

https://dspace.org/

# Factors influencing cyber insurance adoption in South Africa industry

**Mbatha, Nkosinathi Sphiwe**

**2020**

University of the Witwatersrand, Johannesburg

https://hdl.handle.net/10539/30071

Mbatha, Nkosinathi Sphiwe. (2020). Factors influencing cyber insurance adoption in South Africa industry [Master's dissertation, University of the Witwatersrand, Johannesburg]. WireDSpace.https://hdl.handle.net/10539/30071

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

# Factors influencing cyber insurance adoption in South Africa industry

**Nkosinathi Sphiwe Mbatha**

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

**Johannesburg, 2020**

(Version 2019-2020)

# ABSTRACT

Organisations are benefiting from the use of emerging digital technologies for improved efficiencies. These technologies are vulnerable to cyber-attacks resulting in breaches on organisational assets. Cyber-attacks necessitates boards and top management to strategically rethink their cybersecurity approaches to managing cyber risks. The purpose of the study was to explore the factors influencing cyber insurance adoption in the South African industry. The study adapted Technology-Organisation-Environment (TOE) theoretical framework to investigate cyber insurance adoption relevant to the South African context. The review of literature focused on the cybersecurity, cyber risk management, and cyber insurance phenomenon to understand the global and developing world landscape. The research design followed the systemic collection of qualitative data through semi-structured interview questions on the purposefully selected sample of professionals in the public and private sectors of the South African industry. The analysis and interpretation through categorisation of patterns of data collected enabled presentation and discussion of emerging themes resulting in findings. The key findings relate to effective cybersecurity awareness, organisational approach to managing cyber risks, as well as the nature of industry and compliance with legislation. The study established that the combination of effective cybersecurity awareness, the relationship between the strategic organisational approach to cybersecurity and top management support towards cyber risk management as well as compliance with legislation are the factors influencing cyber insurance adoption in the South African industry. In order to meet the research objectives, various conclusions were made. The study concluded that effective cybersecurity awareness must be viewed as a strategic imperative to enable organisations to operate securely. The study also concluded that organisations must proactively approach cybersecurity strategically thereby ensuring effective top management buy-in. The study concluded that the POPI Act is the primary driver of cyber insurance adoption in the South African industry.



# KEY WORDS

Cybersecurity, cyber risk, cyber insurance, cybercrime, cyber-attack.

# DECLARATION

I, Nkosinathi Sphiwe Mbatha, declare that this research report is my own work except as indicated in the references and acknowledgements. It is submitted in partial fulfilment of the requirements for the degree of Master of Management in the field of Digital Business at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in this or any other university.

Name: Nkosinathi Sphiwe Mbatha Signature: 

Signed at … Johannesburg……

On the ……04…….. day of … November…… 2020…..

# DEDICATION

The research report is dedicated to my late mother, Ms Hilda Nonhlanhla Mthethwa, who passed on 23 years ago. As a domestic worker, she did not have the opportunity to study at the university. I, therefore, dedicate this Masters' degree to her for believing in the value of education as an instrument to transform my life, family and broader society. In memory of my late mother, I aspire to share my learnings, experiences and the knowledge gained through mentorship and coaching of youth coming from disadvantage communities.

# ACKNOWLEDGEMENT

I would like to give thanks to God Almighty for He is my light and comfort for everything spiritual. Without God, the Master of Management in Digital Business (MMDB) would not be possible. I would like to thank my family, my wife Sophia Moraka and daughter Sphesihle Mbatha for being my pillar of strength and encouraging me to pursue this qualification. My family suffered the most neglect due to my absence as I was swallowed by the studies. At times, I felt overwhelmed; however, I consistently reminded myself why I enrolled for this qualification in the first place. This was the most difficult initiative I have ever done in my life However I am thankful for persevering till the end.

A big THANK YOU to my supervisor Mr Mthandeni Langa for his guidance, support, and passion for research, which lifted my spirit during points of breakdown. I have learned to be resilient during this challenging period. My friend Monwabisi Kula for your wisdom and deep intellectual prowess that motivated me when my energy was low. To Yoav Tchelet, my former boss (CIO), for encouraging me to pursue a master's qualification and always providing support.

Thank you to my MMDB classmates for walking this challenging journey with me, in particular, Mr Samuel Mahlangu for always being authentic, supportive and understanding. I would like to thank the research participants who provided insightful responses during interview sessions, without whom this research would not be possible.

Last but not least, to my father, Mr Thembinkosi Joshua Mbatha, THANK YOU for raising and teaching me the responsibility of being a man. Ngiyabonga Ndabezitha Shandu kaNdaba.

# TABLE OF CONTENTS

**ABSTRACT** ..... **ii**

**DECLARATION** ..... **iii**

**DEDICATION** ..... **iv**

**ACKNOWLEDGEMENT** ..... **v**

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

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

**LIST OF ACRONYMS** ..... **xi**

**CHAPTER 1. INTRODUCTION** ..... **12**

1.1 PURPOSE OF THE STUDY ..... 12
1.2 CONTEXT OF THE STUDY ..... 13
1.3 RESEARCH PROBLEM ..... 14
1.4 RESEARCH OBJECTIVES ..... 15
1.5 SIGNIFICANCE OF THE STUDY ..... 15
1.6 DELIMITATIONS OF THE STUDY ..... 16
1.7 DEFINITION OF TERMS ..... 17
1.8 ASSUMPTIONS ..... 17

**CHAPTER 2. LITERATURE REVIEW** ..... **19**

2.1 INTRODUCTION ..... 19
2.2 BACKGROUND ..... 19
2.3 THE TECHNOLOGY ORGANISATION ENVIRONMENT FRAMEWORK ..... 21
2.4 LINKING CYBERSECURITY TO DIGITAL TECHNOLOGY ..... 22
2.4.1 INCREASE IN ELECTRONIC DATA ..... 23
2.4.2 INCREASE IN MOBILE DEVICES ..... 24
2.4.3 INCREASE IN ORGANISED CYBERCRIME GROUPS ..... 26
2.4.4 INCREASE OF INTELLIGENT EXTERNAL AND INTERNAL IT SECURITY THREATS ..... 28
2.4.5 THE DIFFICULTY OF TRACING THE ATTACKERS ..... 29
2.4.6 LIMITED CYBERCRIME LAWS ..... 30
2.4.7 LIMITED IT SECURITY KNOWLEDGE AMONG INTERNET USERS ..... 31
2.4.8 PROPOSITION 1 ..... 33
2.5 CYBER RISK MANAGEMENT ..... 33
2.5.1 CYBER INSURANCE AS A MECHANISM TO MANAGE CYBER RISK ..... 35
2.5.2 CYBER RISK IN SOUTH AFRICA ..... 38

2.5.3 Proposition 2 ..... 39
2.6 Cyber insurance market ..... 39
2.6.1 Types of cyber insurance liability covers ..... 42
2.6.2 Drivers of cyber insurance ..... 45
2.6.3 Challenges of cyber insurance ..... 47
2.6.4 Proposition 3 ..... 49
2.7 Conclusion of the Literature Review ..... 49
2.7.1 Proposition 1 ..... 50
2.7.2 Proposition 2 ..... 50
2.7.3 Proposition 3 ..... 50

**CHAPTER 3. RESEARCH METHODOLOGY ..... 51**

3.1 Introduction ..... 51
3.2 Research approach ..... 51
3.3 Research design ..... 52
3.4 Data collection methods ..... 53
3.5 Population and sample ..... 53
3.5.1 Population ..... 53
3.5.2 Sample and sampling method ..... 54
3.6 The research instrument ..... 55
3.7 Procedure for data collection ..... 56
3.8 Data analysis and interpretation ..... 57
3.9 Limitations of the study ..... 58
3.10 Transferability and dependability ..... 58
3.10.1 Transferability ..... 58
3.10.2 Dependability ..... 58
3.10.3 Credibility ..... 59
3.10.4 Confirmability ..... 59
3.11 Demographic profile of the respondent ..... 60
3.12 Ethical considerations ..... 61

**CHAPTER 4. FINDINGS AND DISCUSSION ..... 62**

4.1 Introduction ..... 62
4.2 Discussion pertaining to Proposition 1 ..... 65
4.2.1 Effective cybersecurity awareness ..... 65
4.3 Discussion pertaining to Proposition 2 ..... 73
4.3.1 An organisational approach to managing cyber risk ..... 73
4.4 Discussion pertaining to Proposition 3 ..... 82
4.4.1 Cyber insurance adoption in South Africa industry ..... 82
4.5 Conclusion ..... 89

**CHAPTER 5. CONCLUSIONS & RECOMMENDATIONS ..... 91**

5.1 Introduction ..... 91
5.2 Conclusions regarding research objective 1 ..... 92

5.3 CONCLUSIONS REGARDING RESEARCH OBJECTIVE 2 ..... 92
5.4 CONCLUSIONS REGARDING RESEARCH OBJECTIVE 3 ..... 93
5.5 RECOMMENDATIONS ..... 95
5.6 SUGGESTIONS FOR FURTHER RESEARCH ..... 95

**REFERENCES ..... 97**

**APPENDIX A – Semi-structured Interview Questions ..... 121**

I) SETTING THE SCENE ..... 121
II) CYBER SECURITY ..... 121
III) TECHNOLOGY ..... 122
IV) ORGANISATION ..... 124
V) ENVIRONMENT ..... 124

**APPENDIX B – Participant Information Sheet ..... 126**

# LIST OF TABLES

**Table 1: Comparison of cyber insurance policies Source**..... 41

**Table 2: Cyber insurance challenges**……48

**Table 3: Profile of respondents**..... 54

**Table 4: Demographic profile of respondents**..... ……59

**Table 5: Consistency matrix**..... 62

**Table 6: Cybersecurity perception** ..... 654

**Table 7: Cyber insurance perception** ..... 72

**Table 8: Cybersecurity approach and management support**..... 754

**Table 9: Cyber insurance adoption** ..... 81

**Table 10: Cyber insurance in the public and private sectors**..... 82

# LIST OF FIGURES

**Figure 1: Cybersecurity** ..... 19

**Figure 2: TOE Framework** ..... 20

**Figure 3: Anticipated Projection of global Datasphere** ..... 23

**Figure 4: Global IP traffic, wired and wireless** ..... 24

**Figure 5: Internet users in selected countries in Africa** ..... 25

**Figure 6: Federal cyber-security survey** ..... 27

**Figure 7: Value-vulnerability grid** ..... 33

**Figure 8: Cyber insurance decision** ..... 34

**Figure 9: Proposed cyber insurance claims process** ..... 36

**Figure 10: Most covered losses** ..... 42

**Figure 11: Policy exclusions** ..... 43

**Figure 12: Cyber insurance premium** ..... 44

**Figure 13: Cyber protection** ..... 47

**Figure 14: Summary of research design** ..... 51

# LIST OF ACRONYMS

**4IR – 4th Industrial Revolution**

**AIG – American International Group**

**CIA – Confidentiality Integrity Availability**

**CIO – Chief Information Officer**

**CISO – Chief Information Security Officer**

**EU – European Union**

**GDPR – General Data Protection Regulation**

**ICT – Information and Communications Technology**

**IP – Internet Protocol**

**IT – Information Technology**

**IoT – Internet of Things**

**ISO – International Organisation of Standardisation**

**POPI – Protection of Personal Information**

**SA – South Africa**

**SME – Small Medium Enterprise**

**US – United States**

# CHAPTER 1. INTRODUCTION

This chapter introduces the research study to investigate factors influencing cyber insurance adoption in South Africa. The purpose and significance of the study are elucidated and contextualised in the public and private sectors of the South African industry. The research problem is unpacked in detail thus leading to research objectives. Key constructs that are out of the scope of this study are discussed in this chapter. The study investigates individuals that are positioned at strategic, tactical and operational levels in organisations. These levels are operationalised through organisational cross cutting constructs such as technology, processes and sytems to drive organisational objectives.

## 1.1 Purpose of the study

The origin of the cyber insurance market can be traced back to the 1970s from the technology risk or technology errors and omissions (E&O) (Camillo, 2017). All industries, public and private, are susceptible to cyber risks (Kopp, Kaffenberger, & Jenkinson, 2017). This has resulted in the elevation of cybersecurity's importance and visibility to the highest levels of organisations wherein the executives and boards perceive it as a strategic imperative Kopp et al. (2017). This suggests that executives are cognisant of the impact of the lack of sound cybersecurity practices within organisations. Thus, the consistent increase in cyber-attacks is developing awareness for cyber insurance to provide relief in the event the organisation is attacked (Toregas & Zahn, 2014).

Completely eliminating cybersecurity risks is a challenging task albeit the latest cybersecurity defence technologies and implementing security policies to mitigate the likelihood of a cybersecurity breach (Tabansky, 2017). This suggests that no matter how strong the protection technology and security practices are, there is a possibility that an intruder can gain access to the company's systems and data assets. Also, there may be gaps in terms of internal employee skillset as well as cybersecurity levels of awareness which usually lags sophisticated intruders (Addington & Manrod, 2019). Generally, this reality is particularly prevalent in most organisations due to lack of resources and capabilities to

effectively deal with cyber risks (Sommerrock, Madnick, Siegel, Pulido, Coden, Bartol, & Bernaski, 2018).

In addition, residual cybersecurity risks cannot be entirely mitigated through the deployment of technical controls only (Rohmeyer & Bayuk, 2019). As such, sound cyber resilience is achieved through a combination of technical, procedural, financial and human interventions (Toregas & Zahn, 2014). Cyber insurance fills the gaps left by inadequate technology, skills, and effective levels of cybersecurity awareness to enhance cyber resilience (Tiirmaa-Klaar, 2016). Therefore, the desired outcome of this study was to scrutinise the factors influencing cyber insurance adoption in both the public and private sectors of the South African industry.

## 1.2 Context of the study

Cybersecurity breaches are growing at exponential rates and organisations are seeking to explore methods to lower the effect of cybersecurity breaches (Addington & Manrod, 2019). The advent of increasing internet penetration fuelled by mobile devices, protecting organisational assets such as data, systems, applications, and intellectual property becomes elevated on the Information Technology (IT) and business executives agenda (ISACA, 2016). In 2017, it was estimated that there is 20.35 billion connected Internet of Things (IoT) devices and the figure is likely to increase (Silva et al., 2019). Mitigating the risk that emanates from such connectivity is becoming an overwhelming duty for most Cyber Security professionals as the threat landscape has intensified significantly (IDC, 2018).

Most organisations are digitalising their operations to take advantage of the 4$^{th}$ industrial revolution (4IR) that has a potential to expose the organisation to hacking if cybersecurity risk is inadequately managed (Leitner & Stiefmueller, 2019). According to an IBM study conducted on 477 organisations in 13 different countries including 2634 individuals, it was estimated that the average cost of a data breach could exceed $3.86 million by 2019.

Furthermore, the introduction of regulations such as the General Data Protection Regulation (GDPR) for South African organisations operating in the European Union (GDPR, 2019) and more specifically in the context of South Africa, the Protection of Personal Information Act (POPIA), becomes the drivers for enhanced cybersecurity posture for organisations (*POPIA*, 2013). This is due to stringent rules that emanate from the aforementioned regulations to secure data.

A breach of IT systems could result in lasting reputational damage, revenue loss, and fines to the organisation of any size (ISACA, 2016). Customers could also sue companies in the event their personal information is accessed by an unauthorised party during the breach (North & Pascoe, 2016). Cybersecurity attacks have become sophisticated and therefore require a different approach to mitigating cyber risks (Camillo, 2017). Thus, over and above implementing technical controls, companies must explore cyber insurance to enhance cyber resilience to systems and data (Kesan & Hayes, 2017).

Whilst cyber insurance is not a silver bullet or replacement for improved cybersecurity from people, process and technology perspective; skills, training, policies, and procedures, as well as technology, are still required (Sommerrock et al., 2018). Therefore, cyber insurance can provide a financial shield to ensure operations are resumed speedily post cyber breach in the South African industry.

## 1.3 Research problem

Cybersecurity is a topical issue at the board level due to the impact it has on the reputation and therefore sustainability of the business of any size (ISACA, 2016). The absence of a systemic approach to cyber defence that takes into account the use of best practice frameworks, internal controls, cyber risk management and understanding of ever-changing cybersecurity landscape can be a challenge to organisations (Kshetri, 2015b). Coordination efforts to mitigate cyber threats such as the inability to access critical business systems, unauthorised modification of data as well unavailability of systems is required (Skopik et al., 2016).

Cybersecurity threats can be exploited as a result of unpatched machines, weak passwords, and lack of periodic antimalware updates (Süzen, 2020) as well as

employee negligence or failure to backup mission-critical systems (Nikolov & Slavyanov, 2018). Cyber-attacks such as ransomware, brute-force, and denial of service and leakage/loss of sensitive information by employees who have access to data could result in revenue loss, reputational damage, regulatory fines, and penalties as well as customer ligation suits (Tabansky, 2017).

To ensure confidentiality, integrity, and availability (CIA) of information assets and in light of the rising cyber-attacks, companies must consider adding cyber insurance to mitigate against cyber risks (Sommerrock et al., 2018). Therefore, what are the factors influencing cyber insurance adoption in South Africa industry?

## 1.4 Research objectives

The objective of this research is to investigate factors influencing cyber insurance adoption in South Africa industry from the perspective:

i. Technology about the awareness and effectiveness of cybersecurity technologies.
ii. Organisation about cyber risk management and management support.
iii. Environment about government regulations and the nature of the industry.

## 1.5 Significance of the study

Cyber insurance is a growing industry in developed markets such as the United States (US) and European Union (EU) (N. Shetty et al., 2010; Wang, 2019). The significance of the study is to identify factors pertinent to the adoption of cyber insurance within the South African industry context. Due to the criticality of sound cyber resilient practices for South African organisations, cyber insurance can be an added layer of cyber risk management that ensures sustainability (Huang et al., 2018).

Cyber insurance enables organisations to focus on key strategic objectives such as increased revenue, customer satisfaction, and compliance with applicable laws thereby contributing to the long term viability of the organisation (Brangetto & Aubyn, 2015). However, investment in cyber insurance does not translate to revenue generation or growth for an organisation (Camillo, 2017). The customer concerns with privacy and the introduction of legislation regulating the security of customer data is no longer a nice to have for organisations (King & Raja, 2012), it is a regulatory requirement (GDPR, 2019; POPIA, 2013).

Management of cyber risks can improve organisational performance and improve compliance with internal processes as well as external legislative and regulatory frameworks for improved cybersecurity posture (Contreras et al., 2012; Daud et al., 2018). Due diligence becomes management's main concern in ensuring reasonable cybersecurity by firms of all sizes (Brangetto & Aubyn, 2015).

In the developing world, cyber insurance has proven to enhance value to business by ensuring the swift resumption of operations albeit, at a higher cost, which lowers the demand for adoption (Kshetri, 2015b). Therefore, the study will add local findings to the pool of existing knowledge on the factors influencing the adoption of cyber insurance in the South African industry. As such, relationships between cybersecurity, cyber risk management, and cyber insurance concepts are explored to ground the study into the South African context.

## 1.6 Delimitations of the study

The research study will focus on organisations that operate in the South African industry both public and private sectors. The study will consider employees in the strategic, tactical and operational levels to ascertain their views and experiences on cyber insurance phenomenon. The study will exclude the following aspects:

a) Cyber insurance premium calculations
b) Cyber risk modelling
c) Accumulation risk
d) Insurability of organisations
e) Cyber insurance modelling

f) Cyber insurance pricing
g) Quantification of the value cyber attacks

## 1.7 Definition of terms

**Cyber insurance** refers to insurance contracts designed to mitigate liability issues, property loss and theft, data damage, loss of income from network outage and computer failures, Web-site defacement, and cyber extortion (Bandyopadhyay et al., 2009).

**Cyber risks** are defined as operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems (Eling & Wirfs, 2015).

**Cybersecurity** is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets (R. von Solms & van Niekerk, 2013, p. 1).

**Vulnerability** refers to weak points that are built-in properties of a defined system (Tabansky, 2011).

## 1.8 Assumptions

The research made the following assumptions:

a) Participants will be available and co-operate to ensure that the research study is complete.
b) Participants will provide relevant perspectives based on their understanding of the concepts.
c) Participants have an understanding of cybersecurity, cyber risk, and cyber insurance.
d) Participants will answer diligently to enrich the generation of knowledge through their industry experience.

e) Participants work in the South African industry for both the public and private sectors.

# CHAPTER 2. LITERATURE REVIEW

## 2.1 Introduction

The previous chapter (Chapter 1) provided a high-level purpose, context, and significance of the study by identifying a problem and objectives to the study about the adoption of cyber insurance in the South African industry. Chapter 2 reviews the literature that underpins the study in terms of linkage between cybersecurity and emerging digital technologies. This chapter provides a brief background and explores the causes of cybersecurity incidents that have a significant impact on businesses. The exploration of the Technology-Organisation-Environment (TOE) theoretical framework forms the basis upon which this study is based to elucidate emerging factors leading to the first proposition.

Furthermore, the introduction of the concept of cyber risk management with a particular focus on the South African and developing world context is unpacked in detail. The study then makes a second proposition that attempts to bring to light the potential benefits of a proactive cyber-risk management approach.

Finally, the study delves into the cyber insurance market, various types of cyber insurance covers, the drivers and challenges that have an impact on the adoption of cyber insurance. The third proposition emerges and explores the impact of the operating environment on cyber insurance adoption in South Africa.

## 2.2 Background

Globally, cybersecurity is inevitably receiving the attention as it is considered a different method of warfare (de Bruijn & Janssen, 2017) which necessitates the organisation to search for sustainable countermeasures (Goode, 2018; Von Solms & Van Niekerk, 2013) and any business operation can be impacted negatively (Costa et al., 2019). According to Vicevich (2018, p. 9), "*cybersecurity is national security"* and comprises different aspects that are complex, ranging from legal and legislative issues, global threat actors, and different types of cyber

threats. Threat actors include but not limited to script kiddies, competitors, nation-states, terrorists, employees, customers criminals or malicious hackers (Aloul, Al-Ali, Al-Dalky, Al-Mardini, & El-Hajj, 2012).

The objective of cybersecurity is to ensure confidentiality, integrity, and availability of systems, data and assets (R. von Solms & van Niekerk, 2013). The view is similar to the ISO 27000 standard. International Organisation for Standardisation is the world-renowned entity that publishes and develops standards and best practice frameworks ('ISO - International Organization for Standardization', 2019). The ISO 27000 series contains guidelines and controls for organisations to manage their cybersecurity risk programmes (Herr, 2019). According to Von Solms & van Niekerk (2013), cybersecurity is premised on protecting assets from a range of threats posed by vulnerabilities as illustrated in Figure 1 below.

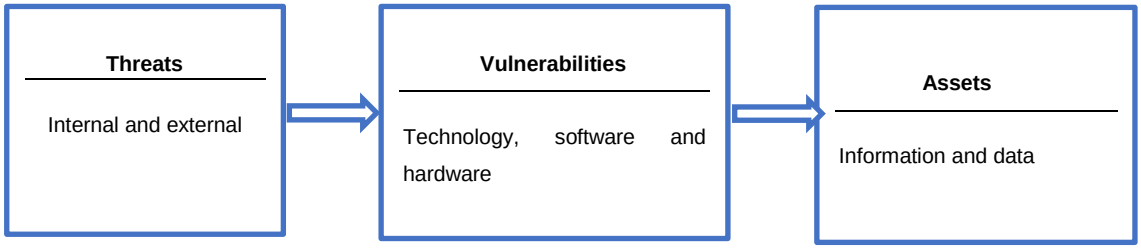



**Figure 1**: Cybersecurity Adapted from (R. von Solms & van Niekerk, 2013)

Figure 1 above indicate that there are various threats due to vulnerabilities of systems, data, and technology that are likely to affect organisational assets, human and their interest negatively if they are not managed properly. As such, threats can emanate both from internal and external because of vulnerabilities inherently on technology, software, and hardware. Such vulnerabilities may negatively affect organisational assets thus must be secured.

Cyberspace has the potential to provide human-kind with benefits that meaningfully improve the quality of life but has various unknown risks that if they are not addressed could result in security incidents (Tabansky, 2017). A security incident is defined as a set of security events linked with a multitude of potentially concerted network activities that merit special consideration by the network administrator (Ab Rahman & Choo, 2015).

## 2.3 The Technology Organisation Environment Framework

The Technology-Organisation-Environment (TOE) framework describes the process by which a firm adopts and implements innovations in the technological, organizational, and environmental contexts (Tornatzky et al., 1990). According to Bandyopadhyay (2012a), the Technology Organization Environment (TOE) framework of (Tornatzky et al., 1990) is appropriate for an adequate model of adoption of cyber insurance. Figure 2 below illustrates an adapted TOE framework that underpins this study. Furthermore, it is stated that "*a model for adoption and utilization of cyber insurance must fundamentally include the factors that affect the perceived valuation of cyber insurance as an instrument to manage cyber risk in the organization*" (Bandyopadhyay, 2012a, p. 3).

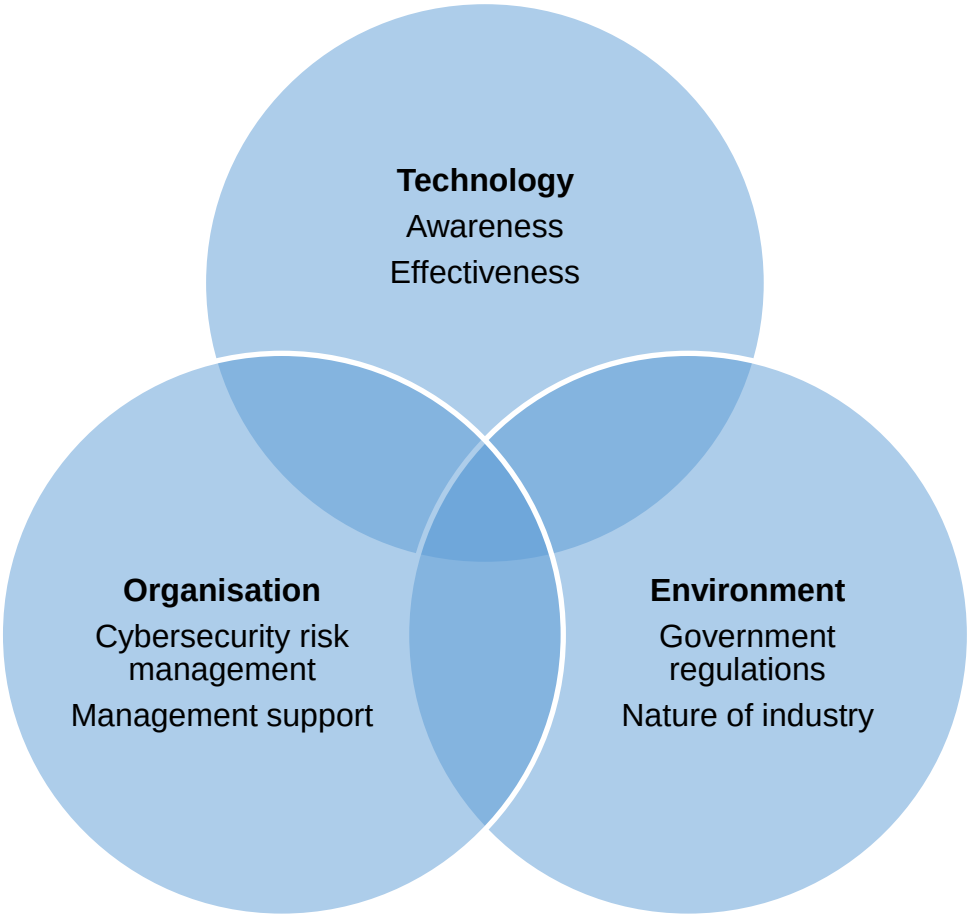



**Figure 2**: TOE Framework Adapted from (Bandyopadhyay, 2012a)

As depicted in figure 2 above, the study will be underpinned by technological, organisational and environmental factors to ascertain the inclination of South African firms to make decisions on cyber insurance adoption as a means to transfer cyber risk to a third party insurer. Cyber insurance adoption in conjunction with the existing cybersecurity controls delivers maximum value for the organisation (Woods & Simpson, 2017).

In the technology context, the study will ascertain whether the company has cybersecurity technologies deployed, how effective it is and how dependent is the organisation on the technology to mitigate against cyber threats. The organisation context explores the risk appetite to determine the extent to which the organisation approaches risk management from an integrated point of view. The study determines the extent of the availability of financial resources to support cybersecurity initiatives to manage cyber risk. Finally, the environmental context considers the extent to which regulatory needs, nature of business and communities of interests play a role in the cyber insurance decision-making.

## 2.4 Linking cybersecurity to digital technology

The growing reliance on digital technologies, while creating significant opportunities for innovation, convenience, and efficiency, comes with digital security and privacy protection risks (OECD, 2018). There is consistency with Toregas & Zahn (2014) view that the losses incurred from cyber-attacks are growing as new technologies spread and reliance on technology increases. The spread of new technologies such as Cloud computing, mobile devices, and social media increases vulnerability to cyber-attacks (Toregas & Zahn, 2014).

Cybersecurity risks are likely to significantly increase business processes become automated, IT assets becoming acquired and businesses placing reliance on IT to achieve their strategic objectives (Bandyopadhyay, 2012b). As such, the focus of organisations lies in using those technologies to enhance the efficiency of their business, not security. The introduction of digital technologies such as Cloud computing, the Internet of Things (IoT), BlockChain, Big Data, and other emerging technologies has extended the cybersecurity landscape due to

unknown vulnerabilities that attackers could exploit (Sommerrock et al., 2018). Cloud computing is services that facilitate the access by consumers to virtual resources that are scalable and dynamic through the Internet from data centres located across the world anytime with any device (Bahrami & Singhal, 2015). There are three types of Clouds i.e. Public, Private and Hybrid which are delivered through the following service models i.e. Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) (Ratten, 2016).

Cybersecurity is a dynamic field that is ever-changing however companies have not caught up with the rate at which new digital technologies are developing and as such cyber-attacks are increasing with vigour and sophistication (Huang et al., 2018). Network security continues to be a challenge for managers and executives due to manifestations of malware that compromise unprotected assets and thus results in security incidents (Yang & Lui, 2014.; Zou et al., 2016). Aloul (2012, p. 2) state that there are seven causes of increased security incidents world-over, namely:

a) increase in electronic data,
b) increase in mobile devices,
c) increase of organised cybercrime groups,
d) increase of intelligent external and internal IT security threats,
e) the difficulty of tracing the attackers,
f) limited cybercrime laws, and
g) limited IT security knowledge among internet users

### 2.4.1 *Increase in electronic data*

According to a study conducted by IDC (2018), the Global Datasphere will grow to 175 Zettabytes by 2025, wherein 49 per cent of data will be stored in public cloud environments. The Global Datasphere quantifies and analyses the amount of data created, captured, and replicated in any given year across the world. Additionally, it looks at how much of that data is stored across various storage components (HDD, flash, optical, tape, and memory).

Figure 3 below illustrates the upward trend that suggests that the world will experience exponential growth in terms of the size of the global Datasphere.

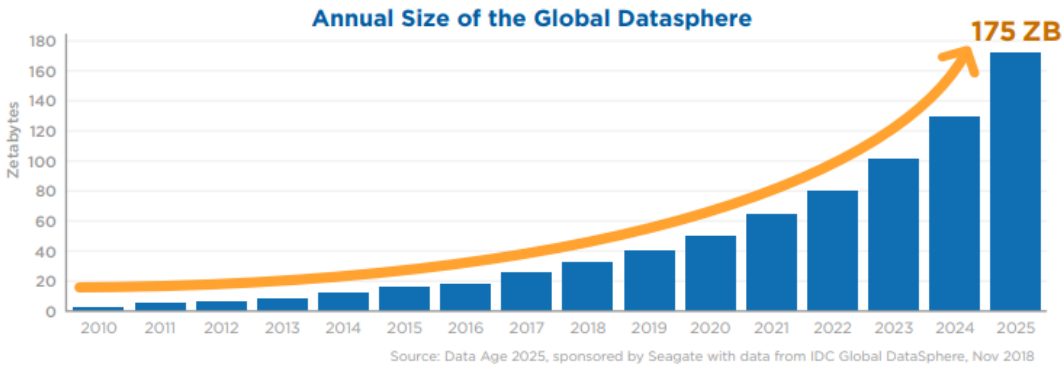



**Figure 3**: Anticipated Projection of global Datasphere Source: (IDC, 2018)

Figure 3 above suggests that as the data grows exponentially, cybersecurity controls must follow a similar path to secure organisational assets. The IDC (2018) report suggests that the increase in data transactions requires organisations to continuously learn and make improvements based on the data.

The factors behind data increase include autonomous cars, humanoid robots, intelligent personal assistants and smart home devices that are shifting how we work, live and play (IDC, 2018). This signals that data will continue to increase and will require modern and effective security mechanisms to secure data stored in cloud storage or internal servers at rest as well as in motion.

### 2.4.2 *Increase in mobile devices*

According to Lee, Cheng & Cheng (2007), the increase in mobile devices has resulted in the creation of economic value. It is estimated that mobile commerce accounts for US6.9 trillion e-commerce by 2004 and that's a sizeable amount by any account (Lee et al., 2007). This increase is attractive for hackers to target mobile devices for malicious intents (Sujithra et al., 2015).

Figure 4 below illustrates the global Internet Protocol (IP) traffic, wired and wireless. The wireless traffic includes both Wi-fi and mobile traffic highlighting exponential growth on both.

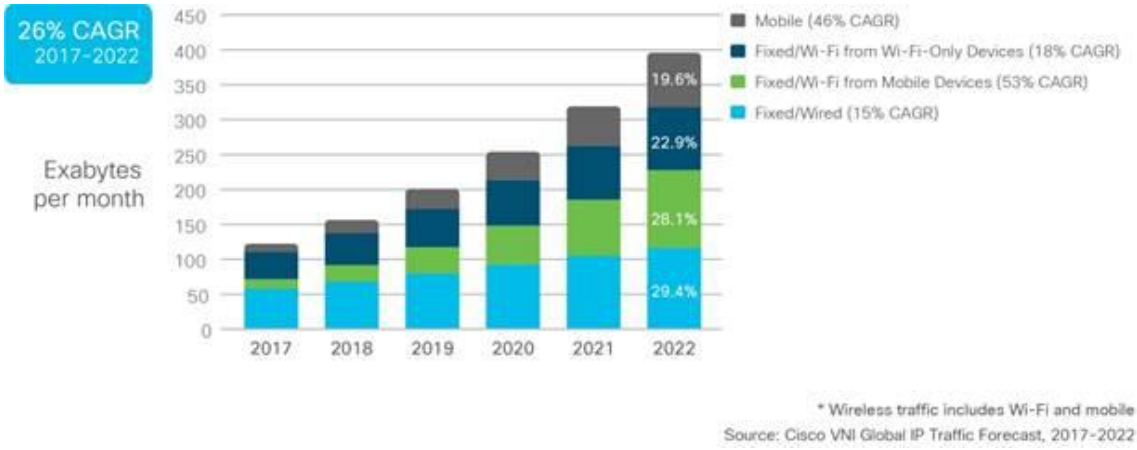



**Figure 4**: Global IP traffic, wired and wireless Source: CISCO Visual Networking Index (2018)

Figure 4 above illustrate the Global IP traffic from the study conducted by CISCO, a global network firm. By 2020 it is predicted that wired networks will constitute 29 per cent of IP traffic, and Wi-Fi, as well as mobile networks, will account for 71 per cent of IP traffic ('Cisco Visual Networking Index', 2018). This view correlates with the increase in mobile devices and as such, mobile devices are likely to become targets for cybersecurity attacks (Pescatore, 2017).

The increase in broadband penetration in South Africa promises to stimulate economic activity and at the same time could expose the citizens to cyber-attacks (Mooketsi, 2015). Malicious actors could use the country's cyberspace as a launching pad for cyber-attacks to the rest of the world (Jardine, 2015). As technology keeps advancing, so are cyber threats that could impact South African organisations negatively resulting in financial losses and damage to reputation (Van Niekerk, 2017).

Figure 5 below illustrates the number of Internet users for selected countries. The countries listed in figure 5 below relate to the developing world, particularly the developing nations. Africa is an attractive destination for cyber-attacks as more and more users have access to the internet (Kshetri, 2019). Globler & Dlamini (2012, p. 1) state that *factors making Africa vulnerable include increasing bandwidth, increasing use of wireless technologies and infrastructure, high levels of computer illiteracy, ineffective or insufficient legislation to deal with cyber-attacks and threats, as well as increasing Internet penetration rates.*

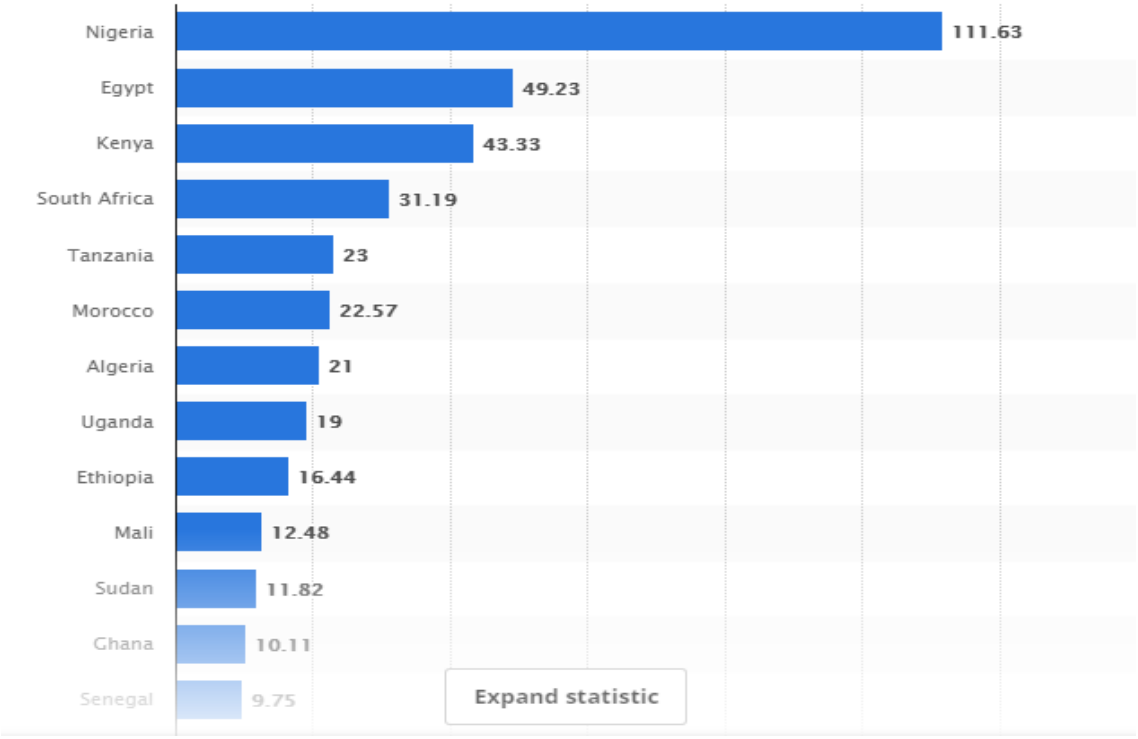



**Figure 5**: Internet users in selected countries in Africa Source: Statista (2019)

According to March 2019 data from Statista (2019), South Africa is ranked number four in terms of the number of Internet users with 31.19 million. Nigeria has 111.63 million, followed by Egypt at 49.23 million and Kenya with 43.33. Majority of the Internet traffic was generated with mobile phones. This can be attributed to the fact that mobile connections are much cheaper compared to the infrastructure associated with traditional PC such as fixed-line internet connection.

The increase in broadband penetration has the potential to leave the country's Internet infrastructure vulnerable (Manda & Backhouse, 2017). Thus, a coordinated effort from all stakeholders such as national government, business, academia, etc. to develop and implement a robust cybersecurity policy framework is necessary.

### 2.4.3 *Increase in organised cybercrime groups*

According to Raghavan & Parthiban (2014, p. 2) *cybercrime is a growing threat in the virtual world as the use of the internet and other digital technologies growth*

*thereby heightening the risk of attack by cybercriminals across the globe*. Cybercrime, in the most trivial form, *is a crime that occurs in a computer and a network* (Sharma et al., 2016, p. 1). *Cybercrime involves using computers and the Internet by individuals to commit crimes* (Hassan et al., 2012, p. 1). Cybercrime activities involve the use of communication devices such as computers, telephones, cellular and other technological devices for illicit ends such as theft, fraud, violating property rights, electronic vandalism and unauthorised access to computer systems and networks (Kshetri, 2015a). According to Hassan et al. (2012, p. 1) *cyber terrorism, identity theft, and spam are identified as types of cybercrimes*.

Cybercrime's increase has been driven by the amplification and opportunities provided by Internet penetration mostly in developing economies (Broadhurst et al., 2014). Broadhurst et al. (2014) state that such an increase, as well as advancement in digital technologies, can attract a range of various criminal actors as hacking tools has become accessible to the general public (Kumari & Mohapatra, 2016). Cybercriminals are much more organised these days as they share knowledge and resources such as stolen confidential data, extracts of code or hacking tools in exchange for financial gain or other virtual goods (Lavorgna & Sergi, 2016). Due to the lucrative nature of cybercrime, *some hackers use communities such as online platforms to organize into groups and launch sophisticated, financially-motivated cyber-attacks* (Benjamin & Hsinchun Chen, 2012, p. 1).

According to Aloul (2012), most governments in the world are introducing laws to combat computer crime, also known as e-crime or cybercrime. The impact of cybercrime is a concern in the modern business environment for most executives. In 2009, the global cybercrime topped $1 trillion (Anderson et al., 2013). That figure has significantly increased over the years to a couple of trillions. It was predicted that the cost of cybercrime is likely to rise from $3 trillion in 2015 to $6 trillion in 2021 with one-third of companies being affected by cybercrime (32%) (Huang et al., 2018). Von Solms & van Niekerk (2013) conclude that the victims of cybercrime are not just companies whose intellectual property is compromised

but extend to broad stakeholders within the value system such as customers, partners, and service providers.

### 2.4.4 *Increase of intelligent external and internal IT security threats*

Chou (2013, p. 5) states that *security threats can occur from both outsides of and within organizations*. According to the 2019 SolarWinds cybersecurity survey conducted on 200 US federal government, IT decision-makers and influencers, 56% of security threats emanated from careless/untrained insiders (SolarWinds Federal Cybersecurity Survey Report, 2019). Figure 6 below illustrates the sources of security threats emanating from the SolarWinds report.

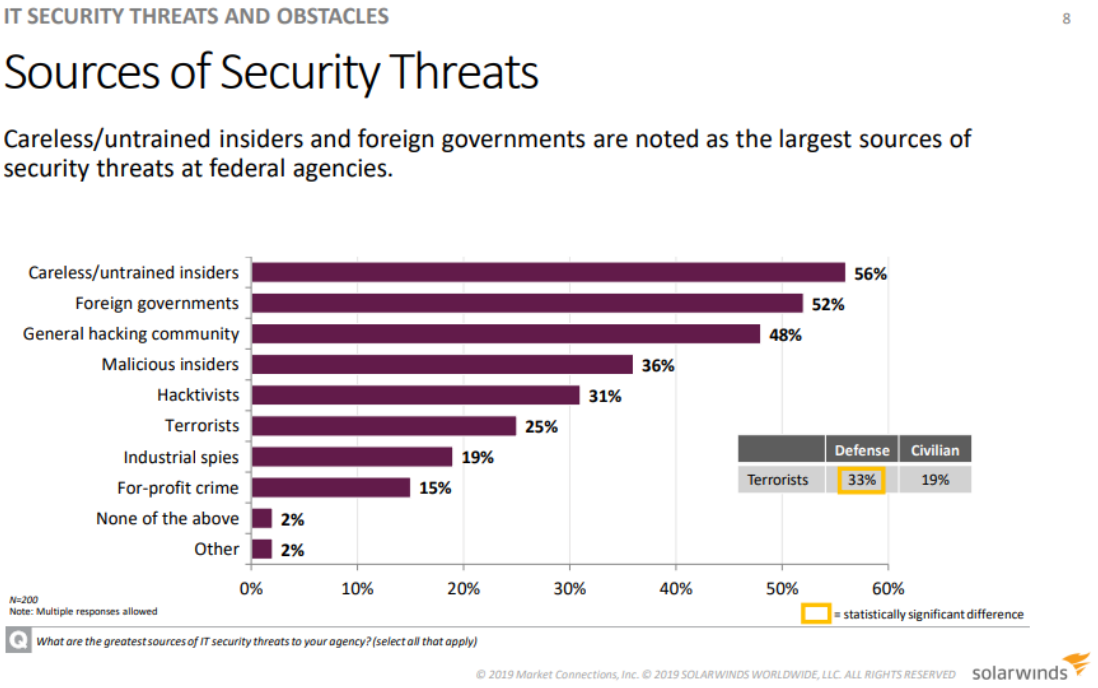



**Figure 6**: Federal cybersecurity survey report. Source: SolarWinds (2019)

About 43% cited lack of employee training/awareness, 41% indicated the increase in the number of devices with access to data and 40% volume of network activity were noted most often as reasons for difficulties with careless or malicious insider threats. The report puts forward that 35% of respondents indicated a lack of IT/security staff to be a challenge that requires urgent attention. About 31% of respondents highlighted the increase in the use of cloud apps and 24% cited

infrastructure as one of the top reasons for malicious threats that are large because of contractors having access to systems.

Cloud computing provides necessary flexibility and efficiencies from storage, processing and cost perspectives, however, sensitive data residing on clouds may be exposed to cyber theft if not adequately secured (Chou, 2013). IDC (2018) report highlight the threats such as the Distributed Denial-of-Service (DDoS), ransomware, botnet, spam, spoofing, phishing, Advanced Persistent Threats (APTs), viruses, worms, hacktivism, spyware, malware and state-sponsored cyber warfare to be increasing cyber risk for users and companies.

According to the 2019 Verizon Data Breach Investigations Report (DBIR), conducted on close to 42000 security incidents and over 2000 data breaches provided by over 70 data sources, both public and private entities, across 86 countries worldwide (*DBIR, 2019)*. About 69% perpetrated by outsiders with 39% of breaches are due to organised crime groups and 23% to nation-states or state-affiliated actors. About 52% of breaches featured hacking, 33% included social attacks and 28% malware attacks. About 43% of breaches involved small business victims, 16% public entities, 15% healthcare, and 10% financial industry. The financial gain represented the biggest driver of data breaches with 71%, followed by 25% breaches motivated by espionage.

### 2.4.5 *The difficulty of tracing the attackers*

The escalating rate of cyber incidents and the associated cyber risks impact negatively on the company brand, reputation, and financial stability of the organisation (*ISACA*, 2016). In spite of the advancement in cybersecurity protective technology, organisations are unable to keep up with the rate of emerging cyber risks (Yang & Lui, 2014). The prevalence of cyberattack tools makes it easier for an attacker to launch an attack with a limited chance of being caught (Sawyer & Hancock, 2018). Cyber-attack can be remotely conducted and automated to multiple victims due to sophisticated attacks thus tracing the true source can be time resource-intensive in terms of time and effort (Kumar & Carley, 2016). This is heightened by the use of Darknet by attackers to hide to their true source (Choi et al., 2013) and the weakness of cyber defence by most

organisations (Goel & Mehtre, 2015). Darknet typically comprises of a network of computers with the anonymised identity of individuals and devices that spans multiple geographies (Arizona State University et al., 2019).

*"Cybercrime exploits cross-national differences in the capacity to prevent, detect, investigate, and prosecute such crime, and is fast becoming a growing global concern"* (United Nations, 2004; Broadhurst et al., 2014, p. 3). In order to track and trace the source of the attack, a different approach is required and includes cooperation and partnership amongst nation-states (Bossong & Wagner, 2018). Intervention could include coordinated breach reporting, effective prosecution, and long jail terms. An Internet-based collaborative environment to protect critical infrastructure such as financial institutions, telco providers, etc. from coordinated cyber-attacks for organisations operating in geographically dispersed locations is another alternative (Hung, 2016).

The cyberspace anonymity poses a challenge and makes geography inapt as cybercrime does not occur within the territory of a single country thus an attack could be launched anywhere and the victims could be in any other part of the world (Brenner, 2006; Nawang, 2017). This view is consistent with Lipson (2002, p. 18) who posit that "*the anonymity enjoyed by today's cyber attackers poses a grave threat to the global information society, the progress of an information-based international economy, and the advancement of global collaboration and cooperation in all areas of human endeavour*." Due to the Internet's limitations, it is time-consuming to build anomaly detection models to detect unknown attacks due to low detection accuracy (Choi et al., 2013).

### 2.4.6 *Limited cybercrime laws*

According to Arfi & Agarwal (2013, p. 1), *cybercrime is a kind of crime that happens in "cyberspace", between computers and the Internet*. Most people have little or no knowledge of cybercrime due to lack of awareness as well as sufficient regulatory framework (E Kritzinger & Solms, 2013) and its potential severe impact on society at large (Arfi & Agarwal, 2013) which includes the direct cost of victimisation, emotional harm, and associated costs (Hutchings, 2014). Cybercrime actors are not easily identifiable due to false identities they use online

(Goldman & McCoy, 2016). There is no link between the real person and the perpetrator, as a result, poses a challenge to identify, arrest, and prosecute cyber criminals that are mostly outside of the law enforcement jurisdiction (Bayoumy, 2018).

According to Armstrong & Forde (2003, p. 1) "*money laundering, drug dealing, terrorism, hacking, fraud, child pornography and the distribution of objectionable material are crimes that are perpetrated using the Internet*." This view is supported by Arfi & Agarwal (2013, pp. 1–2) who state *cybercrimes are "committed through the use of computer and Internet remotely and include child pornography, cyber laundering, cyberstalking, cyber terrorism, cyber theft, and spam*." These crimes can be categorised into two parts i.e. local cybercrime and transnational cybercrime (Dupont, 2018). Local cybercrime physically occurs in the same sovereign territory and transnational cybercrime occurs in different territories for both the perpetrator and the victim.

South Africa has enacted statutes such the Electronic Communications and Transactions Act (ECT), Minimum Information Security Standard, the Regulation of Interception of Communications and Provision of Communication-related information Act, Protection of Personal Information Act, Cybercrimes and Cybersecurity Bill, etc. to regulate and counter effect of the cyberattacks (ww.*justice.gov.za*, 2019). South Africa has the responsibility to promote cybersecurity awareness as the State can be held liable for cybercrimes emanating inside the country (Grobler et al., 2012). This is due to the international treaties that the country has signed which oblige the country to fulfil its commitments hence the national cybersecurity policy framework.

### 2.4.7 *Limited IT security knowledge among internet users*

Lack of cybersecurity awareness is a concern for organisations in all sectors as security is multi-faceted and requires diverse expertise to effectively manage the risk (Hanus & Wu, 2016). This is probably the biggest challenge faced by organisations. As such, a security policy can only be effective if an organisation engages its staff on security awareness that is understandable and employees accept necessary precautions. According to Shaw, Chen, Harris, & Huang

(2009), security awareness is about users understanding and appreciating the importance of cybersecurity as well as their individual and collective responsibilities in line with approved policies to protect company assets (Collins, 2017). Increasing concerns include but not limited to sharing of corporate computing resources with non-employees, using corporate computing resources for non-work related tasks, downloading and installing unsupported and pirated software, opening unsolicited email and attachments.

Inadequate understanding of security can expose the organisation to security threats and vulnerabilities that can lead to security incidents (Muller, 2015). In order to protect organisational assets and profits, organisations must intensify efforts for improved information security by instituting cybersecurity awareness programs to ensure that employees are informed of cybersecurity risks (Gcaza & Solms, 2017). This could be an effective mechanism to lessen the rising threat of cybersecurity breaches and attacks on company infrastructure. In order to ensure holistic awareness and understanding of security threats facing information assets of the organisation is achieved, security awareness must be extended to individuals tasked with managing information security (Tianfield, 2016). Susanto & Almunawar (2012, p. 4) state that "*security awareness means stakeholders comprehend that there is the potential to deliberately or accidentally steal, damage, or misuse the data that is stored in a company's computer system*." Thus, protecting the company's assets (information, physical and personal) from any possible security breach is significant for the continuing sustainability of the organisation.

Education and training must inform employees' actions in terms of do's and don'ts as well as initiate activities to protect against policy violations and must become a formal daily task of employees in an organisation (Crumpler & Lewis, 2019). This must be done in a coordinated and on-going fashion in order to inculcate the right culture within an organisation (Sutherland, 2017). As drivers of change management and culture, top management play a significant role in ensuring organisational security level through planning and reasonable resource allocation (Larson, 2015).

### 2.4.8 *Proposition 1*

The awareness of effective cybersecurity technology controls complement cyber insurance to reduce the impact of cyber-attacks in the South African industry.

## 2.5 Cyber risk management

Gordon, Loeb, & Sohail (2003, p. 1) state that the use of "*the Internet has significantly increased the vulnerability of organisations to information theft, vandalism, and denial-of-service attacks, thereby bringing information security issues to the forefront of the agenda for corporate executives*." This suggests that cyber risk is quite high on the agenda for executives as risk management is interlinked with the long-term sustainability of the company. Bouveret (2018, p. 12) defines *risk* "*as a combination of consequences and likelihood where the likelihood is a function of threat levels and the ease of exploitation of existing vulnerabilities*":

Risk = f (Threat, Vulnerability, Consequences)

According to Gordon et al. (2003, p. 3) cyber risk is "*the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk*". Cyber risks are defined as "*operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems*" (Eling & Wirfs, 2015). Therefore, cyber risk is a major concern among public and private corporations due to its systemic nature and must be managed as such (Bouveret, 2018).

According to Toregas & Zahn (2014), cybersecurity is a business problem and requires that senior IT executives translate the risks of cyber-attacks into numbers that contribute to providing objective information as opposed to common "*fear, uncertainty and doubt*" tactic that IT security personnel employs. Bohme & Schwartz (2010) state that cyber risk must be managed through the usual approach to business risks i.e. eliminate, mitigate, absorb and transfer.

Business risk landscape has increased significantly with the use of the Internet as more and more services are accessible online.

As depicted in Figure 7 below, the cyber-risk management framework requires a risk assessment to take place to determine the high-value vulnerabilities that should receive security resources.

To optimally assess the risk and determine cost-benefit for security investment Gordon, Loeb & Sohail (2003) suggest that a value-vulnerability grid should be used. Figure 7 below illustrates a value-vulnerability grid.

| | | Vulnerability | | |
|---|---|---|---|---|
| | | **High** | **Medium** | **Low** |
| **Value** | **High** | 1 | 2 | 3 |
| | **Medium** | 4 | 5 | 6 |
| | **Low** | 7 | 8 | 9 |

**Figure 7**: Value-vulnerability grid Source: Adapted from (Gordon et al., 2003)

In order to effectively leverage scarce information security resources, "*information falling into boxes 1, 2, 4 and 5 should generally receive the largest share of the information security budget"* (Gordon et al., 2003, p. 4). The priority boxes mentioned above indicate medium and high ratings for both the value and vulnerability hence focused security investments.

Kopp et al. (2017, p.2) posit that "*firms must actively manage cyber risk and invest in cybersecurity, and to some extent transfer and pool their risks through cyber liability insurance policies*." As such, Toregas & Zahn (2014, p.5) proposes a return on security investment (ROSI) to measure which takes into account that "*security is not usually an investment that provides profit but loss prevention*".

Gordon et al. (2003) argue that the higher levels of security protection will require lower levels of cyber-risk insurance (and vice versa). Hence cyber insurance, the transfer of financial risk associated with network and computer incidents to a third party (Bohme & Schwartz, 2010; Franke, 2017). Figure 8 below illustrates the cyber insurance decision plan:




**Figure 8**: Cyber insurance decision plan Source: Adapted from (Gordon et al., 2003)

According to Gordon et al. (2003), a logical cyber insurance decision plan needs implementation and managerial support. The associated steps include conducting an information security risk audit, assessing current coverage, examining available policies, and selecting a policy.

### 2.5.1 *Cyber insurance as a mechanism to manage cyber risk*

Cyber insurance risk policies provide cover for losses that occur as a result of information security beaches (Gordon et al., 2003). Cyber risk possesses unique qualities, including interdependent security and correlated failure. (Vicevich, 2018). Losses due to cyber risk are frequently small and independent but they could also have a low frequency and a high impact ('blackout scenario') (Bouveret, 2018). A cyber-attack can result in data loss, reputation loss, and hinder a business from performing its operational activities thus impact the financial performance of the organisation (Joshi, Joshi, & Mittal,2019). Therefore, hacking plays a significant role in cyberattacks on organisations.

While security protection measures may limit cyber-attacks, an alternative way to manage risk is to transfer the risk to the cyber insurance service provider in the exchange of paying a premium (Yang & Lui, 2014). Therefore, cyber insurance can be an effective instrument to transfer cyber risk and complement the benefits from technological controls that safeguard the information and network assets in organisations (Bandyopadhyay, 2012b, p. 1).

Cyber insurance can improve cybersecurity through the adoption of best practices that could be required as a caveat prior to insurance coverage (Kesan et al., 2005; Kesan & Hayes, 2017). It assists in ensuring that companies appreciate decent security controls and the cost of lack of good security thereby

resulting in larger investment and enhancements in cybersecurity. To achieve the above-stated objective, cyber insurance can add value in pre and post-breach perspectives.

### a. Pre-breach

It is suggested that policies must offer premium reductions or discounts for taking actions that reduce the probability of a loss as a result of the cyber risk (Gordon et al., 2003). Cyber insurance can be used as an incentive to improve information security posture within an organisation (Khalili et al., 2018). This will serve as an incentive for organisations to take coverage for cyber risks. Various models are suggested, such as partnerships between Original Equipment Manufacturer (OEM) and insurance companies to provide benefit to client organisations (Sommerrock et al., 2018).

Insurers can work with companies to design bespoke cyber insurance products thereby increasing awareness, improving the information security posture, assess clients' contingency plans, train personnel, or recommend best practices to reduce the effect and fix the breach. This proactive approach will result in a reduced security incident when it occurs.

### b. Post-breach

A growing trend of the partnership between cyber insurance and third-party service providers (such as OEM, specialists and security experts) is taking shape in the industry to collaborate for loss prevention and post-breach services (Camillo, 2017). According to Herr (2019, p. 1), *AIG partners with cybersecurity service providers such as CrowdStrike and Darktrace to make risk assessments of their clients (Business Wire Staff 2017)*.

In figure 9 below (Bandyopadhyay et al., 2009, p. 3) provides a high-level in the cyber insurance claims process. Post-breach, insurers offer a number of services to insureds (customers), such as crisis management, IT forensic, security advice and legal consultation.

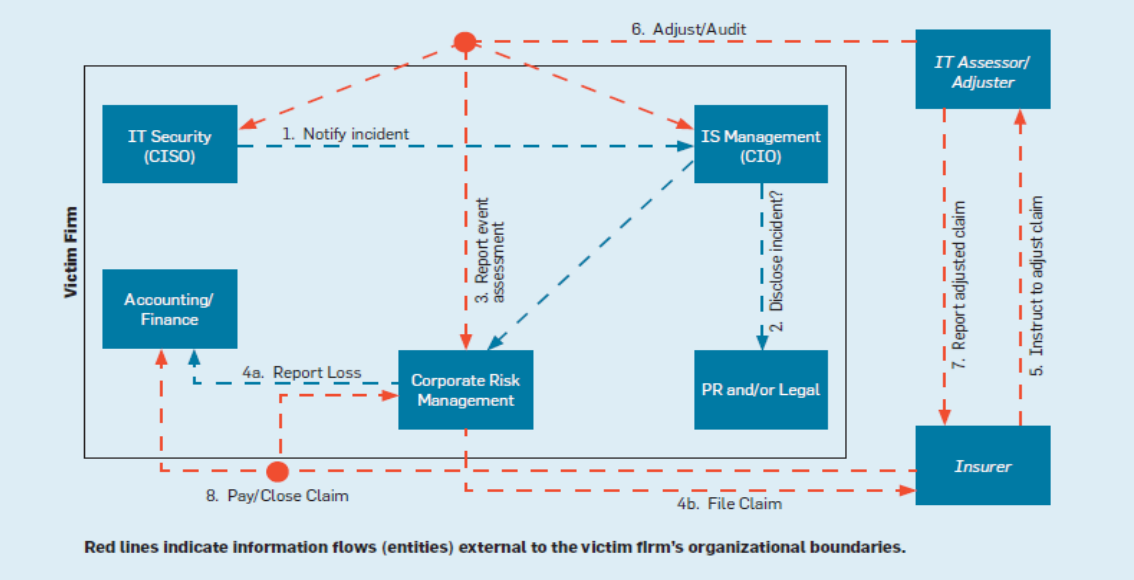



**Figure 9**: Proposed cyber insurance claims process Source: (Bandyopadhyay et al., 2009)

Figure 9 above illustrate an eight-step process to be followed when processing a cyber insurance claim (Bandyopadhyay et al., 2009). According to Sommerrock et al. (2018), insurance policies provide services that evaluate the impact, investigate the attack, and incident response and recovery plans, provide forensics, public relations and communications support, notify customers, and identify appropriate mitigating actions to strengthen resilience in the future (Woods & Simpson, 2017).

First, when the cyber incident occurs, the CIO is notified of the by the CISO. Thereafter the matters are disclosed to legal to obtain an opinion and public relation to managing communication to external stakeholders. The events are then reported on the corporate risk management's risk register and report the loss to the finance unit. Woods & Simpson (2017) adds that insurer partner with cybersecurity experts to limit the impact after the cyber-attack and strive to institute the cause and extent of the loss prior to underwriting the policyholder.

The claim is filed to an insurer who then appoints an IT assessor/adjuster who then adjusts/audits the claim and notifies the CIO, CISO and the corporate risk management unit. As part of cyber insurance contracts, coverage for losses from other information and network assets could be included as well as the cost of

victim notification, liability compensation and cyber extortion (Bandyopadhyay, 2012b). The assessor notifies the insurer who then decides on whether to pay/close the claim.

### 2.5.2 *Cyber risk in South Africa*

According to statistics from the South African Banking Risk Information Centre (SABRIC), in 2017 there were 13,438 incidents across banking apps, online banking, and mobile banking which cost the industry more than R 250 000 000 in gross losses (‘Digital Banking Crime Statistics’, 2019). Incidents from January to August 2018, demonstrate a 64% increase in gross loss. However, when comparing January to August 2017 to the same period in 2018, mobile banking incidents showed an increase of more than 100%, with gross losses of R23 593 631, while online banking incidents showed an increase of 44% with gross losses of R89 368 722.

For the same period, banking app incidents increased by 20%, with gross losses of R70 156 364. SIM swops saw 4040 incidents from January to August 2017, and 8254 incidents from January to August 2018, an increase of 104%. Modus operandi includes social engineering, phishing, vishing or the installation of malware onto a victim’s device by having them click on a link, enabling the criminal to steal sufficient personal information to access their online banking profile. According to SABRIC, there is an upward trend in the following frauds:

a) Phishing, Vishing & SMishing
b) SIM Swops
c) Change of Bank Details Scam
d) Email Hacking

According to the IBM (2017) cost of data breach study conducted to 419 companies in 11 countries and two regions, South Africa’s loss is estimated at $128 million for FY2017 which is higher than the four year average of $115 million. The study predicted that organisations in South Africa, India and Brazil are most likely to experience a material data breach involving 10,000 or more records over the next 24 months with South Africa having the highest probability

of experiencing a data breach. As such companies such as Liberty, ViewFines, City of Johannesburg, etc. have experienced a data breach in the aforementioned period (Moyo, 2018). According to the report from (Fin24.com, 2018), there were five data breaches affecting South Africans i.e.

a) Liberty email hack
b) ViewFines licence details
c) Facebook scandal
d) Master Deed's data breach "biggest" digital security threat in SA
e) Ster-Kinekor's database compromised

### 2.5.3 *Proposition 2*

An organisational approach to cybersecurity determines cyber-risk management support.

## 2.6 Cyber insurance market

Cyber insurance is defined as "*the transfer of financial risk associated with network and computer incidents to a third party*," the insurance company, in exchange for a premium (Toregas & Zahn, 2014, p.6). Toregas & Zahn (2014) posit that the market for cyber insurance policies is at its infancy and expected to grow in the future. According to (Bandyopadhyay, 2012b, p. 1), *cyber insurance refers to the specific insurance contracts that provide coverage against loss from theft of data and IS assets*.

To complement security protective technology, the residual risk that remains is transferable to a cyber insurance provider. As such, the cyber insurance market will mature as more corporates begin to see the value it adds to the business. Hurtaud, Flamand, Hounka (2015) state that there has been a steady increase in the size of the cyber insurance market as the U.S. constitutes about 90% of global cyber insurance market with early adopters being financial services companies, retailers and healthcare organisations with large amounts of personally identifiable information (PII).

In comparison to the EU, the growth is due to the mandatory data breach notification laws in the US. Hurtaud et al. (2015) point out that with the adoption of the GDPR, the EU is likely to catch up with US counterparts as there are requirements to speedily notify authorities when breaches to personal data occur.

The cyber insurance market is projected to be a multi-billion dollar industry which is accelerated by the growing cyber-attacks on companies (Herr, 2019). This view is affirmed by further observations that suggest that the market is likely to reach $20 billion or more by 2025 (Camillo, 2017) and over 70 cyber insurance carriers around the world (Khalili et al., 2018). Cyber insurance enables companies to manage cyber risks by transferring part of their risks to insurers in exchange for paying a premium (Kesan et al., 2004; Kesan & Hayes, 2017).

Bohme & Kataria (2006) agrees with the above prediction and augments that American International Group (AIG) and Lloyd's of London are the leading providers of cyber-insurance in the market. Additionally, other prominent market players include Chubb's Cyber Security, AIG's NetAdvantage Security, Hiscox's Hackers Insurance, Legion Indemnity's INSUREtrust, Lloyd's e-Comprehensive, Marsh's NetSecure, and St. Paul's Cybertech (Gordon et al., 2003).

Camillo (2017) contends that the cyber insurance market today has matured substantially and has become specialised and innovative in terms of product and service offerings. This includes products that cater to small- to medium-sized enterprises (SMEs), the mid-market sector as well as very large multinational corporations. The insurance industry recognizes cybersecurity as an issue at the national and international levels (Vicevich, 2018). As such, companies of all sizes are beginning to appreciate the benefits of cyber insurance as a risk transfer mechanism.

The literature review notes that not all views are uniform and optimistic, particularly earlier studies have divergent views compared to recent studies. Points of divergence on the growth and size of the cyber insurance market are prevalent. For instance, Toregas & Zahn (2014) state that the growth of the cyber insurance market has somewhat been tentative and slow in developed economies such as the US. Gordon et al. (2003) supplement that cyber-risk

insurance is a new product with underwriters being hesitant to offer large policies (relative to traditional insurance).

However, Lloyds offers limits for its e-Comprehensive policy of $50,000,000 and gives custom quotes up to $200,000,000. This observation is consistent with Bandyopadhyay et al. (2009) who posit that cyber insurance products remain underutilized after more than a decade later of commercialisation. This suggests that the forecasting of the evolution of the cyber insurance market needs adjustment.

Since cyber insurance product and service offerings are fairly new in the industry, particularly in the context of South Africa, availability of data on cyber risk and therefore cyber insurance is scarce (Bouveret, 2018). This could be attributed to the fact that institutions that have been compromised do not disclose incidences (Symantec, 2016; Eling & Schnell, 2016). This view is echoed by Bouveret (2018) who states that data on cyber incidents is scarce and therefore limited quantitative analyses of cyber risk.

Lack of common standards to record them is cited as the primary factor, and firms have no incentives to report them (Bouveret, 2018). In the South African context, legislation such as the Protection of Personal Information (POPI) could change that narrative, as firms will be required to report each incident to the regulator (POPIA, 2013). Therefore, residual cybersecurity risks are mitigated using cyber insurance (Bandyopadhyay & Mookerjee, 2017).

Based on the views expressed above, for and against the cyber insurance market size and its potential growth, in South Africa the industry is likely to grow due to the introduction of legislation such as POPI, growing data breaches and cyber-attacks as highlighted above. Indeed, the cyber insurance market is still in its early stages. However, as Eling & Schnell (2016, p.9) point out that *as market development continues, the risk pools will become larger and more data will be available*. Accordingly, future prospects look set to increase upward as the industry matures (Woods & Simpson, 2017).

### 2.6.1 *Types of cyber insurance liability covers*

According to (Hurtaud, Flamand, & Hounka, 2015, p. 3), *cyber insurance can complement an organisation's active security measures by providing insurance coverage in three broad areas:*

a) *Liability for a data breach or loss*
b) *Remediation costs (e.g. for investigating the breach, notifying affected parties, etc.)*
c) *Regulatory fines/penalties and settlement costs*

Camillo (2017) augments that prominent in most cyber insurance policy covers include cyber exposures, which are not included in "traditional" insurance policies (Toregas & Zahn, 2014). Bouveret (2018) states that cyber risk can impact first (the target) and third parties (a counterpart to the target).

According to Gordon et al. (2003, p. 4), the *first-party risk takes place when the insured is faced with the possibility of a loss of profits as a result of the theft of trade secrets, destruction of the property (including hardware, software, and data), and extortion from hackers*. Whereas the third party is due to direct or indirect damage to organisations infrastructure, reputation or revenue because of an attack on systems and data. Table 1 below provides a comparison of different cyber insurance providers, product offering as well as types of policy coverage.

**Table 1: Comparison of cyber insurance policies** (Marotta, Martinelli, Yautsiukhin, & Nanni, 2015)

| | *Coverage* | *Allianz* | *QBE* | *AEGIS* | *CNA* | *InsureTrust* | *CDRM LLC* | *Travelers* | *Zurich* | *ACE* | *Hiscox* | *Insurecon* | *Marsh* | *Chubb* | *AIG* |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| First-Party | Loss or damage to digital assets | x* | x | x | x | x | | x | x | x | x | x | x | x | x |
| | Business Interruption | x* | x | x | x* | x | x | x | x | x | x | x | x | x | x |
| | Cyber extortion | x | x | x | x* | x | x | x | x | | | x | x | | x |
| | Theft of money and digital assets | x | x | | x* | | x | x | x | x | x | x | x | x | |
| Third-Party | Security and privacy breaches | x | x | x | x | x | x | x | x | x | x | x | x | x | x |
| | Computer Foresincs Investigation | x | x | x* | x | x | x | | | x | | x | | | x |
| | Customer notification/PR expenses | x | x | | x | x | x | x | x | x | | x | | x | x |
| | Multi-media liability | x | x | x | | x | | x | x* | x | | | | | x |
| | Loss of third-party data | x* | | x | x* | x | x | x | x | x | x | x | x | x | |
| | Third-party contractual indemnification | | x | | | x | | | x | x | | | | x | |

As can been seen in table 1 above, not all insurance carriers cover the same exposures. Largely, there is a trade-off in terms of the covered risk. Such exposures include loss or damage to digital assets, data recovery, business interruption, notification costs, liability in respect of data breaches, multimedia liability, employee dishonesty, cyber extortion and regulatory defence costs (Camillo, 2017, p. 4). Figure 10 below illustrates the most covered losses due to cyber-attacks.

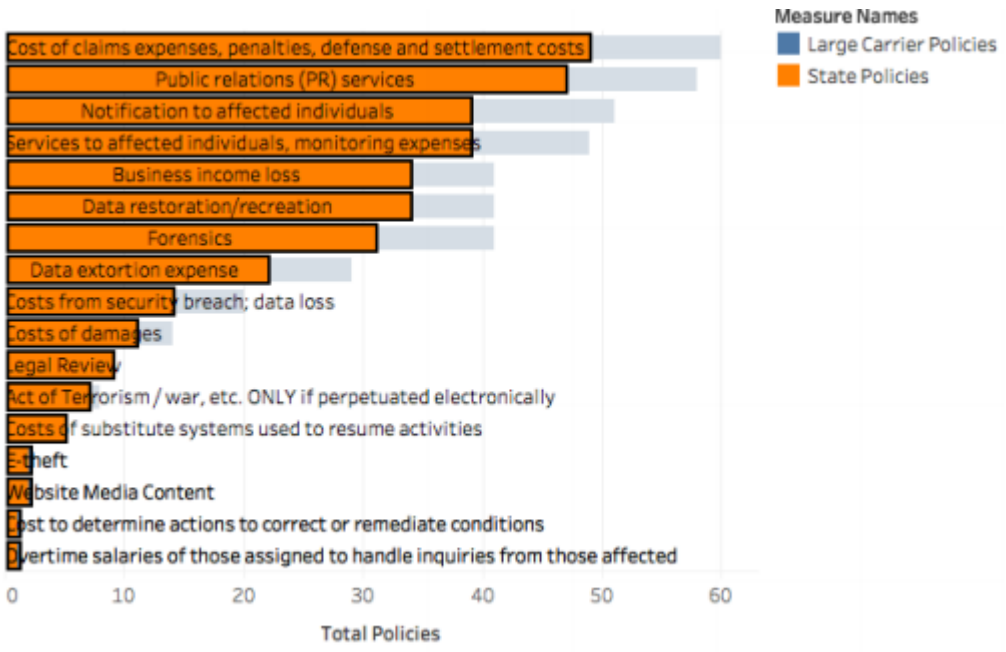



**Figure 10**: Most covered losses Source: (Romanosky et al., 2019)

As shown in figure 10 above, the top five most covered losses are the cost of claims expenses, penalties; public relations services; notification to affected individuals; service to affected individuals and business income loss (Romanosky et al., 2019). With the exception of business income loss, the top four covered losses relate to external stakeholders.

According to Romanosky et al. (2019) cost of claims, expenses related to penalties, defence and settlement costs whereas public relations services include advertising or special promotions as well as media briefing. It is unsustainable to cover all possible risks; figure 11 below illustrates the cyber insurance exclusions.

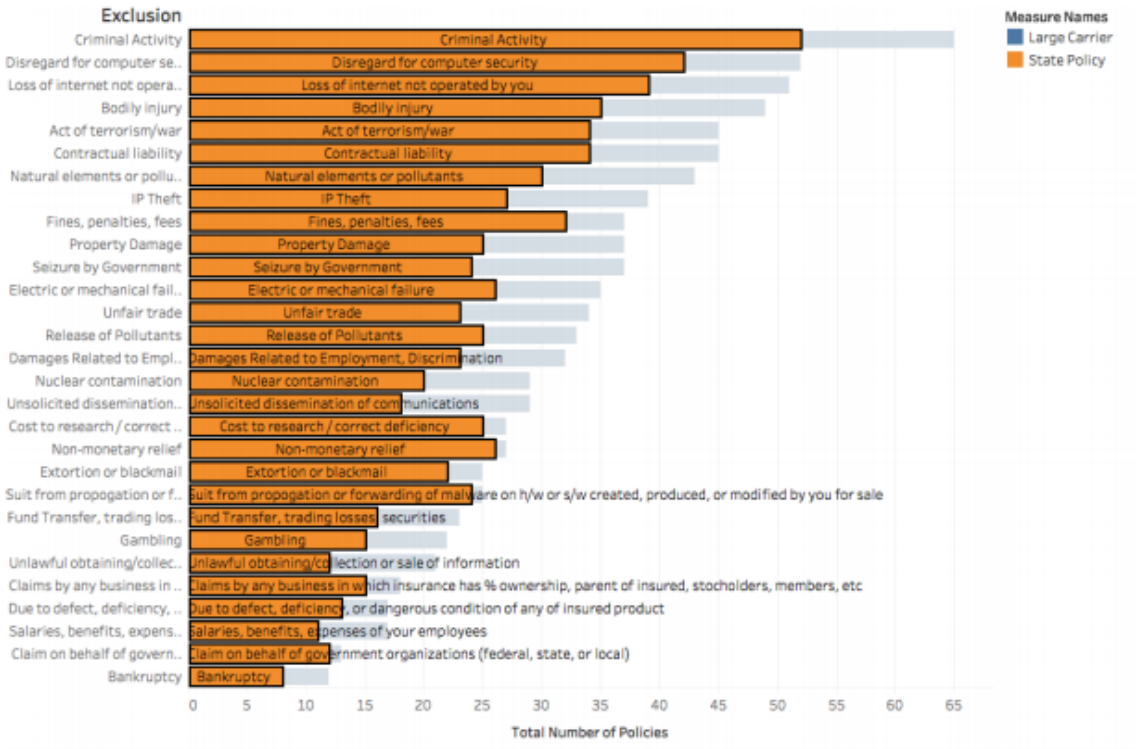



**Figure 11**: Policy exclusions Source: (Romanosky et al., 2019)

According to Romanosky et al. (2019, p. 15), *most exclusions relate to criminal, fraudulent, or dishonest acts, errors or omissions, intentional violation of a law, any ongoing criminal investigation or proceedings, and payment of fines, penalties, or fees*. Additionally, some policies provide further exclusions for infringement of patents, disclosures of trade secrets or confidential information, or violations of securities laws.

The cyber insurance market faces various challenges, with the setting of premiums being one of the biggest issues (Toregas & Zahn, 2014). This view is exacerbated by the belief, as Toregas & Zahn (2014) point out, that risks associated with cyber-attacks are not quantifiable and thus, not insurable. Vicevich (2018) concludes that the insurance industry is unable to pool risk. Figure 12 below illustrates the cyber insurance premiums.

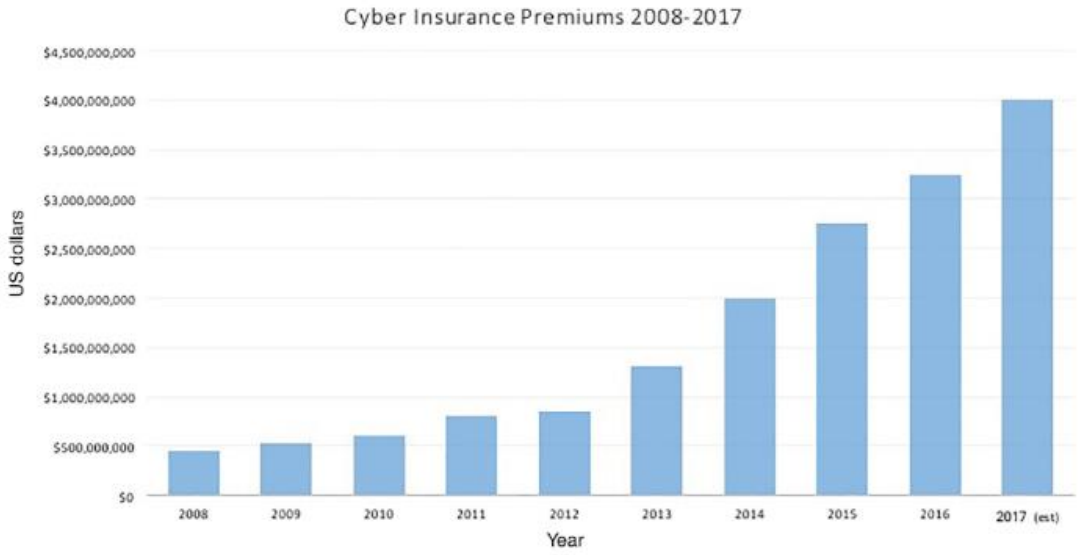



**Figure 12**: Cyber insurance premium Source: (Herr, 2019)

As shown in figure 12 above, there has been an exponential growth in the cyber insurance premium. Between 2012 and 2014 there was an exponential growth of 300% wherein the total premiums from coverage jumped from US$835 million to US$2 billion in 2014 and an estimated US$4 billion in 2017 (Knockless 2015; Herr, 2019). It is suggested that exponential growth was due to demand from small and medium companies. Over 90% of insurers noted growth in demand between 2012 and 2014, mainly from the retail sector (Advisen Ltd. 2014, pp. 4–5; (Herr, 2019, p. 9).

### 2.6.2 *Drivers of cyber insurance*

A growing appreciation of cyber vulnerabilities did not immediately translate into demand for insurance (Camillo, 2017). Despite the awareness of the cyber risks and risk damage they can cause to the organisation, investment in security, as well as availability of cyber insurance, is still scarce thus the rampant cyber-attacks (Yang & Lui, 2014). Cyber insurance is the outsourcing of low frequency, high impact risk (Mukhopadhyay et al., 2013). An opportunity exists for institutions, insurers, legislators, and regulators to create an environment conducive for information sharing for reporting. Firms that are prone to cyber-attacks are more likely to take the cyber insurance (Gordon et al., 2003).

Organisations can adopt cyber insurance as a management tool for reducing the risk of financial losses associated with Internet-related breaches.

Cyber insurance plays an important role in improving the cybersecurity control environment and it mutually beneficial for both the insurers and insureds (Woods & Simpson, 2017). Policy-makers and well as insurance providers have a role to play in the sustainability of the cyber insurance industry. Woods & Simpson (2017, p. 3) posit that a fragmented policy landscape could provide an additional barrier to the growth of the market. Therefore, public-private partnership is essential to ensure that there is a consideration of the interests of all stakeholders in development cybersecurity insurance market and policy measures. Cyber insurance investment translates to improved security due to the adoption of more secure practices within an organisation thereby reducing cyber risks (Kesan & Hayes, 2017).

Organisations are beginning to appreciate the value that the cyber insurance provides i.e. financial cover in the event losses occur due to a security incident (Joshi, Joshi, & Mittal, 2019). This assists an organisation to safeguard against the threat posed by the malicious actors. Joshi et al. (2019) do, however, point out that in order for the cyber insurance to increase adoption by companies, disagreements on coverages and exclusions rules needs to be addressed between insurance providers and insured customer. It can be deduced that interpretation of policy provisions by insured companies and gaps due to lack of cybersecurity by insurance service providers create challenges during a claim. To address this deficit, Joshi et al. (2019), proposes an automated approach that utilises machine learning and artificial intelligence to determine current security controls thereby arriving at an informed policy coverage. This will ensure that all stakeholders have the same understanding of what the cyber insurance policy cover entails. According to Hurtaud, Flamand, Hounka (2015, p. 3) *cyber insurance adoption among organisations remains at a low level in spite of the increase in cyber incidents. In the US, it is estimated that 65% of publicly-traded companies do not have cyber insurance* (Hurtaud et al., 2015). This is an incongruity as 63% of decision-makers indicate that cyber risk is one of their biggest challenges. According to Hurtaud et al. (2015), it is due to the lack of

cyber insurance awareness, underwriting complexity, and the challenge of aligning insurance with risk exposure.

### 2.6.3 *Challenges of cyber insurance*

Cyber insurance serves as an additional layer to cyber resilience however the lack of cogent and systemic approach to risk management could pose a challenge for an organisation if left unattended (Huang et al., 2018). Various scholars have identified different challenges that the cyber insurance market faces. Bandyopadhyay et al. (2009) cite the following three challenges as the most common reason for the cyber insurance market slow growth:

a) Insufficient attack-loss data
b) Lack of product-market experience
c) Accounting difficulties

Furthermore, a 2018 study conducted by the MIT Sloan School of Management and the Boston Consulting Group to 45 interviews with underwriters, brokers, reinsurers, and customers in the U.S., Europe, and Asia added the following challenges facing the cyber insurance market (Sommerrock et al., 2018).

a) The unique nature of cyber risk.
b) The difficulty in measuring and understanding accumulation risk.
c) The limited availability and sharing of cyber incidents and claims data.
d) The impact of regulation.
e) The effect of new technologies on cybersecurity.

The underdevelopment for the cyber insurance market is due to underwriters' lack of experience with cyber risk and scarce actuarial data impeding economical pricing (Wirfs, 2016). The lack of standardisation reflects the fact that cyber insurance is a relatively new cover, its evolution out of existing products (e.g. tech E&O and property insurance) and the competitive nature of the business (Camillo, 2017). Data on cyber risk are scarce since companies are either unaware of a cyber-attack (Toregas & Zahn, 2014) or the victims are reluctant to

report such events. Eling & Schnell (2016) argue that most empirical papers on cyber risk rely on data breach information (not loss information).

Yang & Lui (2014, p. 2) highlight two main challenges associated with cyber insurance i.e. adverse selection and moral hazard. The challenge with adverse selection arises when the insurance provider is unable to distinguish between high and low-risk hosts. Woods & Simpson (2017) adds that adverse selection occurs where a firm may apply for cyber insurance in the knowledge that they are relatively more exposed to cyber risk. Figure 13 below illustrates the different types of protections that the company should explore.

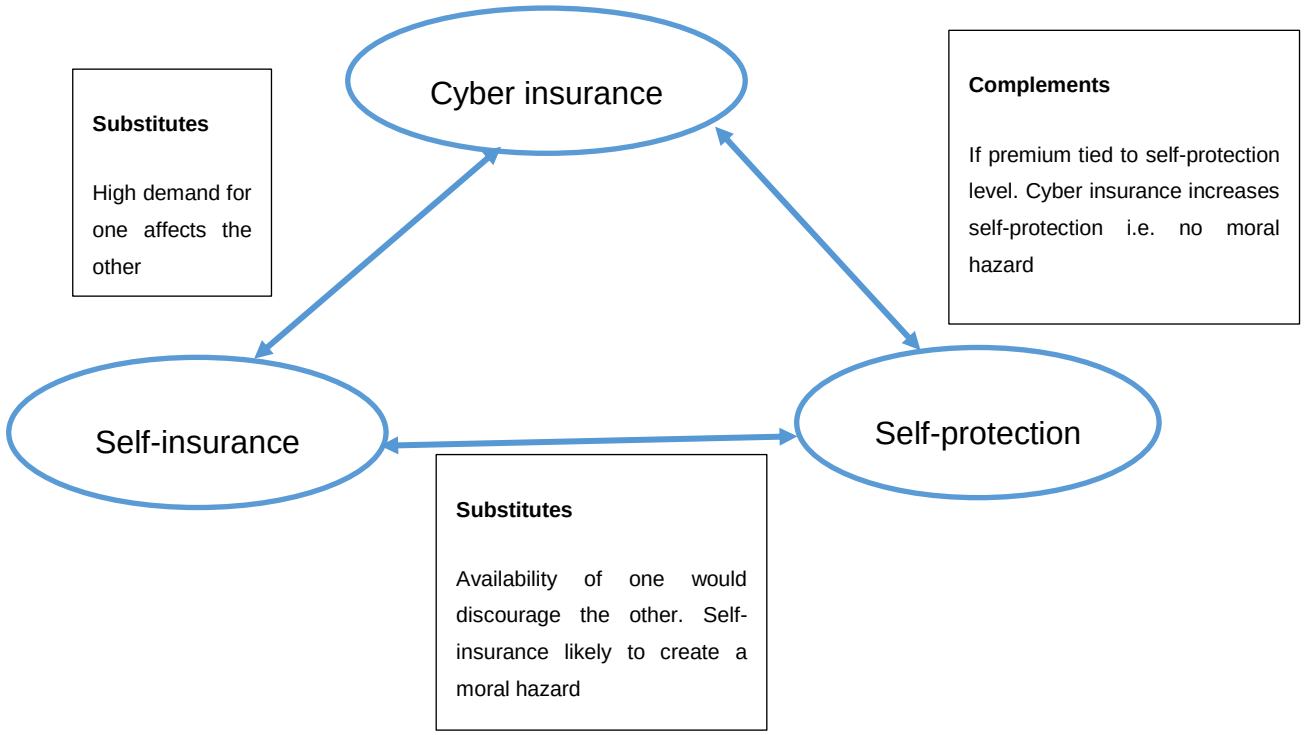



**Figure 13**: Cyber protection Adapted from (Kesan et al., 2005)

As shown in figure 13, the combination of self-protection and insurance raises the problem of moral hazard, in which nodes covered by insurance may take fewer secure measures, or even falsify their loss (Yang & Lui, 2014). Moral hazard happens when the insurance provider cannot observe the protection level of nodes (Yang & Lui, 2014) and can be addressed by the ongoing relationship between the insurer and the policyholder (Woods & Simpson, 2017). Table 2 below summarises cyber insurance challenges based on three categories:

**Table 2: Cyber insurance challenges** Source: Toregas & Zahn (2014)

| Category | Challenge |
|---|---|
| Legal framework | ▪ uncertainty about liability<br>▪ spotty coverage and insurance loopholes<br>▪ lack of standards or "bad" standards |
| Conceptual issues | ▪ quantification of risks and costs<br>▪ cyber risk not seen as a business problem or underestimated<br>▪ Correlated, interrelated and global risks<br>▪ lack of re-insurance |
| Setting premiums | ▪ lack of actuarial data<br>▪ uncertainty about normative standards<br>▪ premiums too high |

These factors have led to conservatism by providers that err on the safe side by overpricing their products (Bandyopadhyay et al., 2009). If that trend grows, the cyber insurance market may be unsustainable (Vicevich, 2018).

### 2.6.4 *Proposition 3*

Compliance with regulations enables organisations to adopt cyber insurance in the South African industry to reduce the risk of financial losses associated with cyber breaches.

## 2.7 Conclusion of the Literature Review

In this chapter, a review of the literature on cyber insurance was conducted. Background of cybersecurity was provided to highlight the impact on organisations. A TOE framework was nominated to underpin this chapter to meet

the research objectives (Tornatzky et al., 1990). A link between cybersecurity and digital technology was unpacked to illustrate the risks to organisations that come with emerging technologies.

The effects of cyber risks were explored and cyber insurance was proposed to complement existing controls to minimize financial loss. A brief exploration of cyber risks in the context of South Africa was presented and various incidents highlighted. The global size of the market was presented and types of liability covers were discussed. Various cybersecurity threats that influence factors cyber insurance were discussed as well as benefits to organisations.

Cyber insurance is without challenges, as such, drivers of adoption were highlighted. This study is based on the adapted (Tornatzky et al., 1990) theoretical framework called Technology-Organisation-Environment (TOE) framework. The theoretical perspectives are used to identify factors influencing cyber insurance adoption in the public and private sectors in South Africa. Three propositions that will be tested and validated through a qualitative approach are listed below:

### 2.7.1 *Proposition 1*

The awareness of effective cybersecurity technology controls complement cyber insurance to reduce the impact of cyber-attacks in the South African industry.

### 2.7.2 *Proposition 2*

An organisational approach to cybersecurity determines cyber risk management support.

### 2.7.3 *Proposition 3*

Compliance with regulations enables organisations to adopt cyber insurance in the South African industry to reduce the risk of financial losses associated with cyber breaches.

# CHAPTER 3. RESEARCH METHODOLOGY

## 3.1 Introduction

The literature review, Chapter 2, enabled the study to gain deeper insights into cybersecurity, cyber risk management, and cyber insurance theories. This chapter presents the research approach and the high-level design of this study. The data were collected using structured interviews based on the questions in Appendix A. The research questions were designed based on the constructs of the TOE framework and aligned with three propositions. This was done in an attempt to gain in-depth industry perception on the adoption of cyber insurance in the public and private sectors in South Africa. Thematic content analysis was employed to analyse data.

The study will ensure the highest regard to ethical considerations to ensure the transferability and credibility of the research methodology employed. Therefore, the purpose of this study is to present an understanding of the constructs in charge of proving or disproving the propositions based on the real-world perception of the factors influencing the adoption of cyber insurance in public and private sectors in South Africa.

## 3.2 Research approach

This study employed a qualitative research approach to explore and understand the meaning participants assign to the concept of cyber insurance in South Africa (Creswell & Creswell, 2017). The rationale is due to the study's relevance to socio-economic factors influencing the adoption of cyber insurance in the public and private sectors in South Africa. The research approach used to collect data was predominantly qualitative for the nominated demographic who are assumed to have an understanding of the study based on their work experience in the space. The study employs an inductive approach as it provides methodical flexibility through observing emerging patterns and themes from the interview questions (Liu, 2016).

## 3.3 Research design

The research design is grounded on the propositions that were framed using the TOE framework as an overall guide and feedback from open-ended semi-structured interview questions conducted to 10 participants that were deemed to possess the necessary skills, experience, and understanding of cyber insurance (Creswell & Creswell, 2017). The research study design comprises of research objectives, which lead to the three propositions using the interview questions which is most suitable for a qualitative study to make an inquiry on the cyber insurance concept (Flick, 2014).

Underpinned by the TOE framework to identify factors influencing the adoption of cyber insurance in the public and private sectors in South Africa, the premise on semi-structured interviews to elucidate socio-economic on the three propositions made (Creswell & Creswell, 2017). In line with the research objectives and to develop theory from the ground, the study uses the inductive approach with an intention to pursue South African industry insights (Thomas, 2003). Figure 14 below illustrates the high-level research design supported by the three propositions derived from the TOE framework.

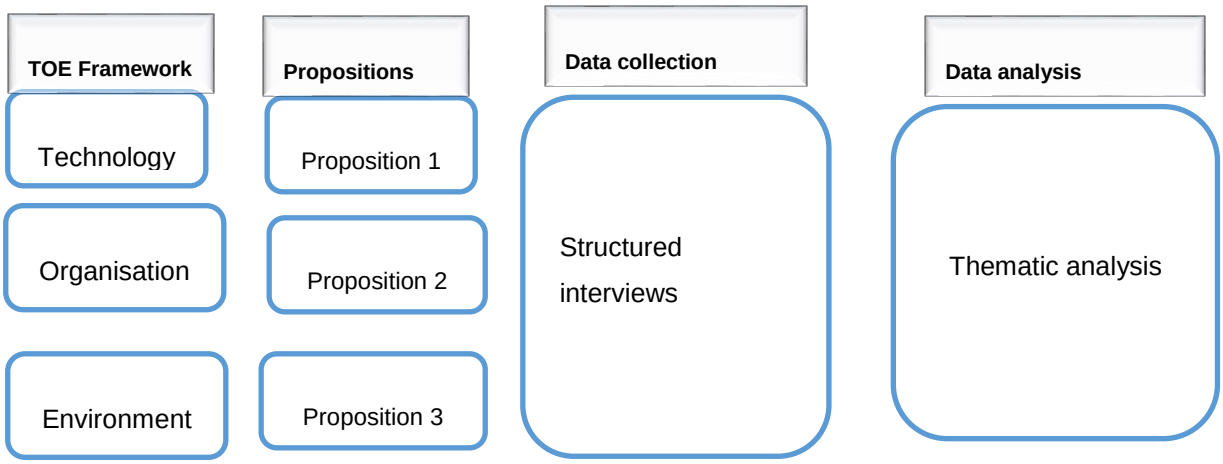



**Figure 14**: Summary of research design

As shown in figure 14 above, the research study has adapted the TOE framework (Bandyopadhyay, 2012b) which translates to three propositions centred on the technology, organisation, and environment. The study is conducted by investigationg individuals that are positioned at strategic, tactical and operational

levels in organisations. These levels are operationalised through organisational cross cutting constructs such as technology, processes and sytems to drive organisational objectives.Structured interview questions are designed using the elements of the TOE framework and thematic analysis will be used to inductively analyse the findings from the semi-structured interview questions (Creswell & Creswell, 2017). Data analysis is based on the thematic content analysis to extract essences and essentials of participant meanings (Miles et al., 2014).

## 3.4 Data collection methods

The data collection method employs semi-structured interviews as the method best suited for the description of the factors influencing the adoption of cyber insurance in the public and private sectors in South Africa. There are 10 face-to-face semi-structured interview questions that are used to probe 10 participants to gain deeper insight into cyber insurance adoption in the South African industry (Creswell & Creswell, 2017).

The emphasis was to ask probing questions to gain deeper insight into the cyber insurance adoption in the South African industry using the TOE framework on IT professionals (Harrell & Bradley, 2009). The participants are purposefully selected as they have the necessary understating of the research problem and questions due to their experience in IT (Creswell & Creswell, 2017). Collected data were used to triangulate in order to nullify or affirm the research study's theoretical perception (Langa, 2016).

## 3.5 Population and sample

### 3.5.1 *Population*

The population consists of all IT professionals in the public and private sectors (including cyber insurance providers) in the South African industry operating at strategic, tactical and operational organisation levels to enable triangulation (Creswell & Creswell, 2017). The rationalisation was to probe the level of

understanding, knowledge, and experience in various levels of cyber insurance concept thus answering semi-structured interview questions (Taherdoost, 2016).

### 3.5.2 *Sample and sampling method*

Qualitatively, 10 participants were interviewed comprising Chief Information Officer (CIO), Chief Information Security Officers, Executive Manager, Heads of Department, Information Security Manager, IT Audit Manager, Cyber Risk, and Risk Consulting, as well as Principal Specialist responsible for cybersecurity, cyber risk and cyber insurance from selected organisations. The selected sample was justified based on the primary aim to understand the factors influencing cyber insurance adoption in South Africa industry. The study focused on companies operating in the South African public and private sector albeit some organisations have global operations thus assigning an international perspective to enhance diverse viewpoints.

The study employed purposive random sampling through the use of the LinkedIn professional network that is small in the South African cyber insurance industry adoption context and will be covered in-depth (Miles et al., 2014). Table 3 below highlights the profile of interview respondents.

**Table 3: Profile of respondents**

| Description of respondent type | Number to be sampled |
|---|---|
| Divisional Head: ICT Governance & Compliance | 1 |
| Chief Information Security Officer | 2 |
| Manager: Information Security | 1 |
| IT Audit Manager | 1 |
| Executive Manager: Enterprise Architecture, IT Governance, risk and compliance | 1 |
| Head of IT | 1 |
| Principal Specialist | 1 |
| Client Manager: Cyber Risk and Risk Consulting | 1 |

| | |
|---|---|
| Chief Information Officer | 1 |
| **TOTAL number of respondents** | **10** |

The sample size of 10 participates was reasoned satisfactory as the information required for the research study was responded with sufficient assertion thus reaching the saturation point. Saturation occurs where no new discernments from the added analysis are found (Bowen, 2008) or all angles of the study have been sufficiently covered (Fusch & Ness, 2015). In terms of this specific study, the saturation point was grasped at the eighth interview with the remaining two interviews conducted to confirm the saturation point had been reached.

## 3.6 The research instrument

The research instrument was based on the qualitative method using the semi-structured interviews that were linked to the three propositions stemming from the TOE theoretical framework (Talmy, 2010). Ten semi-structured interview questions based on TOE framework constructs are designed in English for ease of understanding by participants and interpretation. Qualitative research interview is defined as "*an interview, whose purpose is to gather descriptions of the life-world of the interviewee with respect to interpretation of the meaning of the described phenomena*" (Opdenakker, 2006, p. 1).

Appendix A illustrates the semi-structured interview questions. The advantage of semi-structured interview questions is that it is conducted through face-to-face as well as using the telephone. Face-to-face and telephone semi-structured interviews have the advantage of being scheduled at the appropriate place and time as well as spontaneous response with frequent follow-up questions to probe further (Opdenakker, 2006). Out of 10 interviews, nine were conducted face-to-face as participants are located in Gauteng Province and only one was conducted using telephone due to time and availability constraints albeit being located in Gauteng Province. The disadvantages of telephone interviews are that the participant is not visible and there is a possibility of communication interruption.

To alleviate the loss of communication, all interviews were recorded using a recording device with the permission of participants and transcribed using Otter.ai

web application. Appendix B provides the participant information sheet and consent form.

## 3.7 Procedure for data collection

The procedure of research encompasses open-ended semi-structured interview questions; a collection of data occurred at the participant's preferred location, creating data analysis inductively from basic codes to general themes, and arriving at interpretations of the meaning of the data thus enabling report writing (Creswell & Creswell, 2017).

The technique used to collect data on the purposive sample was semi-structured face-to-face and to some extent, telephonic interviews wherein participants were given an opportunity to express their experiences, understanding, and views on the cyber insurance phenomenon (Hox & Boeije, 2005). Prior to the commencement of the interview process, the interviewer explained the purpose of the interview and requested the interviewees to familiarise themselves with the Participant Information Sheet to complete and sign the consent form (Appendix B). Ten semi-structured interview questions were designed and developed based on the TOE framework (Appendix A). Participants were identified using the LinkedIn professional network to ensure experience, understanding, and views on the cyber insurance phenomenon. Contact of participants occurred through email to arrange for an interview session that occurred between 28 October 2019 to 18 November 2019. Out of ten interviews, nine were face-to-face and only one was telephonic due to time constraints on the part of the participant.

Whilst notes were taken, all interviews were recorded using a recording device with permission from the interviewee. The interview started with the researcher providing an introduction to the research study and proceeded with open-ended questions that were semi-structured to allow the participant to provide prompt feedback. Where necessary, follow up questions were asked to probe for further insight thus enriching the data collection technique. Towards the end of the interview, all interviewees were thanked for their time and insightful contribution to the research study. The recorded data was then uploaded on the Otter.ai web

application to transcribe recordings. The output of the transcript was compared to recordings as well as the notes taken to ensure accuracy and completeness that became useful for data analysis and interpretation.

## 3.8 Data analysis and interpretation

The qualitative method chosen follows a systemic approach wherein purposeful sampling of 10 participants led to the collection of data using open-ended semi-structured interview questions that were analysed using thematic analysis followed by interpretation of findings (Creswell & Creswell, 2017). Recording of 10 interviews was uploaded on Otter.ai web application to facilitate transcriptions. Microsoft Excel was used to extract and present raw data to enable coding.

Coding in qualitative analysis enables breaking down data to develop expansive categories and themes to reach saturation as well as conducting triangulation thus eliminating research bias (Yeh & Inman, 2007). Saturation occurs where no new discernments from the added analysis are found (Bowen, 2008) or all angles of the study have been sufficiently covered (Fusch & Ness, 2015). In terms of this specific study, the saturation point was reached at the eighth interview with the remaining two interviews conducted to confirm the saturation point had been reached.

Triangulation supports a finding to demonstrate multiple independent sources that are in agreement or do not contradict so that they can complement each (Miles et al., 2014). Triangulating multiple instances on various sources from disparate industries in terms of strategic, tactical and operational viewpoints to collaborate to enhance the trustworthiness of findings (Miles et al., 2014). This examination and re-examination of various sources at dissimilar points in time validated the transparent interpretive and constructive processes of the researcher (Yeh & Inman, 2007). Whilst thematic was a predominant method of analysis, quantitising strategy was employed to transform qualitatively collected data to numbers (Langa, 2016) thereby obtaining deeper meaning from participants experiences (Creswell & Creswell, 2017). Data interpreted through finding deeper meaning, ideas emerging and insights from the study were

subsequently displayed or presented on the report using texts, quotations, tables, and figures (Yeh & Inman, 2007). The weighing of participant's words and researcher interpretations took place thus creating equilibrium ensuring interpretation of deeper meaning from experiences (Miles et al., 2014).

## 3.9 Limitations of the study

The research study was limited to the sample of 10 participants that do not represent the entire South African industry. As such, the views and opinions are limited in scope. Qualitative studies are deemed to be subjective in nature (Creswell & Creswell, 2017) therefore the views, experiences, and meanings are contextual to the 10 participants (Miles et al., 2014) and analysis of data took longer to complete as it was conducted manually using Microsoft Excel. Some of the participants were quite senior in their respective careers so scheduling time in their diary became a challenge, which was overcome by scheduling according to their availability.

## 3.10 Transferability and dependability

### 3.10.1 *Transferability*

The study employed purposive sampling through the use of the LinkedIn professional network that is small in the South African cyber insurance industry adoption context which was covered in-depth (Miles et al., 2014). The sample comprised 10 participants who purposefully have sufficient understanding and experience of the South African industry in terms of cyber insurance phenomenon (Hox & Boeije, 2005). The findings are contextual which can thus be transferred or applied to another situation or population (Noble & Smith, 2015).

### 3.10.2 *Dependability*

The study ensures dependability through unique feedback based on the personal/human experiences of participants (Noble & Smith, 2015). The findings are unique for each identified source so that variation in participant experience is

considered (Kuper et al., 2008). As such, each participant's feedback is considered important to the research study findings as it adds an element of uniqueness and provides varying insights in a clear and transparent manner (Noble & Smith, 2015). The use of codes, categories, and themes as well as triangulating multiple sources to enable effective data to display assisted in meeting dependability criteria (Yeh & Inman, 2007).

### 3.10.3 *Credibility*

The purpose of the study was described to all participants to ensure consistency and truth value (Connelly, 2016). The research study employed the TOE framework (Bandyopadhyay, 2012b) to ensure that interview questions were relevant to the cyber insurance phenomenon to obtain findings (Creswell & Creswell, 2017). The study employed saturation and triangulation to ensure credibility wherein researcher bias was eliminated (Yeh & Inman, 2007).

This ensured that collected data reached the point of redundant or saturation at the eighth interview resulting in no new knowledge added to the study (Yeh & Inman, 2007). Triangulation was utilised to eliminate researcher subjectivity and support the attainment of multidimensionality to the data set (Yeh & Inman, 2007). The study sought to uniquely present findings in the most accurate manner by describing or interpretation participant experience with the cyber insurance phenomenon (Kuper et al., 2008).

### 3.10.4 *Confirmability*

To ensure confirmability and therefore enhancing findings, the research study sought to pay attention to participants by probing more clarity seeking questions in a given context to unearth hiding participant experiences of cyber insurance phenomenon (Noble & Smith, 2015). As such, this was attained through the combination of transferability and credibility as well as employing reflexive strategy as the researcher is a cybersecurity professional (Kuper et al., 2008).

## 3.11 Demographic profile of the respondent

The study intended to identify and interview 10 participants and as such all respondents cooperated with the researcher's request and presented on Microsoft Excel Spreadsheet. The respondents are categorised on the role, the number of professional years of experience, industry, and description as well as the perceived level to meet research objectives (Patil et al., 2005). Table 4 below presents the demographic profile of 10 respondents:

**Table 4: Demographic profile of respondents**

| Professional Profile | | | | | |
|---|---|---|---|---|---|
| **Participant number** | **Role** | **Number of professional years of experience** | **Industry** | **Description** | **Perceived level** |
| 1 | Divisional Head: ICT Governance & Compliance | 14 | Public Municipality | Local government municipality | Strategic |
| 2 | Chief Information Security Officer (CISO A) | 14 | Private Beverage | Multinational beverage corporation with operations in SA | Strategic |
| 3 | Manager: Information Security | 12 | Private Telecommunication | One of the big four telecommunication corporate in SA | Tactical |
| 4 | IT Audit Manager | 10 | Public Government | A government regulator | Tactical |
| 5 | Executive Manager: Enterprise Architecture, IT Governance, risk and compliance | 24 | Public Logistics | A State Owned Entity in the logistics sector | Strategic |
| 6 | Chief Information Security Officer (CISO B) | 12 | Private ICT | A managed ICT service provider to local and offshore customers | Strategic |
| 7 | Head of IT | 10 | Public Financial Services | A state owned entity in the financial services sector | Tactical |
| 8 | Principal Specialist | 14 | Private Manufacturing | Multinational steel manufacturing corporation with SA operations | Tactical |
| 9 | Client Manager: Cyber Risk and Risk Consulting | 7 | Private Financial Services | A Lead Risk Advisor and Cyber Insurance Broker globally with SA operations | Tactical |
| 10 | Chief Information Officer | 23 | Public Financial Services | A state owned entity in the financial services sector | Strategic |
| | **Average Experience** | **14** | | | |

Table 4 above illustrates the professional profiles of 10 participants. In line with the ethical prescripts, the demographic profile of respondents was carefully designed to maintain anonymity thus ensuring participant's privacy (Randall &

Koppenhaver, 2004). Information that was collected about respondents pertains to the role/function as well as the number of professional years of experience to ensure consistency with the chosen purposive sampling strategy (Miles et al., 2014). The average number of professional years of experience is 14 which illustrates the depth of understanding of the cyber insurance concept. Two participants that had a similar job title of Chief Information Security Officer (CISO) namely CISO A and CISO B from the Beverages and ICT sectors respectively of the South African industry. The industry is categorised as public and private with five per sector with industry description. Respondents are also categorised as strategic, tactical and operational levels wherein five respondents were perceived to strategic and the remaining five being tactical based on their role. None of the respondents was perceived to be operational which was the limitation of the study to provide varying perspectives.

## 3.12 Ethical considerations

Prior to data collection and ethics clearance was issued by the authorising committee to eliminate harm to respondents (Roberts, 2015). During the data collection process, consent was obtained from respondents taking into account the needs of the research project and balancing them with respondents right to privacy (Houghton et al., 2010). As such respondents identities were anonymised to maintain confidentiality thereby protecting respondents from any potential prejudice (Markham, 2012).

Respondents recording and transcriptions were kept secure in a password-protected computer to ensure the confidentiality and integrity of data collected through the interview process (Parry & Mauthner, 2004). Data analysis and interpretation were subjected to scrutiny to minimise researcher bias thereby ensuring the trustworthiness of data collected (Dowling, 2005). Due care was exercised to ensure the research project adheres to ethical conduct (Langa, 2016) as such enhancing research credibility.

# CHAPTER 4. FINDINGS AND DISCUSSION

## 4.1 Introduction

Chapter 3, the Research Methodology, provided a systemic approach and design of the qualitative research to obtain insights from the purposefully selected sample using open-ended semi-structured interview questions to collect data (Hox & Boeije, 2005). As shown in Table 4 above, the sample comprised five respondents from the public sector and another five from the private sector of the South African industry. The average years of experience are 14 years thus providing a sufficient combination of knowledge, skills, and understanding of the cyber insurance concept. Private sector organisations in Beverages, ICT, Manufacturing, and Financial services industries have global operations. Based on the sample, two Chief Information Security Officer (CISO) professionals from the Beverages and ICT sectors, namely, CISO A and CISO B respectively for ease of identification. Out of ten participants, nine interviews were through face-to-face and one through telephone due to the non-availability of the respondent. Recordings of all interviews took place using the recording device and recordings were uploaded onto Otter.ai web application to transcribe. Microsoft Excel was utilised to code and classify data into categories leading to emerging themes (Creswell & Creswell, 2017).

Chapter 4, Findings and Discussion, seeks to present and discuss the findings obtained through 10 interview questions to provide deeper meaning and interpretation of perspectives obtained from 10 participants (Creswell & Creswell, 2017). To ensure credibility and transferability of findings to another context, triangulation and saturation concepts are employed thus enriching the meaning of participants experiences (Yeh & Inman, 2007). The categories of saturation include the demand-side, which represents nine organisations that may adopt cyber insurance and one supply-side organisation that is a cyber insurance service provider. The study employed inductive thematic analysis of findings as the most suitable approach to meet research objectives (Langa, 2016) thus classifying respondents as strategic, tactical and operational management levels based on their perceived role, understanding and experience (White, 2009).

Operations pertain to respondents who provide input to management through administrative tasks, tactical pertains to interpreting and organising tasks for decision making and strategic level is about aggregating and analysis for informed decision making (White, 2009).

Furthermore, analysis and interpretation of findings seek to confirm or deny propositions emanating from the literature review (Ryan, 2006). Alignment of research objectives, research propositions, research interview questions and emerging research themes from findings took place to ensure transparency and consistency. Table 5 below illustrates the alignment to ensure consistency throughout the research process.

**Table 5: Consistency matrix**

| **Research objectives** | **Propositions** | **Interview questions** | **Emerging themes** |
|---|---|---|---|
| Technology about the awareness and effectiveness of cybersecurity technologies. | The awareness of effective cybersecurity technology controls complement cyber insurance to reduce the impact of cyber-attacks in the South African industry. | 1. How long have you been a professional, your job title and description?<br>2. What is your perception of cybersecurity?<br>3. Describe the importance of cyber insurance.<br>4. What is your general perception of cybersecurity | Effective cybersecurity awareness |

| | | | |
|---|---|---|---|
| | | and/or cyber insurance?<br><br>5. Describe how your organisation ensures awareness of cybersecurity technology. | |
| Organisation about cyber risk management and management support. | An organisational approach to cybersecurity determines cyber risk management support. | 6. Describe how your organisation approaches cybersecurity.<br><br>7. To what extent does your organisation manage cyber risk?<br><br>8. Describe management support to cyber risk management for your organisation. | An organisational approach to managing cyber risk |
| Environment about government regulations and | Compliance with regulations enables organisations to | 9. Describe the extent to which your organisation must comply with | Cyber insurance adoption in South Africa industry. |

| | | | |
|---|---|---|---|
| the nature of the industry. | adopt cyber insurance in the South African industry to reduce the risk of financial losses associated with cyber breaches. | government regulations?<br><br>10. Describe the nature of your industry and how it approaches the cyber insurance. | |

Table 5 above illustrates the alignment of research objectives, propositions emanating from the literature review, interview questions and the emerging themes from collected data through semi-structured interviews. The objective of this study is to investigate factors influencing cyber insurance adoption in the South African industry from the perspective of technology, organisation, and environment. The TOE framework enabled the formulation of three propositions based on the literature review that culminated in the design of ten interview questions (Bandyopadhyay, 2012b). The outcome of the data collected from the purposive sample inductively led to three emerging themes (Miles et al., 2014).

## 4.2 Discussion pertaining to Proposition 1

Proposition 1 from the literature review proposed that the awareness of effective cybersecurity technology controls complement the adoption of cyber insurance to reduce the impact of cyber-attacks in the South Africa industry. The design of five questions provided answers to the proposition that ultimately led to the theme below which is linked to the research objective on technology about awareness and effectiveness.

### 4.2.1 *Effective cybersecurity awareness*

Cybersecurity awareness has a direct link to the perception of cybersecurity technology within an organisation. During the interview process, participants had

to select options designed through literature to gauge their general perception of cybersecurity. Table 6 below illustrates the perceptions of cybersecurity as obtained from the purposefully selected sample of 10 professionals in the South African industry.

**Table 6: Cybersecurity perception**

| Cyber Security Perception | | |
|---|---|---|
| **Cyber Security** | **Responses** | **Ratio** |
| Secure electronic data activity on servers, workstations and mobile devices | 6 | 60% |
| Facilitates implementation of cybercrime laws | 3 | 30% |
| Detects, prevents and corrects external and internal threats to mitigate cyber risks | 10 | 100% |
| Improves end-user knowledge about secure practices | 6 | 60% |
| Enhances the privacy and protection of personal information | 7 | 70% |

Table 6 above illustrates the participants' responses in terms of their general cybersecurity perceptions. Quantitising strategy was employed to transform qualitatively collected data to numbers (Langa, 2016) thereby obtaining deeper meaning from participants experiences (Creswell & Creswell, 2017). Overall, the responses seemed positive with few respondents noting negative sentiments. Notably, all respondents seemed to agree that cybersecurity detects, prevents and corrects external and internal threats to mitigate cyber risks (Carlton & Levy, 2017; Stallings et al., 2012). IT Audit Manager stated "*Cybersecurity is important for the business to operate securely*" suggesting organisations must pay attention to cybersecurity for long-term sustainability.

70% of respondents consider cybersecurity as a mechanism that enhances the privacy and protection of personal information. The Manager: Information Security agrees, "*Cybersecurity ensure organisations maintain customer's information and is protected at all time i.e. privacy*" highlighting the need for

organisations to protect customers information. It is the organisation's responsibility to uphold and protect customer's privacy for information collected, processed and stored on information systems (Isaak & Hanna, 2018; Mubarak Alharbi et al., 2013).

60% of respondents considered cybersecurity to secure electronic data activity on servers, workstations, and mobile devices. The Principal Specialist added, "*Cybersecurity is about securing infrastructure to prevent hackers from accessing systems or applications*", reinforcing the importance of cybersecurity at the multinational manufacturing organisation to secure physical operations from disruptions (Mo et al., 2011). On a separate event, 60% of respondents suggested that cybersecurity improves end-user knowledge about secure practices. The CIO supports, "*The biggest weakest link in cybersecurity is people"* thus, putting into effect the need for organisations to educate end-users. There is a close link between effective cybersecurity practices and the level of end-user understanding of cybersecurity thus making end-users key stakeholders in protecting organisational assets (Bakhshi, 2017; Stanton et al., 2005).

Finally, only 30% of respondents consider cybersecurity to facilitate the implementation of cybercrime laws. CISO B seemed to disagree, "*whether you have cybersecurity controls within the organisation or not, it doesn't influence the laws, therefore, it is an indirect relationship*" highlighting that cybercrime laws facilitate cybersecurity implementation (Choucri et al., 2014) and not the other way around.

Overwhelmingly, out of ten respondents nine (90%) demonstrated positive sentiment towards the importance of awareness of cybersecurity technology and the benefits to their respective organisations. Only one (10%) respondent appeared to have a negative view about the state of awareness at their organisation. Lack of security awareness is a concern for organisations in all sectors as security is multi-faceted and requires diverse expertise to effectively manage the risk (Ben-Asher & Gonzalez, 2015). As such, the Divisional Head: ICT Governance & Compliance stated "*In this organisation, cybersecurity is not taken seriously due to the cost of maintaining the proper cybersecurity programme, cost of implementation and lack of understanding the value of data,"*

suggesting that the metropolitan municipality cybersecurity maturity is low. The Client Manager: Cyber Risk and Risk Consulting echoed this view "*that budget and management buy-in can be an issue in some organisations*" thus requiring an effective strategic approach to obtain management buy-in is necessary. Whilst most companies do invest in cybersecurity, CISO B indicates "*that cybersecurity investment needs to be taken a lot seriously by companies*". As such, cybersecurity is perceived as the barrier to business activities (Li et al., 2019).

Further, the Divisional Head: ICT Governance & Compliance insists, "*The organisation does not review policies, no awareness, no understanding of the disclaimer for responsibilities. Security is perceived as a tedious act that is not part of employees' job descriptions*". CISO B agrees with the negative sentiment by asserting that "*several organisations see security as a nuisance; they do not see it as delivering in their value chain*". Organisations should conduct cost-benefit or rate of return analysis to enable improved investments thus avoiding over or under investments to cybersecurity (Chronopoulos et al., 2017; Rowe & Gallaher, 2006).

On a positive note, CISO A perceives cybersecurity "*…as the standard of living and more organisations are beginning to appreciate the impact of secure practice to protect their revenue. It is a reality every organisation must ensure it fully understands its implications".* The Executive Manager: Enterprise Architecture, IT Governance, Risk and Compliance concurs "*cyber touches many realms in daily operation, with the increase in digitalisation, organisations are likely to be exposed to cyber vulnerabilities. It is important to take care of cybersecurity as lack thereof has significant implications for the organisation*". Cybersecurity can affect reputation, revenue generation and profits resulting in increased costs that affect innovative ideas to keep customers loyal (Shackelford et al., 2015). This suggests that cybersecurity must be addressed at the strategic level in order to ensure the attainment of business objectives. The CIO supports the view that suggests that cyber "...*is a necessity for organisations to continue to operate sustainably, therefore, cybersecurity is survival and it makes good sense to protect assets as cyber incidents can close down the company if left unattended*".

CISO A contends, "*Traditional way of conducting training and awareness such as email communication cannot be measured*". In support of this assertion, the Principal Specialist adds, "*traditional methods are no longer giving desired results that the company needs. Furthermore, email communication alone is not effective and not measurable. Online assessments are becoming a norm wherein the level of employee awareness can be measured*". The Client Manager: Cyber Risk and Risk Consulting support this view by stating that "*there has to be education preferably E-learning to people dealing with infrastructure*". Since according to Head of IT, "*Cybersecurity is about securing infrastructure to prevent hackers from accessing systems or applications*." Gaming can be an effective tool to drive and measure the level of understanding of cybersecurity awareness among employees (Hendrix et al., 2016). The IT Audit Manager adds, "*face to face awareness training to employees where employees can ask questions is one of the effective methods to drive good behaviour amongst employees*". The Principal Specialist posits, *"Effective cybersecurity awareness campaigns involve interacting directly with end-users"*. Alternative delivery methods include dissemination of content through various channels as well as face to face presentations to drive effective awareness programmes (Abawajy, 2014).

To solidify the importance of cybersecurity awareness at the tactical level, the Information Security Manager from the telecommunications organisation that has continental and global operations argues, "*Cybersecurity is important in ensuring the protection of organisational assets which can be attained by implementing and having a cybersecurity awareness programme*". At the strategic level, Executive Manager: Enterprise Architecture, IT Governance, Risk, and Compliance from a publicly owned logistics entity supports the view and augment "*it is critical to have cybersecurity to secure organisational assets as cybersecurity ensure organisations maintain the protection of customer's information at all time*". Furthermore, at the tactical level, the IT Audit Manager from the national regulator insists, "*Cybersecurity is important due to frequent processing of information by organisations delivering a service to customers thus important for a business to operate securely*". Securing organisational assets requires a combination of cybersecurity technology as well as resources such as human and financial to attain business-wide strategic goals (Posey et al., 2015).

The CIO concludes, "*It is a necessity for organisations to continue to operate sustainably, therefore, cybersecurity is survival and it makes good sense to protect assets as Cyber incidents can close down the company*".

At the tactical level, there is resonance in terms of the responsibility to distribute communication content and make employees aware of cybersecurity within the organisation. Both the IT Audit Manager and the Principal Specialist suggests that a representative within IT must ensure effective cybersecurity awareness takes place frequently. Hence, the Head of IT from a publicly owned entity states, "*The organisation conducts quarterly awareness programme to educate end-users to drive behaviour*". Strategically, the CIO points out, "*Organisation has an awareness programme that is running every year. It is compulsory that the organisation embarks on to increase the level of awareness*". For awareness to be effective, the CIO suggests, "*EXCO team must be the advocate of this initiative. There must be an element of fun people as employees win prices. The program runs continuously and the message must continuously change to ensure effectiveness. The organisation does themes around phishing, ransomware, secure practices, etc.*"

Effective cybersecurity is not without challenges within an organisation. The Executive Manager: Enterprise Architecture, IT Governance, Risk and Compliance points out challenges with cybersecurity "*many users are not cybersecurity savvy i.e. user receiving a phishing email and clicking on the link and get compromised*". However, the CIO insists, "*phishing attacks are proactively identified in his organisation*" highlighting approaches to counter phishing attacks by organisations. There is a general resonance at the strategic level about the need to educate users as the CIO state "*employees need to be aware of cyber risks as the weakness is the people*". Head of IT agrees, "*An organisation can protect the data from external threats however individuals within an organisation can compromise the organisation*". Client Manager adds, "*It is crucial to educate the end-user as they are easy targets*". As such, the human element is the weakest link and requires undivided attention in terms of training and education to ensure that the cybersecurity program delivers the desired results (Pfleeger et al., 2014).

It appears that the strategic viewpoint varies from the tactical viewpoint. In isolation, CISO B from the ICT industry suggests, "*Cybersecurity is moving from technical focus areas to be strategic where companies are adopting cyber strategies as it is a business risk. Board seeing cybersecurity as strategic is long overdue*" thus illustrating support at the right level of decision-making. CISO B posits "*At the principle level, it is important to run the security awareness programme for users to understand what is allowed or not. It's important that security technology must be clear to end-users*". In support of CISO B's assertion of cybersecurity being strategic imperative, the Client Manager: Cyber Risk and Risk Consulting agree with the narrative to compare and contrast it with the developed countries. Client Manager contends, "*Cybersecurity is a key strategic risk in the developed territories as well as in countries where technology is advance*" suggesting that South African organisations can learn lessons from their counterparts in other territories.

Emphasis must be to outline strategic priorities and directions, organisations must establish clear plans guided by vision and mission as well setting realistic strategic objectives that can be achieved over a period of time (Borum et al., 2015). The Client Manager further state "*South Africa is ranked as having the most people affected by cyber-crime in the world. It means that many people within the country do not understand the implications of the lack of understanding of cybersecurity".*

Review of literature confirms that South Africa is ranked third world-over as a country where most people are experiencing cybercrime (Gcaza & Solms, 2017). Therefore, the Client Manager concludes that to ensure effective cybersecurity awareness, "*Educate the Executive Committee (EXCO), Management Committee (MANCO) as well as people on the ground for the content to have a significant impact".* In agreement with the Client Manager, CISO A emphasised, "*the need to educate executive to gain necessary buy-in*". To get executive management buy-in, simple and clear articulation of cybersecurity value add to business operations is a requirement suggesting to avoid technical jargon (B. von Solms & von Solms, 2018).

In conclusion, holistically, the responses seemed positive with few respondents noting negative sentiments in terms of the importance of effective cybersecurity awareness. Overwhelmingly, out of ten respondents nine (90%) demonstrated positive sentiment towards the importance of awareness of cybersecurity technology and the benefits to their respective organisations. Only one (10%) respondent appeared to have a negative view about the state of awareness at their organisation.

It appeared there is a need for organisations to make end-users aware of cybersecurity to effectively mitigate the risks. To ensure effective cybersecurity awareness, the suggestion of various mechanisms took place. Mechanisms included gaming to keep employees engaged, online training such as E-learning and surveys that are measurable, as well as face-to-face presentations. Thus, the relationship between effective cybersecurity practices and the level of end-user understanding of cybersecurity is crucial in protecting organisational assets.

It seems organisations in all sectors consider lack of security awareness as a concern. Perception of the human element as the weakest link requires attention in terms of training and education to ensure that the cybersecurity program delivers the desired results. As such, end-users are an important shield in ensuring effective identification and prevention of cyber risks. Acknowledging various organisational levels, effective cybersecurity awareness requires a strategic approach to obtain management buy-in.

Lack of management buy-in resulted in the perception of cybersecurity as a barrier to business activities. As such, cybersecurity interventions must occur at the strategic level in order to drive change and ensure the attainment of business objectives. In order to obtain management buy-in and the board, simple and clear articulation of cybersecurity value add to business operations is a requirement suggesting to avoid technical jargon. This will ensure that cybersecurity initiatives get necessary buy-in in terms of human and financial support. Based on the evidence above, the study confirms the proposition, therefore, the awareness of effective cybersecurity technology controls complement cyber insurance to reduce the impact of cyber-attacks in the South Africa industry.

## 4.3 Discussion pertaining to Proposition 2

Proposition 2 pertains to the approach organisations take towards cybersecurity thus determining support to cyber risk management in the South Africa industry. This was achieved by designing three interview questions that culminated in the emerging theme to provide the answer to proposition 2. The below section will discuss in detail how the organisational approach to cybersecurity determines management buy-in to manage cyber risk. To support different types of cybersecurity approaches within an organisation, exploring the linkage between management buy-in and cyber insurance perception took place.

### 4.3.1 *An organisational approach to managing cyber risk*

The exploration of the organisational approach to cybersecurity determines the extent of management buy-in to make resources available to manage cyber risk in the South Africa industry. The approach the organisation takes towards managing cybersecurity risk has a direct link to cyber insurance perception as such the outcome of interview questions seeks to explore the relationship. Table 7 below illustrates the perceptions of cyber insurance from the sample of 10 professionals from varying industries in South Africa.

**Table 7: Cyber insurance perception**

| Cyber Insurance Perception | | |
|---|---|---|
| **Cyber Insurance** | **Responses** | **Ratio** |
| Complements an organisation's cybersecurity measures | 8 | 80% |
| Improves the cybersecurity control environment | 6 | 60% |
| Transfers risk of financial loss/liability associated with cyber-attacks | 10 | 100% |
| Challenge with the setting of premiums and policy coverage | 4 | 40% |
| Lack of explainable understanding of cyber insurance | 0 | 0% |

Table 7 above highlight the participant's responses to cyber insurance perceptions. Similar to Table 6 above, the transformation of raw data to words necessitated quantitisation (Langa, 2016) to reinforce a deeper understanding of participants' experiences (Creswell & Creswell, 2017). Overwhelmingly, all respondents perceived cyber insurance as a mechanism that enables organisations to transfer the risk of financial loss/liability with cyber-attacks. As the Client Manager: Cyber Risk and Risk Consulting point out "*cyber insurance pays for liability that emanates from the cyber incident wherein the cyber insurance pays to fix the incident as well as lawsuits so that the company resumes operations as soon as possible*". A view supported by the Principal Specialist that cyber insurance "…*covers for loss of productivity in the event of cyber-attack*". Further, the Head of IT extends, "*Cyber insurance enables the organisation to cover financial losses and maintain access to data in the event the organisation is hacked or attacked*". However, CISO A contends that having cyber insurance "*does not necessarily improve security controls*" however supports the view that "*it covers financial losses*". Manager: Information Security caution, "*There has to be some kind of synergy between cyber insurance and control measures implemented by the organisation"*. The benefits of cyber insurance include the shield that could potentially result in financial losses for organisations emanating from a cyber breach (Camillo, 2017; Franke, 2017)

Considered important, 80% of respondents perceive cyber insurance to complement an organisation's cybersecurity measures. Divisional Head: IT Governance and Compliance highlight the importance of cyber insurance by stating, "*It improves the cybersecurity control environment and transfers the risk of financial loss/liability associated with cyber-attack to the third party*." CISO B argues by stating, "*Cyber insurance only transfers the financial risk but not responsibility*". This view is compatible with the IT Audit Manager who states "*cyber insurance complements the existing controls and does not improve controls therefore organisations can use cyber insurance for compensation in the event of cyber-attack*." Cyber insurance complements an organisation's cybersecurity controls in case liability for data breach or loss, remediation costs such as legal and public relations as well as regulatory fines/penalties and settlement costs takes place (Hurtaud et al., 2015).

The other 60% consider cyber insurance to improve the cyber-security control environment. The Principal Specialist suggests "*Cyber insurance cover ensures that the business gets to operate in the shortest period after the breach thereby revenue preservation*". Client Manager: Cyber Risk and Risk Consulting contend, "*Whilst managing risk does not translate to revenue generation, it ensures that controls are placed to enable the organisation to operate risk-free*." Cyber insurance plays a significant role in enhancing cybersecurity controls within an organisation (Woods & Simpson, 2017).

Like any initiative, cyber insurance has inherent challenges, as such, 40% of respondents indicated that there is a challenge with the setting of premiums and policy coverage. The Client Manager: Cyber Risk and Risk Consulting posit from a cyber insurance service provider point of view, "*Underwriters are starting to exclude cyber incidents to their covers as it is challenging for actuarial professionals to determine the risk premium*" highlighting a need to unpack risk premium to determine what's covered and excluded. The lack of historical information to enable efficient cyber insurance product pricing (Tøndel et al., 2015) thus coverage tend to be expensive with numerous policy exclusions (Peters et al., 2018).

Interestingly, none of the respondents indicated a lack of explainable understanding of cyber insurance, which suggests that the sample has knowledge, experience, and understanding of the cyber insurance phenomenon. As the CIO put it "*With the sophistication of cybercrime, companies are forced to have cyber insurance. It is about when they will the hackers get to your network. You will never be 100% insured*". Therefore, cyber insurance addresses the residual after the implementation of cybersecurity control measures (S. Shetty et al., 2018).

Next, based on the responses from participants in terms of organisational cybersecurity approach, responses implied two approaches i.e. top-down and bottom-up wherein management support could be proactive or reactive. Table 8 below illustrates the link between cybersecurity approach and management support that determines the extent to which cyber risk is managed within an organisation.

**Table 8: Cybersecurity approach and management support**

| Cyber Security Approach | Management Support | Responses | Ratio |
|---|---|---|---|
| Top-down | Proactive | 6 | 60% |
| Top-down | Reactive | 3 | 30% |
| Bottom-up | Reactive | 1 | 10% |
| | **Total** | **10** | **100%** |

Table 8 illustrates the relationship between cybersecurity approach in terms of top-down vs bottom and management support concerning proactive and reactive. In the context of this study, top-down relates decision-making, goals, objectives, and actions that are driven from top management to manage cyber risks (Linkov et al., 2014). Whereas bottom-up is about conducting risk assessments to influence top management of the organisation to make risk-informed decisions (Linkov et al., 2014).

In this study, 60% of respondents appeared to lean towards a top-down approach with proactive management support. The Manager: Information Security state "*the objective of cybersecurity is to mitigate the risk that the organisation faces on a daily basis therefore the organisation takes cyber risk management serious to protect assets*". In addition, "*There is management support wherein the Information Security Risk Committee is established to proactively deal with technology issues*" which indicates that the organisation is proactive in decision-making in terms of cyber risk tolerance. As reflected in the organisation's risk appetite statement, the IT Audit Manager emphasises "*the risk register is the driving force to determine cyber risk tolerance levels*." The organisation must, therefore, ensure that attainable goals are set with adequate capability to counter the effects of cyber risks thus enhanced business outcomes (Cherdantseva et al., 2016; Johnson, 2015).

In line with top-down proactive management support, the Executive Manager: Enterprise Architecture, IT Governance, Risk, and Compliance state, "*A function that deals with cybersecurity exists with a structure that comprises of experts on cybersecurity*." The IT Audit Manager views "*the separate establishment of an information security function as necessary to ensure accountability*". Highlighting the importance of best practice frameworks the Head of IT indicates that

cybersecurity "…*is approached at the high level i.e. policies, standards that support security ISO 27001/2, frameworks to obtain guidance by implementing an end-to-end cybersecurity programme to minimise cybersecurity breach and continuously improve on measures*". To emphasise the point, the Executive Manager highlight "*Cyber risk is supported across the entire organisation and all the way to the board*". CISO B advises, "*The board must own the risk and not transfer it to insurance*" to monitor the status of cyber risk in the organisation and take proactive decisions in the interest of the organisation. The Principal Specialist adds, "*The Audit Committee has an item where cyber risks are discussed because of the importance*." Suggesting that the board is paying attention to cyber risk thus takes place at the highest level of the company.

Organisations that have established board committees are less likely to breached as cyber risks are proactively mitigated through early detection and response thus adding value to business operations (Higgs et al., 2016). Whilst the management of cybersecurity is everyone's business within an organisation, the board has the responsibility to provide oversight thus long-term sustainability of an organisation (Rothrock et al., 2018). The Client Manager advises, "*It is important for the CIO/CISO to communicate clearly in terms of the human and financial resources needed, timeframe and benefits to the organisation*" highlighting that cybersecurity and associated risk get attention at the board and C-suite level. Further, proactive management support "… *comes with educating the C-suite and impact assessments are necessary to guide CEOs. They must be empowered to make decisions that are in the best interest of the organisation*".

In terms of the risk register, the Executive Manager indicated, "*A risk register exists to track the implementation of risks with automatic escalations if certain risks are not being adequately managed*". This proactive approach seems to be supported by the Head of IT who highlights "*Due to recent attacks on South African companies, implementation of security measures have received top management attention*" suggesting human and financial resources are allocated commensurate with the risk of the organisation faces. Whilst the organisation approaches cybersecurity from a top-down perspective, the Principal Specialist has a different view that suggests "*The management support is there although a*

*lot is still required in terms of financial and human resources that are needed*" suggesting that resources are required to mitigate the cyber risks. The Client Manager: Cyber Risk and Risk Consulting appreciate organisational constraints by acknowledging "*budget spend can be an issue to some organisations however it is crucial to priorities activities on the roadmap*."

Since cybersecurity is high on the board agenda list, sufficient resources must be provided to adequately manage cyber risks (Johnson, 2015). The Principal Specialist also acknowledges the effect of cyber-attacks in South Africa and posits, "*due to the recent media coverage on the effect of cybersecurity incidents, cybersecurity is getting more attention*". The CIO concludes, "*Cybersecurity takes precedence for example it receives attention from the Managing Director's office*." Suggesting that management of cybersecurity risks receives attention from the highest level of the organisation to ensure that all staff is on board and therefore understand their role in cyber defence (Islam & Stafford, 2017).

Next, 30% of respondents indicated their organisations approach cybersecurity in the top-down however reactive fashion. The Divisional Head: ICT Governance and Compliance indicated that at the metropolitan municipality "*Influential stakeholders such as Enterprise Risk and Internal Audit are utilised as they carry weight*" suggesting the type of approach the organisation takes towards managing cybersecurity. From a managed ICT service point of view, CISO B states "*organisations are advised to adopt and implement best practice frameworks such as ISO27000 standards as a guide to Information Security Management system*".

There appears to be minimal management support where the organisation's perception is reactive. For instance, the Divisional Head: ICT Governance and Compliance postulate, "*Cybersecurity is perceived as burdensome*" highlighting the lack of management support for cybersecurity initiatives in this organisation. This view correlates with the negative sentiment that cybersecurity perception as the barrier to business activities at the metropolitan municipality. The reactive approach towards cyber risk symbolises that in several organisations cybersecurity is seen as a disruption to business operations (Lewis, 2014). CISO B believes that the approach to cybersecurity depends on the type of leadership

within the organisation. CISO B contends "*It is very much dependent on who the leader and to what extent they have the understanding and appreciation of the impact of cybersecurity i.e. if the CEO is aware of cybersecurity, then cybersecurity initiatives get supported*."

The Client Manager: Cyber Risk and Risk Consulting observe from a customer perspective that cyber risk "…*usually falls into the CIO or CISO purview*". To get management support the Client Manager suggests that EXCO must be "...*fully aware of cyber risks thereby cascading the message from EXCO, MANCO and down to the people on the ground*." Further, "*Oftentimes employers don't appreciate cybersecurity; they see it as a tick box exercise as opposed to strategic value add. With effective management support, cybersecurity can defend the organisation's income stream, customer satisfaction, and loyalty*."

Representing the remaining 10% of respondents wherein organisations indicated bottom-up approach that is reactive, CISO A from a multinational Beverage company state "*The organisation uses project-based approach from the operational and tactical point of view*" illustrating the limited extent of existence of management support in this organisation. In this approach, the organisation's prioritise cybersecurity initiatives based on set metrics and report on benefits realised on investments (Moore et al., 2015). As opposed to an operational project-based view, the IT Audit Manager posits "…*organisation approaches cybersecurity from strategic planning then cascaded down the value chain by implementing controls in a project-based approach*" which suggests that the organisation's top-down approach is proactive.

Cybersecurity has earned its place in the boardrooms of most organisations and executives consider it as a strategic risk that could negatively impact company earnings if left unattended (Newmeyer, 2015). The Client Manager: Cyber Risk and Risk Consulting are of the view that "*cybersecurity must link to organisational strategy, corporate governance and enterprise risk management to be fully effective in an organisation*." The CIO states "*Cybersecurity strategy is embedded in the organisational strategy as a strategic imperative"* highlighting sufficient attention from top management.

In terms of management support, CISO A suggests, "*Support is there due to fear of not knowing what cyber risk is about and limited funding to carry out initiatives which suggest minimal management support*." In opposition, the IT Audit Manager advises that whilst there is management support at his organisation, "*it is insufficient as there is no dedicated resource responsible for cybersecurity on a daily basis*." CISO A is of the view that the structure contributes to how cyber risk is managed as such "*cyber risk is seen as slowing down business*" and therefore the organisation is reactive towards cyber risk management (Lewis, 2014). CISO B supports this view by stating, "*Organisations are mostly reactive*." With the increase of cyber-attacks, there should be more efforts to protect information and business systems (Brangetto & Aubyn, 2015).

The Client Manager: Cyber Risk and Risk Consulting assert "*South Africa is very ignorant around cyber risk understanding whereas in developed territories understand of cyber risk has matured*" implying they are cyber risk resilient to protect revenues (Elmarie Kritzinger & Von Solms, 2012). Further, from the service provider point of view, the Client Manager postulate "*South African companies tend to be reactive towards risk assessments*" as such companies should be proactive to ensure sound cybersecurity posture to manage cyber risk at the right level of decision making within an organisation (Higgs et al., 2016). The CIO concludes, "*The organisation keeps abreast of what is happening in the market and industry* in terms of cyber risks thus staying ahead of the curve."

In conclusion, overwhelmingly, all respondents considered cyber insurance as a mechanism that enables organisations to transfer the risk of financial loss/liability associated with cyber-attacks. It appears that respondents perceive the benefits of cyber insurance to safeguard against financial losses for organisations emanating from cyber breaches as well as complementing the organisation's cybersecurity measures. Cyber insurance shields against data breach or loss, remediation costs such as legal and public relations as well as regulatory fines/penalties and settlement costs takes place. It appears that lack of historical information in the context of South Africa results in a challenge to price risk premium.

Seemingly, the link between cybersecurity approach and management support determines the extent to which cyber risk management occurs within an organisation. The cybersecurity approach can be either top-down or bottom wherein top-down pertains to decision-making or bottom-up pertains to risk assessments. In this study, 60% of respondents appeared to lean towards a top-down approach with proactive management support.

Organisations that have top-down cybersecurity approach and proactive management support have institutionalised risk register driven by organisational risk appetite and risk committee to provide accountability and oversight, communication of cyber risks as well as organisational structures. Organisations that are top-down and proactive seem to have boards that have cyber risk as a top agenda item thereby enhanced revenue streams, customer loyalty, and brand reputation. It appears such boards provide sufficient human and financial resources to manage cyber risks from the highest level of the organisation to ensure that all staff is aware. Therefore, the staff understands their role in cyber defence. Perception of organisations that have established board committees is less likely to be attacked as cyber risks are proactively mitigated through timely discovery and reaction thus long sustainability.

Further, 30% of respondents indicated their organisations approach cybersecurity in the top-down however reactive fashion. There appears to be minimal management support where the organisation's perception is reactive. There seems to be a correlation between the lack of management support for cybersecurity initiatives and cybersecurity perception as the barrier to business activities. It seems reactive approach links with lack of awareness towards cyber risk which symbolises cybersecurity is seen as a burden.

Further, reactive management support is linked with the extent to which executive management understands cyber risk. Suggesting that cybersecurity awareness must be intensified at top management and the message cascaded to staff on the ground to defend income streams, customer loyalty, and brand reputation.

The remaining 10% of respondents represent organisations that indicated a bottom-up approach and reactive management support. These organisations

seem to not drive cyber risk management from a strategic level instead they react to events as they happen. Seemingly, this was prevalent to organisations that do not have structures to monitor and mitigate cyber risks on a frequent basis. As such, this option could result in a negative impact on company earnings. In line with the analysis, the study confirms the proposition, therefore, the organisational approach to cybersecurity determines cyber-risk management support.

## 4.4 Discussion pertaining to Proposition 3

In this section, the relationship between the need for organisations to comply with various government legislations and the cyber insurance adoption takes place. Further, the manner in which an organisation perceives cyber insurance determines organisational appetite for adoption. The research study explored the perceptions per sector to determine the drivers for cyber insurance adoption in South Africa industry.

### 4.4.1 *Cyber insurance adoption in South Africa industry*

The findings of cyber insurance in the South African industry reveals interesting outcomes. During the interview process, participants were asked to indicate whether they have adopted cyber insurance in their respective industries. Table 9 below illustrates the status of cyber adoption from the purposefully selected sample of 10 professionals in the South African industry.

**Table 9: Cyber insurance adoption**

| Cyber Insurance Adoption | | |
|---|---|---|
| **Status** | **Response** | **Ratio** |
| Adopted | 5 | 50% |
| Not Adopted | 5 | 50% |
| **Total** | **10** | **100%** |

As shown in Table 9, out of 10 respondents, 50% indicated that they have adopted cyber insurance in their organisation meanwhile the other 50% indicated that cyber insurance adoption has not occurred in their organisations. Table 10

below illustrates the comparison of cyber insurance adoption by sector and industry.

**Table 10: Cyber insurance in the public and private sectors**

| Adoption by Sector | Adoption by Industry | Not Adopted by Sector | Not Adopted Industry |
|---|---|---|---|
| Public | Metropolitan Municipality | Public | Regulator |
| Public | Financial Services | Public | Logistics |
| Private | Financial Services | Public | Financial Services |
| Private | Telecom | Private | Beverages |
| Private | ICT | Private | Manufacturing |

This represents 40% public whereas 60% constitute private sector organisations that have adopted cyber insurance. Two Respondents namely Divisional Head: ICT Governance & Risk and CIO from Metropolitan Municipality and Financial Services industries, respectively, represented public sector organisations that indicated cyber insurance adoption. To understand the rationale, the Divisional Head stated, "*50% of financial loss has been insured through a cyber insurance service provider based on the risk appetite defined by the enterprise risk management*". Interestingly, the Divisional Head had earlier indicated that the organisation is proactive in terms of cybersecurity however, it lacks management support to drive cyber risk management. The Divisional Head postulate, "*In general, few government institutions have adopted cyber insurance. This municipality could be the first in the public sector*."

Further, the CIO noting the importance of cyber insurance "…*that it gets the organisation to operations quicker after cyber-attack has taken place*" highlighting that the organisation considered potential cybersecurity incident and structured cyber insurance adoption along those lines. From a cyber insurance provider point of view, the Client Manager argues, "*Most South African organisations are not proactive as they seek cyber insurance cover after an attack has occurred*". Further, the Client Manager poses a question "*From a government point of view, what will the hacker do when they get access to citizen information?* The collection, storage, and processing of citizens sensitive data that resides on

information systems present an opportunity for attackers to launch cyber-attacks on public institutions to disrupt the network and gain unauthorised access to data (Kesan & Hayes, 2017).

Three respondents namely the Client Manager: Cyber Risk and Risk Consulting, Manager: Information Security as well as CISO B from Financial Services, Telecom and ICT industries, respectively, represent private sector organisations that indicated cyber insurance adoption. Client Manager posits, "*cyber insurance is necessary since most organisations are data driven in terms Artificial Intelligence, Big Data, Internet of Things, etc.*" highlighting the need to protect data as well the link between cyber insurance and emerging digital technologies (Huang et al., 2018). Unpacking the driver for cyber insurance adoption in the Telecom organisation, the Manager: Information Security contends, "*Business must operate all the time*" suggesting cybersecurity controls complement cyber insurance to manage cyber risk.

Warning potential buyers, CISO B highlights buyers and cyber insurance provider responsibilities stating, "*Buyers must be a lot more informed, implement cyber essentials before signing a cyber insurance policy*" as the repudiation of claim can occur if there is sufficient proof that there were no effective controls. Extending further, "*cyber insurance service providers must explain in simple terms the provisions of policy cover*" highlighting the need to engage cybersecurity specialists to fully understand what is being bought and value it has on business.

However, in the context of South Africa, there seems to be a slow uptake of cyber insurance adoption. The Client Manager concludes, "*South African corporates do not understand the risk and what cover they need*" thus an opportunity for insurance companies to educate potential clients on their product offering. The level of cyber insurance adoption needs to mature in South Africa to ensure resilience from cyber incidents that are occurring at an alarming rate (Woods & Simpson, 2017).

Overwhelmingly on both public and private sectors of the South African industry, government legislations seem to influence cyber insurance adoption. Divisional

Head indicated, "*The metropolitan municipality is highly regulated and must comply with various legislations such as POPI, RICA, MFMA, etc*." A view shared by Manager: Information Security "*Relevant legislation include but not limited to POPI, RICA, GDPR, etc*." highlighting the organisation's readiness to ensuring processes are compliant to protect customer data. CISO B explains that as a managed service company operating in South Africa, "*regulations such as GDPR, POPI, etc. are relevant; however, the organisation also operates in global markets where GDPR is relevant such EU*. Similarly, with Client Manager "*The organisation is Multinational Corporation based in Chicago, London and Johannesburg. In SA, legislation is the driver for cyber insurance adoption thus the organisation adheres to King 4, POPI, etc. In other territories that the organisation operates in, as a Lead Risk Advisor and Lead Insurance Broker globally it must comply with relevant laws and regulations"*. Companies operating in South Africa have a duty to protect customer data in line with the provisions of the POPI act (Swartz & Da Veiga, 2016).

In terms of the five organisations that indicated to have not adopted cyber insurance, three (60%) represent the public sector and the remaining two (40%) represent the private sector. Respondents include the IT Audit Manager, Executive Manager: Enterprise Architecture, IT Governance, Risk, and Compliance as well as Head of IT who represents the regulator, state-owned logistics and publicly owned financial services industries, respectively, from the public sector.

Noting the importance of cyber insurance, the IT Audit Manager states "*Cyber insurance has not been adopted yet which the organisation must look into*. *With increasing cyber-attacks, cyber insurance can provide a financial shield*." Suggesting the lack of accountability or ownership of cyber risks in terms of government regulations in this organisation. The Executive Manager acknowledges, "*That it is impossible to mitigate all possible cyber risks*." Signifying that risks that are prevalent in cyber space warrants cyber insurance thus it is "*unlikely that all cyber risks can be mitigated"*.

Further, the argument "Cyber insurance reduces the effects of cyber-attacks on organisations thereby business continuity." This illustrates the criticality of cyber

insurance, yet "*Cyber insurance has not been adopted, however, the organisation has adopted other insurance covers such as logistics, goods, machinery, and locomotives in line with core operational functions of the organisation*." The Head of IT indicates, "*The organisation complies with all government rules and regulations in South Africa*." However, "*cyber insurance has not been adopted*", as a compensating control "*internal best practices such as COBIT 5 as well as legislation such as POPI are adopted by the organisation*."

In addition, the Executive Manager state, "*The organisation complies with rail safety regulations which are linked to operating licence."* The Executive Manager concludes, "*POPI may not be a factor for this organisation. POPI is more on staff medical records ensuring fit to drive a train*." Companies operating in South Africa must take precautions to protect the privacy for individual's data in their control and ensure compliance with the POPI act (Scharnick et al., 2016).

The remaining two respondents namely CISO A and Principal Specialist represent the Beverages and Manufacturing industries, respectively, from the South African private sector. CISO A concedes that cyber insurance is quite new in the South African industry arguing, "*Few organisations have adopted the cyber insurance*". CISO A states "*currently organisations are not investing in the acquisition of cyber insurance however there is likely to be an increase in cyber insurance as cyber-attacks on organisations gets advanced and legislations such as POPI get introduced*." Principal Specialist concurs with CISO A by stating "*Cyber insurance is new territory, actuarial scientists are finding it difficult to set up the premiums thus not easy to quantify the premium. Cyber insurance is still new in the industry, even insurance companies are able not to price premium correctly, to determine what is covered and not covered*. There seems to be uniformity on the lack of knowledge around cyber insurance, suggesting that cyber insurance provider must educate potential buyers on product offerings and various options. CISO A points out "*There is still a shortage of cyber security skills in SA however no effort from organisations to improve the skillset. This could be the motivation for cyber insurance adoption*." CISO B whose organisation has adopted cyber insurance insists, "*Controls must be in place whether cyber*

*insurance is there or not. Over and above cyber insurance adoption, organisations must emphasise on the effectiveness of cybersecurity controls.*"

Whilst cyber insurance adoption has not materialised, CISO A notes cyber insurance importance by stating, "*Cyber insurance assists businesses against cyber-attacks by insuring against loss, reputation as well as profit thereby protecting the organisation against losses*." Head of IT agrees "…*that cyber insurance assists in protecting the reputation of the organisation*." In terms of government legislation, CISO A and Principal Specialist's organisations are multinational corporations. As such, Principal Specialist contends, "…*there is a lot of regulation to comply. Locally, it is POPI, Cybercrime Bill, ECT Act, etc. Globally it includes GPDPR, Sarbanes Oxley (US)"* This suggests that the organisation operates in a highly regulated environment. Therefore, the organisation has insurance for company assets, "*however cyber insurance has not been adopted*". CISO A elaborates that the organisation complies with various regulations.

Further, "*Since the organisation is global, compliance with POPI, GDPR and other applicable laws comes from multiple regions"*. However, in the South African subsidiary, "*there are no dedicated resources responsible for legal and regulatory compliance*". CISO A concludes, "*There is no appetite for cyber insurance adoption in this organisation. The organisational processes are not mature*." Advising that if there was a cyber-attack there could be a financial loss. Therefore, more education is required to understand what value cyber insurance can add to the organisations as it appears the organisations have invested in technology and not in cyber insurance.

In conclusion, out of 10 respondents, 50% indicated that they have adopted cyber insurance in their organisation meanwhile the other 50% indicated that cyber insurance adoption has not occurred in their organisations. Organisations who have adopted cyber insurance represents 40% public and 60% private. Organisations that have adopted cyber insurance perceive it as important as it gets the organisation quicker to operations after a breach.

However, in the context of South Africa, there seems to be a slow uptake of cyber insurance adoption. Thus, an opportunity for insurance companies to educate potential clients on their product offering. Overwhelmingly on both public and private sectors of the South African industry, government legislations seem to influence cyber insurance adoption. The majority of respondents indicated that applicable South African laws included but not limited to POPI, RICA, MFMA, KING 4, Cybercrime Bill and ECT, etc. thus becoming the driver for cyber insurance adoption. Multinational organisations cited GDPR (UK) and Sarbanes Oxley (US) as applicable in other territories where they operate.

In terms of the five organisations that indicated to have not adopted cyber insurance, three (60%) represent the public sector and the remaining two (40%) represent the private sector. Interestingly, organisations that have not adopted cyber insurance all acknowledge the importance of cyber insurance suggesting that risks that are prevalent in cyberspace warrants cyber insurance.

Most respondents seem to suggest that cyber insurance is quite new in the South African industry arguing that pricing for risk premium as the main challenge as well as not understanding what is covered. Proposing the need to engage and collaborate with cybersecurity specialists to fully understand what cyber insurance covers and the value it has on business. There seems to be uniformity on the lack of knowledge around cyber insurance, suggesting that cyber insurance provider must educate potential buyers on product offerings and various options. There appears to be an increased likelihood of financial losses for organisations that have not adopted cyber insurance. As such, more education is required to understand what value cyber insurance can add to the organisations as it appears the organisations have invested in technology and not in cyber insurance. Therefore, compliance with regulations enables organisations to adopt cyber insurance in the South Africa industry to reduce the risk of financial losses associated with cyber breaches.

## 4.5 Conclusion

Chapter 4, Findings and Discussion provided insightful analysis and interpretation of findings from the sample of 10 respondents. Alignment of objectives, propositions, interview research questions culminated to the emergence of the following three themes:

a) Effective cybersecurity awareness
b) An organisational approach to managing cyber risk
c) Cyber insurance adoption in South Africa industry

The research found that to have effective cybersecurity awareness, boards and executive management must drive change as a strategic imperative, support the initiatives through human and financial resources as well as cascade communication to staff on the ground. Indeed, the awareness of effective cybersecurity technology controls complement cyber insurance to reduce the impact of cyber-attacks in the South Africa industry.

The study found a link between cybersecurity approach and management support that determines the extent to which cyber risk management occurs within an organisation. Organisations that have top-down cybersecurity approach and proactive management support have institutionalised risk register driven by organisational risk appetite and risk committee to provide accountability and oversight, communication of cyber risks as well as organisational structures.

There appears to be minimal management support where the organisation's perception is reactive. There seems to be a correlation between the lack of management support for cybersecurity initiatives and cybersecurity perception as the barrier to business activities. It seems reactive approach links with lack of awareness towards cyber risk which symbolises cybersecurity is seen as a burden. Therefore, organisational approach to cybersecurity determines cyber-risk management support.

The study found a 50/50 split between organisations who have adopted cyber insurance and those who have not adopted cyber insurance. The majority of organisations who have adopted cyber insurance represents public sector (60%)

and the remaining 40% represents the public sector. The biggest driver of adoption of cyber insurance for both public and private sector organisation is government legislation which includes but not limited to POPI, RICA, MFMA, KING 4, Cybercrime Bill and ECT.

here seems to be uniformity on the lack of knowledge around cyber insurance, advising that cyber insurance provider must educate potential buyers on product offerings and various options. There appears to be an increased likelihood of financial losses for organisations that have not adopted cyber insurance. As such, more education is required to understand what value cyber insurance can add to the organisations as it appears the organisations have invested in technology and not in cyber insurance.

In conclusion, a combination of effective cybersecurity awareness, organisational approach to managing cyber risk and compliance with government legislations are factors influencing cyber insurance adoption in the South African industry to reduce the risk of financial losses associated with cyber breaches.

# CHAPTER 5. CONCLUSIONS & RECOMMENDATIONS

## 5.1 Introduction

The purpose of this study was to investigate the factors influencing cyber insurance adoption in South Africa industry. Cyberspace inherently has cyber risks that result in cyber-breaches in the event cybersecurity measures are inadequate. Even with the most sophisticated cybersecurity defence arsenal, cyber-breaches can still occur. Thus, cyber insurance manages residual risk after the implementation of cybersecurity controls. Cyber insurance can provide a financial shield to ensure business resume operations post cyber breach in the South Africa industry.

The research objective was to investigate factors influencing cyber insurance adoption in the South Africa industry from the perspective of technology, organisation, and environment (TOE). To discover factors influencing cyber insurance adoption, the study employed the TOE framework as the basis for exploration leading to an intensive literature review. The review of the literature resulted in the formulation of three propositions in line with TOE. The literature revealed the importance of effective cybersecurity, the relationship between the organisational approach to cybersecurity and management support. Further, a review of literature established that organisations adopt cyber insurance to transfer the risk of financial liability to the third party thereby improved compliance with government regulations.

The study employed a qualitative research method using semi-structured interviews as an instrument to collect data in order to address the research problem. The coding and categorisation of data enabled the analysis of the emerging themes. The study employed saturation, triangulation, and quantitising leading to the systemic interpretation and presentation of data. Data presentation employed a combination of words and tables to support the three propositions. The chapter then concluded with findings confirming propositions using the utmost ethical standards thus ensuring credibility and transferability of the study. The remainder of this chapter integrates findings from the previous chapter with

research objectives. Finally, the presentation of recommendations and suggestions for further research occurs.

## 5.2 Conclusions regarding research objective 1

Factoring cybersecurity awareness as part of the day-to-day work yields desired outcomes for the organisation. To ensure effective cybersecurity awareness, organisations must be proactive and awareness should not be a once-off event. Organisations must create awareness to educate end-users about the risks associated with unsecured practices. Organisations must keep on educating employees and ensuring that employees are kept engaged through exciting content that they are able to relate as cyber threats are becoming more sophisticated. Examples include ensuring that staff is well trained up on the clean desk policy, understanding why the awareness is necessary and inform employees about the various social engineering threats they should lookout. Employees must be cautious when opening suspicious emails/links.

It is critical to have cybersecurity to secure organisational assets. Organisations must be aware of the risks on all the layers of cyberspace thus important to run the security awareness programme on a continuous basis. It is crucial for users to understand what is allowed or not and that cybersecurity risks are clear to end-users. An online security programme should have a technical element to help improve the security posture of an organisation. To ensure effectiveness, cybersecurity must begin at the board and top management levels to drive change. This plays a big role in driving awareness and getting buy-in, which in turn informs the amount of airtime that cybersecurity gets in the organisation. Therefore, organisations in South Africa seem to have low maturity when it comes to effective cybersecurity awareness

## 5.3 Conclusions regarding research objective 2

With the increase of cyber-attacks, there should be more efforts to protect information assets by organisations in South Africa. Cyber insurance is quite new and few organisations have entered the cyber insurance space thus it is not

mature yet. Having cyber insurance does not necessarily improve security controls however it covers financial losses. Cyber insurance only transfers the financial risk but not responsibility. Behavioural risk management is required as opposed to the current blanket approach to cyber risk management. Organisations must ensure there is sufficient budgeting, allocate resources such as people and operate effectively to manage the ever-increasing cyber risks. Implement various solutions in terms of defence in depth and monitoring for cyber resilience.

Defined cybersecurity strategy forms the basis for cybersecurity risk mitigation strategies to ensure the successful operationalisation of the cybersecurity strategy. Effective controls ensure that stakeholders have visibility of security posture. Organisations must understand the risk and align with best practice frameworks that are recognised worldwide. Seemingly, organisations that approach cybersecurity in a proactive manner and have management buy-in tend to have to sound cybersecurity posture, thus mitigating cyber risks. Cyber risk management receives sufficient support to ensure successful mitigation, both in terms of budget allocation and sponsorship in organisations that are proactive and have management support.

Boards and top management must be empowered to make decisions that are in the best interest of the organisation. Therefore, it is important for the CIOs/CISOs to communicate clearly in terms of the resources (human and financial) needed, timeframe and benefits to the organisation. Organisations must use risk registers to identify cybersecurity risks, come up with mitigating strategies and implement countermeasures. Boards must establish a risk committee to oversees and monitor the process of identifying, assessing and responding to cybersecurity risks

## 5.4 Conclusions regarding research objective 3

Organisations in the private sector viewed cyber insurance adoption as one of the strategies to comply with laws in a competitive way. Meanwhile, organisations in the public sector seemed to adopt cyber insurance out of fear of the unknown

in terms of legislation. Cyber insurance can help organisations to meet the requirements of the POPIA and other data protection requirements.

In the context of the South African industry, emerging legislations such as POPI and to some extent for organisations that have global operations seem to propel executive buy-in. This is an angle in which cybersecurity buy-in to the executives as a business imperative and not a nice to have. Cyber insurance adoption should only occur after cybersecurity controls are in place not when there are gaps. It must not be a tick box exercise. Cyber insurance providers must partner with cybersecurity specialists to arrive at better premiums. Organisations should have controls at a reasonable level, thereafter consideration of cyber insurance policy needs to fit for purpose. There must be ongoing/continuous improvement in cyber risk management. Most attacks are happening due to weak controls on web applications. As such, basics from design, implementation, monitoring must be in place.

Buyers must be a lot more informed, implement cyber essentials before signing a cyber policy. It is important to engage cybersecurity specialists to fully understand what is being bought and the value it has on business. Buyers must be mindful of the terms and conditions i.e. if there are no controls, frameworks implemented, monitored and continuous improvement, those basics must be in place. Controls must be in place whether cyber insurance is there or not as a repudiation of a claim can occur if it can be proven that there were no effective controls. The board must own the risk and not transfer it to an insurance provider. Cyber insurance providers must collaborate with cyber specialists to arrive at a better premium.

On a cost versus benefits scale, the price and cost of buying cybersecurity insurance will not be viable and will certainly not make business sense if it will exceed the potential sanctions (penalties and fines) for non-compliance. This is the principle in which many executives view cybersecurity insurance. It can, therefore, be deduced that cyber insurance is currently a grudge purchase and in this study, half of the organisations indicated to have not adopted it.

## 5.5 Recommendations

The adoption of cyber insurance in certain instances raises questions about what law an organisation can ignore due to the transfer of cyber risk to the cyber insurance provider. Cyber insurance must be recognised from a strategic point of view, as such, it is recommended that cybersecurity as function resides with CISO and not CIO as cyber risk is the last thing on CIO's mind. When it comes to cybersecurity, the South African industry should approach it differently. Individual companies are approaching cybersecurity in a siloed manner.

Digital technologies such as Artificial Intelligence, Internet of Things; Big Data, Cloud Computing, and other emerging technologies. are the future. Thus, requires effective cybersecurity to protect the organisational assets. With the exception of high-status enterprises such as the City of Johannesburg, Banks, Liberty, etc. that have recently been attacked by cybercriminals, most entities in South Africa keep such information to themselves. South African companies must disclose cyber attacks as well as associated losses as the study found that most events relate to US and EU countries which were the limitation of this study.

It is recommended that organisations consider the combination of effective cybersecurity awareness, organisational approach to managing cyber risk and compliance with government legislations as factors influencing cyber insurance adoption in the South African industry to reduce the risk of financial losses associated with cyber breaches.

## 5.6 Suggestions for further research

The study was limited to the sample of only 10 professionals purposefully selected to represent public and private sector sentiments on the cyber insurance phenomenon. For future research, the expansion of the study is necessary to include more respondents thus enriching the development of knowledge in the context of South Africa. This will ensure that collected data contains diverse viewpoints in the South African context.

The cyber insurance is relatively new in South Africa; therefore, future studies need to focus on both the demand side as well as the supply side. This will result in the development of knowledge relevant to the South African industry as the review of literature consisted mostly of cases outside of South Africa.

Future research needs to be conducted on quantification of cyber-attacks to determine cyber insurance pricing models thus contributing to knowledge development in this discipline in South Africa and other developing economies. Further, the examination of the relationship between the organisational approach to cyber risk and management support as a determinant for cyber insurance adoption in South Africa needs further scrutiny.

# REFERENCES

*09_Gordon2003FrameworkUsingCyberInsurance.pdf*. (2003). Retrieved 7 August 2019, from http://ns2.dpix.pestiest.hu/~mfelegyhazi/courses/EconSec/readings/09_Gordon2003FrameworkUsingCyberInsurance.pdf

Ab Rahman, N. H., & Choo, K.-K. R. (2015). A survey of information security incident handling in the cloud. *Computers & Security*, *49*, 45–69. https://doi.org/10.1016/j.cose.2014.11.006

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237–248. https://doi.org/10.1080/0144929X.2012.708787

Addington, D., & Manrod, M. (2019). Cyber security threats and solutions for the private sector. *Understanding New Security Threats*.

*Africa number of internet users by country 2019*. (n.d.). Statista. Retrieved 5 August 2019, from https://www.statista.com/statistics/505883/number-of-internet-users-in-african-countries/

Aloul, F. A. (2012). The Need for Effective Information Security Awareness. *Journal of Advances in Information Technology*, *3*(3). https://doi.org/10.4304/jait.3.3.176-183

Aloul, F., Al-Ali, A. R., Al-Dalky, R., Al-Mardini, M., & El-Hajj, W. (2012). Smart Grid Security: Threats, Vulnerabilities and Solutions. *International Journal*

*of Smart Grid and Clean Energy*, 1–6. https://doi.org/10.12720/sgce.1.1.1-6

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. (2013). Measuring the Cost of Cybercrime. In R. Böhme (Ed.), *The Economics of Information Security and Privacy* (pp. 265–300). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-39498-0_12

Arfi, N., & Agarwal, D. S. (2013). *Knowledge of Cybercrime among Elderly*. *4*(7), 7.

Arizona State University, Benjamin, V., Valacich, J. S., University of Arizona, Chen, H., & University of Arizona. (2019). DICE-E: A Framework for Conducting Darknet Identification, Collection, Evaluation with Ethics. *MIS Quarterly*, *43*(1), 1–22. https://doi.org/10.25300/MISQ/2019/13808

Armstrong, H. L., & Forde, P. J. (2003). Internet anonymity practices in computer crime. *Information Management & Computer Security*. https://doi.org/10.1108/09685220310500117

Bahrami, M., & Singhal, M. (2015). The role of cloud computing architecture in big data. In *Information granularity, big data, and computational intelligence* (pp. 275–295). Springer.

Bakhshi, T. (2017). *Social engineering: Revisiting end-user awareness and susceptibility to classic attack vectors*. 1–6.

Bandyopadhyay, T. (2012a). *ORGANIZATIONAL ADOPTION OF CYBER INSURANCE INSTRUMENTS IN IT SECURITY RISK MANAGEMENT– A MODELING APPROACH*. 7.

Bandyopadhyay, T. (2012b). *Organizational Adoption of Cyber Insurance Instruments in IT Security Risk Management– A Modeling Approach*.

Bandyopadhyay, T., & Mookerjee, V. (2017). A model to analyze the challenge of using cyber insurance. *Information Systems Frontiers*, 1–25.

Bandyopadhyay, T., Mookerjee, V. S., & Rao, R. C. (2009). Why IT managers don't go for cyber-insurance products. *Communications of the ACM*, *52*(11), 68. https://doi.org/10.1145/1592761.1592780

Bayoumy, Y. (2018). *Cybercrime Economy-A Netnographic Study on the Dark Net Ecosystem for Ransomware*.

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, *48*, 51–61.

Benjamin, V., & Hsinchun Chen. (2012). Securing cyberspace: Identifying key actors in hacker communities. *2012 IEEE International Conference on Intelligence and Security Informatics*, 24–29. https://doi.org/10.1109/ISI.2012.6283296

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of Cyber Risk: An Empirical Analysis[dagger]. *Geneva Papers on Risk & Insurance; London*, *40*(1), 131–158. http://0-dx.doi.org.innopac.wits.ac.za/10.1057/gpp.2014.19

Böhme, R., & Kataria, G. (2006). *Models and Measures for Correlation in Cyber-Insurance.* WEIS.

Bohme, R., & Schwartz, G. (2010). *Modeling Cyber-Insurance: Towards A Unifying Framework*. 36.

Borum, R., Felker, J., Kern, S., Dennesen, K., & Feyes, T. (2015). Strategic cyber intelligence. *Information & Computer Security*, *23*(3), 317–332. https://doi.org/10.1108/ICS-09-2014-0064

Bossong, R., & Wagner, B. (2018). A Typology of Cybersecurity and Public–Private Partnerships in the Context of the European Union. In *Security Privatization* (pp. 219–247). Springer.

Bouveret, A. (2018). Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3203026

Bowen, G. A. (2008). Naturalistic inquiry and the saturation concept: A research note. *Qualitative Research*, *8*(1), 137–152.

Brangetto, P., & Aubyn, M. (2015). Economic aspects of national cyber security strategies. *Brangetto P., Aubyn MK-S. Economic Aspects of National Cyber Security Strategies: Project Report. Annex*, *1*(9–16), 86.

Brenner, S. W. (2006). Cybercrime jurisdiction. *Crime, Law and Social Change*, *46*(4), 189–206. https://doi.org/10.1007/s10611-007-9063-7

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). *An Analysis of the Nature of Groups Engaged in Cyber Crime* (SSRN

Scholarly Paper ID 2461983). Social Science Research Network. https://papers.ssrn.com/abstract=2461983

Camillo, M. (2017). Cyber risk and the changing role of insurance. *Journal of Cyber Policy*, *2*(1), 53–63.

Carlton, M., & Levy, Y. (2017). Cybersecurity skills: Foundational theory and the cornerstone of advanced persistent threats (APTs) mitigation. *Online Journal of Applied Knowledge Management*, *5*(2), 16–28.

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, *56*, 1–27.

Choi, S., Song, J., Kim, S., & Kim, S. (2013). A model of analyzing cyber threats trend and tracing potential attackers based on darknet traffic: A model of analyzing cyber threats trend and tracing potential attackers. *Security and Communication Networks*, n/a-n/a. https://doi.org/10.1002/sec.796

Chou, T.-S. (2013). Security threats on cloud computing vulnerabilities. *International Journal of Computer Science & Information Technology*, *5*(3), 79.

Choucri, N., Madnick, S., & Ferwerda, J. (2014). Institutions for cyber security: International responses and global imperatives. *Information Technology for Development*, *20*(2), 96–121.

Chronopoulos, M., Panaousis, E., & Grossklags, J. (2017). An options approach to cybersecurity investment. *IEEE Access*, *6*, 12175–12186.

*Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper*. (2018). Cisco. Retrieved 29 July 2019, from https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html

Collins, R. M. L. (2017). *Proactive Cybersecurity Through Active Cyber Defense*.

Connelly, L. M. (2016). Trustworthiness in qualitative research. *Medsurg Nursing*, *25*(6), 435–437.

Contreras, J. L., DeNardis, L., & Teplinsky, M. (2012). Mapping Today's Cybersecurity Landscape America the Virtual: Security, Privacy, and Interoperability in an Interconnected World: Foreword. *American University Law Review*, *5*, 1113–1130. https://heinonline.org/HOL/P?h=hein.journals/aulr62&i=1162

Costa, P., Montenegro, R., Pereira, T., & Pinto, P. (2019). The Security Challenges Emerging from the Technological Developments. *Mobile Networks and Applications*, *24*(6), 2032–2037. https://doi.org/10.1007/s11036-018-01208-0

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Crumpler, W., & Lewis, J. A. (2019). The cybersecurity workforce gap. *Center for Strategic and International Studies, Washington, DC.[Online]. Available: Https://Www. Csis. Org/Analysis/Cybersecurityworkforce-Gap*.

Daud, M., Rasiah, R., George, M., Asirvatham, D., & Thangiah, G. (2018). Bridging the gap between organisational practices and cyber security compliance: Can cooperation promote compliance in organisations? *International Journal of Business and Society*, *19*(1), 161–180.

de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1–7.

*Digital Banking Crime Statistics*. (2019). Retrieved 7 August 2019, from https://www.sabric.co.za/media-and-news/press-releases/digital-banking-crime-statistics/

Dowling, R. (2005). Power, subjectivity and ethics in qualitative research. In *Qualitative research methods in human geography* (pp. 19–29). Oxford University Press.

Dupont, B. (2018). Mapping the International Governance of Cybercrime. *Governing Cyber Security in Canada, Australia and the United States*, *38*, 23.

Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance; London*, *17*(5), 474–491. http://0.search.proquest.com/docview/1847390592/abstract/D84AFF71C59B4F4EPQ/1

Eling, M., & Wirfs, J. H. (2015). *Modelling and Management of Cyber Risk*. 24.

*Five massive data breaches affecting South Africans*. (2018). Fin24. https://www.fin24.com/Companies/ICT/five-massive-data-breaches-affecting-south-africans-20180619-2

Flick, U. (2014). *An introduction to qualitative research*. Sage.

Franke, U. (2017). The cyber insurance market in Sweden. *Computers & Security*, *68*, 130–144.

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report*, *20*(9), 1408.

Gcaza, N., & Solms, R. von. (2017). A Strategy for a Cybersecurity Culture: A South African Perspective. *The Electronic Journal of Information Systems in Developing Countries*, *80*(1), 1–17. https://doi.org/10.1002/j.1681-4835.2017.tb00590.x

*General Data Protection Regulation (GDPR) – Final text neatly arranged*. (2019). General Data Protection Regulation (GDPR). Retrieved 3 August 2019, from https://gdpr-info.eu/

Goel, J. N., & Mehtre, B. (2015). Vulnerability assessment & penetration testing as a cyber defence technology. *Procedia Computer Science*, *57*, 710–715.

Goldman, Z. K., & McCoy, D. (2016). Deterring financially motivated cybercrime. *Journal of National Security Law and Policy*.

Goode, J. (2018). *Comparing Training Methodologies on Employee's Cybersecurity Countermeasures Awareness and Skills in Traditional vs. Socio-Technical Programs*.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM*, *46*(3), 81–85. https://doi.org/10.1145/636772.636774

Grobler, M., & Dlamini, Z. (2012). *Global Cyber Trends a South African Reality*. 8.

Grobler, M., van Vuuren, J. J., & Leenen, L. (2012). Implementation of a Cyber Security Policy in South Africa: Reflection on Progress and the Way Forward. In M. D. Hercheui, D. Whitehouse, W. McIver, & J. Phahlamohlaka (Eds.), *ICT Critical Infrastructures and Society* (Vol. 386, pp. 215–225). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-33332-3_20

Hanus, B., & Wu, Y. “Andy”. (2016). Impact of users’ security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, *33*(1), 2–16.

Harrell, M. C., & Bradley, M. A. (2009). *Data collection methods. Semi-structured interviews and focus groups*. Rand National Defense Research Inst santa monica ca.

Hassan, A. B., Lass, F. D., & Makinde, J. (2012). *Cybercrime in Nigeria: Causes, Effects and the Way Out*. *2*(7), 6.

Hendrix, M., Al-Sherbaz, A., & Bloom, V. (2016). Game Based Cyber Security Training: Are Serious Games suitable for cyber security training? *International Journal of Serious Games*, *3*(1). https://doi.org/10.17083/ijsg.v3i1.107

Herr, T. (2019). *Cyber insurance and private governance: The enforcement power of markets*. Regulation & Governance. https://doi.org/10.1111/rego.12266

Higgs, J. L., Pinsker, R. E., Smith, T. J., & Young, G. R. (2016). The Relationship between Board-Level Technology Committees and Reported Security Breaches. *Journal of Information Systems*, *30*(3), 79–98. https://doi.org/10.2308/isys-51402

Houghton, C. E., Casey, D., Shaw, D., & Murphy, K. (2010). Ethical challenges in qualitative research: Examples from practice. *Nurse Researcher*, *18*(1), 15–25. https://doi.org/10.7748/nr2010.10.18.1.15.c8044

Hox, J. J., & Boeije, H. R. (2005). *Data collection, primary versus secondary*.

Huang, K., Siegel, M., & Madnick, S. (2018). Systematically Understanding the Cyber Attack Business: A Survey. *ACM Comput. Surv.*, *51*(4), 70:1–70:36. https://doi.org/10.1145/3199674

Hung, H. (2016). *Confronting Cybersecurity Challenges through US-Singapore Partnership*.

Hurtaud, S., Flamand, T., de la Vaissiere, L., & Hounka, A. (2015). Cyber insurance as one element of the cyber risk management strategy. *Available at: Www2. Deloitte. Com/Lu/En/Pages/Risk/Articles/Cyber-Insurance-Element-Cyber-Risk-Management-Strategy. Html*.

Hurtaud, S., Flamand, T., & Hounka, A. (2015). *Cyber Insurance as one element of the Cyber risk management strategy*. 6.

Hutchings, A. (2014). Crime from the keyboard: Organised cybercrime, co-offending, initiation and knowledge transmission. *Crime, Law and Social Change*, *62*(1), 1–20. https://doi.org/10.1007/s10611-014-9520-z

*InfoRegSA-POPIA-act2013-004.pdf*. (2013). Retrieved 3 August 2019, from http://www.justice.gov.za/inforeg/docs/InfoRegSA-POPIA-act2013-004.pdf

Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer*, *51*(8), 56–59.

Islam, M., & Stafford, T. (2017). *Information Technology (IT) integration and cybersecurity/security: The security savviness of board of directors*.

*ISO - International Organization for Standardization*. (2019). ISO. Retrieved 28 July 2019, from http://www.iso.org/cms/render/live/en/sites/isoorg/home.html

Jardine, E. (2015). *Global cyberspace is safer than you think: Real trends in cybercrime*.

Johnson, K. N. (2015). Managing cyber risks. *Ga. L. Rev.*, *50*, 547.

Joshi, K., Joshi, K. P., & Mittal, S. (2019). *A Semantic Approach for Automating Knowledge in Policies of Cyber Insurance Services*. 8.

*Justice/Legislation*. (2019). Retrieved 5 August 2019, from http://www.justice.gov.za/legislation/legislation_main.htm

Kesan, J. P., & Hayes, C. M. (2017). Strengthening cybersecurity with cyberinsurance markets and better risk assessment. *Minn. L. Rev.*, *102*, 191.

Kesan, J. P., Majuca, R. P., & Yurcik, W. (2004). *The Economic Case for Cyberinsurance*.

Kesan, J. P., Majuca, R. P., & Yurcik, W. (2005). Cyber-insurance As A Market-Based Solution To The Problem Of Cybersecurity. *WEIS*.

Kesan, J. P., Majuca, R. P., & Yurcik, W. J. (2005). *CYBERINSURANCE AS A MARKET-BASED SOLUTION TO THE PROBLEM OF CYBERSECURITY—A CASE STUDY*. 47.

Khalili, M. M., Naghizadeh, P., & Liu, M. (2018). Designing Cyber Insurance Policies: The Role of Pre-Screening and Security Interdependence. *IEEE Transactions on Information Forensics and Security*, *PP*, 1–1. https://doi.org/10.1109/TIFS.2018.2812205

King, N. J., & Raja, V. (2012). Protecting the privacy and security of sensitive customer data in the cloud. *Computer Law & Security Review*, *28*(3), 308–319.

Kopp, E., Kaffenberger, L., & Jenkinson, N. (2017). *Cyber risk, market failures, and financial stability*. International Monetary Fund.

Kritzinger, E, & Solms, S. (2013). A Framework for Cyber Security in Africa. *Journal of Information Assurance & Cybersecurity*, 1–10. https://doi.org/10.5171/2012.322399

Kritzinger, Elmarie, & Von Solms, S. (2012). A framework for cyber security in Africa. *Journal of Information Assurance & Cybersecurity*, *2012*, 1.

Kshetri, N. (2015a). Cybercrime and cybersecurity issues in the BRICS economies. *Journal of Global Information Technology Management*, *18*(4), 245–249.

Kshetri, N. (2015b). India's cybersecurity Landscape: The roles of the private sector and public-private partnership. *IEEE Security & Privacy*, *13*(3), 16–23.

Kshetri, N. (2019). *Cybercrime and Cybersecurity in Africa*.

Kumar, S., & Carley, K. M. (2016). *Understanding DDoS cyber-attacks using social media analytics*. 231–236.

Kumari, N., & Mohapatra, A. (2016). *An insight into digital forensics branches and tools*. 243–250.

Kuper, A., Lingard, L., & Levinson, W. (2008). Critically appraising qualitative research. *Bmj*, *337*, a1035.

Langa, M. (2016). *Adapting information technology management for effective information technology strategy leadership*.

Larson, S. (2015). The cyber security fair: An effective method for training users to improve their cyber security behaviors. *Information Security Education Journal*, *2*(1), 11–19.

Lavorgna, A., & Sergi, A. (2016). Serious, therefore organised? A critique of the emerging" cyber-organised crime" rhetoric in the United Kingdom. *International Journal of Cyber Criminology*, *10*(2), 170–187.

Lee, C.-C., Cheng, H. K., & Cheng, H.-H. (2007). An empirical study of mobile commerce in insurance industry: Task–technology fit and individual differences. *Decision Support Systems*, *43*(1), 95–110. https://doi.org/10.1016/j.dss.2005.05.008

Leitner, C., & Stiefmueller, C. M. (2019). Disruptive Technologies and the Public Sector: The Changing Dynamics of Governance. In A. Baimenov & P. Liverakos (Eds.), *Public Service Excellence in the 21st Century* (pp. 237–274). Springer Singapore. https://doi.org/10.1007/978-981-13-3215-9_8

Lewis, J. A. (2014). National perceptions of cyber threats. *Strategic Analysis*, *38*(4), 566–576.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13–24.

Linkov, I., Anklam, E., Collier, Z. A., DiMase, D., & Renn, O. (2014). Risk-based standards: Integrating top–down and bottom–up approaches. *Environment Systems and Decisions*, *34*(1), 134–137. https://doi.org/10.1007/s10669-014-9488-3

Lipson, H. (2002). *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*. https://doi.org/10.1184/R1/6585395.v1

Liu, L. (2016). Using Generic Inductive Approach in Qualitative Educational Research: A Case Study Analysis. *Journal of Education and Learning*, *5*(2), 129. https://doi.org/10.5539/jel.v5n2p129

Manda, M. I., & Backhouse, J. (2017). *Digital transformation for inclusive growth in South Africa. Challenges and opportunities in the 4th industrial revolution*. 2nd African Conference on Information Science and Technology, Cape Town, South Africa.

Markham, A. (2012). Fabrication as Ethical Practice. *Information, Communication & Society*, *15*(3), 334–353. https://doi.org/10.1080/1369118X.2011.641993

Marotta, A., Martinelli, F., Yautsiukhin, A., & Nanni, S. (2015). *A Survey on Cyber-Insurance*. 53.

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). Qualitative data analysis: A methods sourcebook. 3rd. *Ed: Thousand Oaks, CA: Sage*.

Mo, Y., Kim, T. H.-J., Brancik, K., Dickinson, D., Lee, H., Perrig, A., & Sinopoli, B. (2011). Cyber–physical security of a smart grid infrastructure. *Proceedings of the IEEE*, *100*(1), 195–209.

Mooketsi, T. R. (2015). *Factors affecting internet and broadband penetration in South African ordinary schools*.

Moore, T., Dynes, S., & Chang, F. R. (2015). Identifying how firms manage cybersecurity investment. *Available: Southern Methodist University.*

*Available at: Http://Blog. Smu. Edu/Research/Files/2015/10/SMU-IBM. Pdf (Accessed 2015-12-14)*, *32*.

Moyo, A. (2018). *SA's average data breach costs escalate*. ITWeb. https://www.itweb.co.za/content/Pero37ZgOnXMQb6m

Mubarak Alharbi, I., Zyngier, S., & Hodkinson, C. (2013). Privacy by design and customers' perceived privacy and security concerns in the success of e-commerce. *Journal of Enterprise Information Management*, *26*(6), 702–718. https://doi.org/10.1108/JEIM-07-2013-0039

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not? *Decision Support Systems*, *56*, 11–26. https://doi.org/10.1016/j.dss.2013.04.004

Muller, L. P. (2015). Cyber Security Capacity Building in Developing Countries. *Opportunities and Challenges. Norwegian Institute of International Affairs*.

Nawang, N. I. (2017). *Combating anonymous offenders in the cyberspace: An overview of the legal approach in Malaysia*. 13–18.

Newmeyer, K. P. (2015). Elements of national cybersecurity strategy for developing nations. *National Cybersecurity Institute Journal*, *1*(3), 9–19.

Nikolov, L., & Slavyanov, V. (2018). *Network infrastructure for cybersecurity analysis*. International scientific conference.

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evidence-Based Nursing*, *18*(2), 34–35.

North, J., & Pascoe, R. (2016). Cyber security and resilience It's all about governance. *Governance Directions*, *68*(3), 146.

Opdenakker, R. (2006). *Advantages and disadvantages of four interview techniques in qualitative research*. *7*.

Parry, O., & Mauthner, N. S. (2004). Whose Data are They Anyway?: Practical, Legal and Ethical Issues in Archiving Qualitative Research Data. *Sociology*, *38*(1), 139–152. https://doi.org/10.1177/0038038504039366

Patil, S. R., Cates, S., & Morales, R. (2005). Consumer food safety knowledge, practices, and demographic differences: Findings from a meta-analysis. *Journal of Food Protection*, *68*(9), 1884–1894.

Pescatore, J. (2017). Cyber Security Trends: Aiming Ahead of the Target to Increase Security in 2017. *SANS Institute InfoSec Reading Room*.

Peters, G., Shevchenko, P. V., & Cohen, R. (2018). Understanding cyber-risk and cyber-insurance. *Macquarie University Faculty of Business & Economics Research Paper*.

Pfleeger, S. L., Sasse, M. A., & Furnham, A. (2014). From weakest link to security hero: Transforming staff security behavior. *Journal of Homeland Security and Emergency Management*, *11*(4), 489–510.

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets. *Journal of Management Information Systems*, *32*(4), 179–214. https://doi.org/10.1080/07421222.2015.1138374

Raghavan, A., & Parthiban, L. (2014). The effect of cybercrime on a Bank's finances. *International Journal of Current Research & Academic Review*, *2*(2), 173–178.

Randall, S., & Koppenhaver, T. (2004). Qualitative data in demography: The sound of silence and other problems. *Demographic Research*, *11*, 57–94. https://doi.org/10.4054/DemRes.2004.11.3

Ratten, V. (2016). Continuance use intention of cloud computing: Innovativeness and creativity perspectives. *Journal of Business Research*, *69*(5), 1737–1740. https://doi.org/10.1016/j.jbusres.2015.10.047

Roberts, L. D. (2015). Ethical issues in conducting qualitative research in online communities. *Qualitative Research in Psychology*, *12*(3), 314–325.

Rohmeyer, P., & Bayuk, J. L. (2019). What Can We Do? In *Financial Cybersecurity Risk Management* (pp. 105–124). Springer.

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity*, *5*(1). https://doi.org/10.1093/cybsec/tyz002

Rothrock, R. A., Kaplan, J., & Van Der Oord, F. (2018). The board's role in managing cybersecurity risks. *MIT Sloan Management Review*, *59*(2), 12–15.

Rowe, B. R., & Gallaher, M. P. (2006). *Private sector cyber security investment strategies: An empirical analysis*. The fifth workshop on the economics of information security (WEIS06).

Ryan, A. B. (2006). Methodology: Analysing qualitative data and writing up your findings. *Researching and Writing Your Thesis: A Guide for Postgraduate Students*, 92–108.

Sawyer, B. D., & Hancock, P. A. (2018). Hacking the human: The prevalence paradox in cybersecurity. *Human Factors*, *60*(5), 597–609.

Scharnick, N., Gerber, M., & Futcher, L. (2016). *Review of data storage protection approaches for POPI compliance*. 48–55.

Shackelford, S. J., Proia, A. A., Martell, B., & Craig, A. N. (2015). Toward a global cybersecurity standard of care: Exploring the implications of the 2014 NIST cybersecurity framework on shaping reasonable national and international cybersecurity practices. *Tex. Int'l LJ*, *50*, 305.

Sharma, P., Doshi, D., & Prajapati, M. M. (2016). Cybercrime: Internal security threat. *2016 International Conference on ICT in Business Industry Government (ICTBIG)*, 1–4. https://doi.org/10.1109/ICTBIG.2016.7892727

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, *52*(1), 92–100. https://doi.org/10.1016/j.compedu.2008.06.011

Shetty, N., Schwartz, G., Felegyhazi, M., & Walrand, J. (2010). Competitive Cyber-Insurance and Internet Security. In T. Moore, D. Pym, & C. Ioannidis (Eds.), *Economics of Information Security and Privacy* (pp. 229–247). Springer US. https://doi.org/10.1007/978-1-4419-6967-5_12

Shetty, S., McShane, M., Zhang, L., Kesan, J. P., Kamhoua, C. A., Kwiat, K., & Njilla, L. L. (2018). Reducing informational disadvantages to improve cyber risk management. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *43*(2), 224–238.

Silva, J. D. C., Rodrigues, J. J. P. C., Saleem, K., Kozlov, S. A., & Rabêlo, R. A. L. (2019). M4DN.IoT-A Networks and Devices Management Platform for Internet of Things. *IEEE Access*, *7*, 53305–53313. https://doi.org/10.1109/ACCESS.2019.2909436

Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, *60*, 154–176.

*SolarWinds Federal Cybersecurity Survey Report—January 2019*. (2019). 30.

Stallings, W., Brown, L., Bauer, M. D., & Bhattacharjee, A. K. (2012). *Computer security: Principles and practice*. Pearson Education Upper Saddle River, NJ, USA.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, *24*(2), 124–133.

*State-of-cybersecurity_res_eng_0316.pdf*. (2016). Retrieved 3 August 2019, from https://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf

Sujithra, M., Padmavathi, G., & Narayanan, S. (2015). Mobile device data security: A cryptographic approach by outsourcing mobile data to cloud. *Procedia Computer Science*, *47*, 480–485.

Susanto, H., & Almunawar, M. N. (2012). *Information Security Awareness Within Business Environment: An IT Review*. 25.

Sutherland, E. (2017). Governance of cybersecurity-The case of South Africa. *African Journal of Information and Communication*, *20*, 83–112.

Süzen, A. A. (2020). A Risk-Assessment of Cyber Attacks and Defense Strategies in Industry 4.0 Ecosystem. *International Journal of Computer Network & Information Security*, *12*(1).

Swartz, P., & Da Veiga, A. (2016). *PoPI Act-opt-in and opt-out compliance from a data value chain perspective: A South African insurance industry experiment*. 9–17.

Tabansky, L. (2011). *Basic Concepts in Cyber Warfare*. 18.

Tabansky, L. (2017). Cyber Security Challenges: The Israeli Water Sector Example. In *Cyber-Physical Security* (pp. 205–219). Springer.

Taherdoost, H. (2016). Sampling methods in research methodology; how to choose a sampling technique for research. *How to Choose a Sampling Technique for Research (April 10, 2016)*.

Talmy, S. (2010). Qualitative interviews in applied linguistics: From research instrument to social practice. *Annual Review of Applied Linguistics*, *30*, 128–148.

Thomas, D. R. (2003). *A general inductive approach for qualitative data analysis*. 11.

Tianfield, H. (2016). *Cyber security situational awareness*. 782–787.

Tiirmaa-Klaar, H. (2016). Building national cyber resilience and protecting critical information infrastructure. *Journal of Cyber Policy*, *1*(1), 94–106.

Tøndel, I. A., Meland, P. H., Omerovic, A., Gjære, E. A., & Solhaug, B. (2015). *Using cyber-insurance as a risk management strategy: Knowledge gaps and recommendations for further research*.

Toregas, C., & Zahn, N. (2014). *Insurance for Cyber Attacks: The Issue of Setting Premiums in Context*. 20.

Tornatzky, L. G., Fleischer, M., & Chakrabarti, A. K. (1990). *Processes of technological innovation*. Lexington books.

Van Niekerk, B. (2017). An analysis of cyber-incidents in South Africa. *African Journal of Information and Communication*, *20*, 113–132.

Vicevich, D. L. (2018). The Case for a Federal Cyber Insurance Program Comment. *Nebraska Law Review*, *2*, [i]-606. https://heinonline.org/HOL/P?h=hein.journals/nebklr97&i=567

von Solms, B., & von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information & Computer Security*, *26*(1), 2–9. https://doi.org/10.1108/ICS-04-2017-0025

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102.

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Wang, S. S. (2019). Integrated framework for information security investment and cyber insurance. *Pacific-Basin Finance Journal*, *57*, 101173.

White, G. (2009). Strategic, tactical, & operational management security model. *Journal of Computer Information Systems*, *49*(3), 71–75.

Wirfs, J. H. (2016). *How to Organize Cyber Risk Transfer?*

Woods, D., & Simpson, A. (2017). Policy measures and cyber insurance: A framework. *Journal of Cyber Policy*, *2*(2), 209–226. https://doi.org/10.1080/23738871.2017.1360927

Yang, Z., & Lui, J. C. S. (2014). *Contents lists available at ScienceDirect Performance Evaluation*.

Yeh, C. J., & Inman, A. G. (2007). Qualitative data analysis and interpretation in counseling psychology: Strategies for best practices. *The Counseling Psychologist*, *35*(3), 369–403.

Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A survey on wireless security: Technical challenges, recent advances, and future trends. *Proceedings of the IEEE*, *104*(9), 1727–1765.

*ZYKLN2E3.pdf*. (2017). Retrieved 5 August 2019, from https://www.ibm.com/downloads/cas/ZYKLN2E3

# APPENDIX A – Semi-structured Interview Questions

## *I) SETTING THE SCENE*

| **1. How long have you been a professional, your job title and description?** | |
|---|---|
| **Response** | |

| **2. What is your perception of the general term "Industry 4.0: The 4th Industrial Revolution" or 4IR?** | |
|---|---|
| **Response** | |

## *II) CYBER SECURITY*

| **3. Describe your perception of the link between 4IR and cybersecurity.** | |
|---|---|
| **Response** | |

| **4. What is your general perception of cybersecurity and/or cyber insurance?** | |
|---|---|
| ☐ **Secure electronic data activity on servers, workstations and mobile devices** | ☐ **Facilitates implementation of cybercrime laws** |
| ☐ **Detects and prevents organised crime groups** | ☐ **Improves knowledge about secure practices** |
| ☐ **Detects, prevents and corrects external and internal threats** | ☐ **Can be used to improve internal controls** |
| ☐ **Traces attackers** | ☐ **Mitigate against cyber risks** |
| ☐ **Compromise privacy and sense of control** | ☐ **Lack explainable understanding of cyber insurance** |

☐ **General Comment:**

*III)* ***TECHNOLOGY***

| | |
|---|---|
| **5.** | **Describe how your organisation ensures availability of cybersecurity technology?** |

| | |
|---|---|
| **Response** | |

| |
|---|
| **6. Describe how your organisation approaches the effectiveness of cybersecurity?** |

| | |
|---|---|
| **Response** | |

## *IV) ORGANISATION*

| **7.** | **Describe how your organisation approach cyber risk management?** |
|---|---|
| **Response** | |
| **8.** | **Describe top management support to ensuring integrated risk management for your organisation?** |
| **Response** | |

## *V) ENVIRONMENT*

| **9.** | **Describe the extent to which your organisation must comply with government regulations such as the Protection of Personal Information?** |
|---|---|

| | |
|---|---|
| **Response** | |

| | |
|---|---|
| **10.** | **Describe the nature of your industry and how it approaches the adoption of cyber insurance?** |
| **Response** | |

Thank you for your participation!

- - - oOo - - -

# APPENDIX B – Participant Information Sheet

## Participant Information Sheet

Dear Sir / Madam,

My name is Nkosinathi Sphiwe Mbatha and I am a Masters student in Digital Business at the University of the Witwatersrand in Johannesburg. As part of my studies, I have to undertake a research project, and I am investigating factors influencing cyber insurance adoption in South Africa industry. The aim of this research project is to investigate the factors influencing cyber insurance adoption in South Africa.

As part of this project, I would like to invite you to take part in an interview. This activity will involve 10 interview questions and will take around 45-60 minutes. With your permission, I would also like to record the interview using a digital mobile phone. You will not receive any direct benefits from participating in this research, and there are no disadvantages or penalties for not participating. You may withdraw at any time or not answer any question if you do not want to. The interview will be completely confidential and anonymous as I will not be asking for your name or any identifying information, and the information you give to me will be held securely and not disclosed to anyone else. I will be using a pseudonym (false name) to represent your participation in my final research report. If you experience any distress or discomfort at any point in this process, we will stop the interview or resume another time.

If you have any questions anytime during the research process about this research, feel free to contact me or my supervisor on the details listed below. This study will be written up as a research report which will be available online through the university library website. If you wish to receive a summary of this report, I will be happy to send it to you (optional). If you have any concerns or complaints regarding the ethical procedures of this study, you are welcome to contact the University Human Research Ethics Committee (Non-Medical), telephone +27(0) 11 717 1408, email Shaun.Schoeman@wits.ac.za

Yours sincerely,

Mr Nkosinathi Sphiwe Mbatha

2261524@students.wits.ac.za / 0725105773

Supervisor: Mthandeni Langa, mthandeni@gmail.com, 0829482920

# Consent Form

**Title of project: Factors influencing cyber insurance adoption in South Africa industry**

**Name of researcher: Nkosinathi Sphiwe Mbatha**

I, …….., agree to participate in this research project. The research has been explained to me and I understand what my participation will involve. Please circle the relevant options below.

I agree that my participation will remain anonymous YES NO

I agree that the researcher may use anonymous quotes

in his / her research report YES NO

I agree that the interview may be audio recorded YES NO

I agree that the information I provide may be used YES NO

anonymously by other researchers following this project

…… (signature)

…… (name of participant)

…… (date)