethics Committee (approval number: 2020FOBREC761). The questionnaire should take about 10-15 minutes to complete. Thank you for your time.

Please sign the consent form. You were given a copy of this form on request.

Signature of participant	Date



## Appendix 2: Ethical clearance from the university



P.O. Box 1906 • Bellville 7535 South Africa • Tel: +27 21 4603291 • Email: fbmsethics@cput.ac.za  
Symphony Road Bellville 7535


Office of the Chairperson Research Ethics Committee	Faculty: <b>BUSINESS AND MANAGEMENT SCIENCES</b>
--	--

The Faculty's Research Ethics Committee (FREC) on **28 April 2020**, ethics **Approval** was granted to **Sinoxolo Mokolo (214197328)** for **MTech: Business Information Systems** research activity at Cape Peninsula University of Technology.

Title of dissertation/thesis/project:	<b>THE DESIGN OF INFORMATION SECURITY MANAGEMENT FRAMEWORK FOR CAPE TOWN organizations</b>  Lead Supervisor (s): Prof E. Ruhode
---------------------------------------	---

### Comments:

**Decision: Approved**

	<b>8 May 2020</b>
Signed: Chairperson: Research Ethics Committee	Date

Clearance Certificate No | 2020FOBREC761

## Appendix 3: Questionnaire

### Section A

- Please can you answer the following questions to the best of your ability.
- Please tick the appropriate box

#### 1. Gender

Male	<input type="checkbox"/>
Female	<input type="checkbox"/>

#### 2. Age (yrs)

20-24	25-29	30-35	36-40	41-49	50+
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

#### 3. Department and position of the participant

IT Technician	IT manager	Web Designer	Master Website Developer	Software Developer
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

#### 4. Work experience (yrs)

1-3	4-6	7-9	10-14	15-19	20+
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

#### 5. Highest level of completed education

Diploma	Degree	Master	Doctorate
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### Section B

- Please fill in in the spaces given to the best of your ability.

#### 6. What is the information security management faced by SMME's?

---

---

---

**7. Does the organisation have any information security policies?**

---

**8. If present are the information security policies conveyed to employees?**

---

---

---

**9. How often are the policies reviewed?**

---

---

---

**10. Does the organisation have a designated department and budget for information security management?**

---

---

**11. Does the organisation conduct any risk assessment when interacting with individuals outside the organisation?**

---

---

---

**12. Is Information asset controlled through the granting of non-disclosure and confidentiality agreement?**

---

---

---

**13. In dealing with customers what are the information security measures implemented?**

---

---

---

---

---

**Section C**

- Please answer with either a YES (Y) or a NO (N) to the best of your ability.

14. Does the organisation offer any information security management training to the employees and how frequently?	
15. Does the organisation have guidelines to protect intellectual property rights?	
16. Does the organisation have reporting mechanism on information security incidence?	
17. Does the organisation have an access control policy?	

**Section D**

- Please complete this section if you have any other issues that you may want to bring to the researcher's attention with regards to the study.

**18. Any other issues**

---

---

---

---

---

**THANK YOU FOR PARTICIPATING**