Cybersecurity and Governance Framework of Information Systems in the South African Mining Industry

by

ANTHONY GRAHAM PLESSIS

submitted in accordance with the requirements for

the degree of

MASTER OF COMMERCE

in the subject of

BUSINESS MANAGEMENT

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR

PROFESSOR TSHILIDZI ERIC NENZHELELE

November 2021

DECLARATION

Name: **Anthony Graham Plessis**

Student number: **3325-102-5**

Degree: **Master of Commerce: Business Management**

CYBERSECURITY AND GOVERNANCE FRAMEWORK OF INFORMATION SYSTEMS IN THE SOUTH AFRICAN MINING INDUSTRY

I declare that the above dissertation is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

I further declare that I submitted the dissertation to originality checking software and that it falls within the accepted requirements for originality.

I further declare that I have not previously submitted this work, or part of it, for examination at Unisa for another qualification or at any other higher education institution.

2 NOVEMBER 2021

SIGNATURE DATE

ACKNOWLEDGEMENTS

I would like to thank God for the wisdom and perseverance that He has given me during my master’s studies, and indeed, throughout my life. You are Alpha and Omega. "I can do everything through Him who gives me strength." (Philippians 4: 13).

To my late father, Benjamin Plessis, you have been an inspiration to me throughout my life. You were a principled father and your guidance and encouragement to do well, inspired me to stay positive in the midst of life challenges. My late brothers, James Plessis, and Pascal Plessis, you have always supported and encouraged me to do well. I will forever remember you for inspiring and supporting me in life and to succeed in everything I pursued. I think and reminisce about you every day and you inspired me in spirit to complete this qualification. May your souls rest in peace and rise in glory.

To my mother, Lulu Plessis, I thank you with deep gratitude for nurturing and raising me whilst instilling an independent and positive spirit in me. I am deeply grateful to my loving, supportive, encouraging, and patient wife, Nancy Plessis, whose faithful support during the journey of this study is greatly appreciated. I am forever grateful to my loving and supporting daughters, Carmen, and Liesel Plessis, for your enduring and everlasting love and support. To my loving wife and daughters, I thank you with deep appreciation for your faith and confidence in me to continue to drive my quest for excellence and purpose.

I would like to take this opportunity to express my sincere gratitude to my supervisor, Professor Tshilidzi Eric Nenzhelele for your patience, support, guidance, and encouragement. I could not have asked for a more supportive supervisor and would not have been able to reach this milestone without your support. Thank you to Dr Tawanda Chiyangwa for conducting the statistical analysis of this dissertation. The University of South Africa (UNISA) for the financial assistance. I would also like to thank all the participants in the South African mining industry for their contribution that made the outcome and success of this study possible.

ABSTRACT

South Africa’s political, social, and economic landscape has been dominated by mining, given that, for so many years, the sector has been the mainstay of the South African economy. The South African mining industry can be attributed to the high level of the industries’ technical and production expertise, as well as its comprehensive research and development activities. Mining in South Africa is of interest in that mining enterprises are particularly vulnerable to the theft of corporate information as opposed to operational information. ICT security has never been more important to mining enterprises than now. Mining enterprises face cybersecurity threats as mining is a contentious area and not everyone is pro-mining. Due to the occurrence of several high-impact cybersecurity incidents, it is apparent that the new cyberspace not only offers benefits but also generates cyber-risks to all industries. Consequently, enterprises must have comprehensive plans to deal with information systems security attacks. The purpose of this study was to assess cybersecurity in the South African mining industry.

This study was quantitative and descriptive in nature and used a web-based questionnaire to collect data. This study concluded that the enterprises in the South African mining industry conform to IT governance practices, have an appreciation and support for information security access control processes, excellent network security infrastructure and reliable information security policies. However, management and executives in the South African mining industry is not easily convinced to fund security solutions. Furthermore, non-compliant or weak and unreliable control measures will essentially expose enterprises to negative IT security audit findings, cyber security risks and data breaches to classified information. The study established factors that influence information security in the South African mining industry positively and negatively. Recommendations are made to help mining enterprises to protect their ICT environments more securely, efficiently, and effectively.

KEY WORDS

Mining; cybersecurity; data breaches; hacking; policies; procedures; auditable controls; data; information; communication; network; technology.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

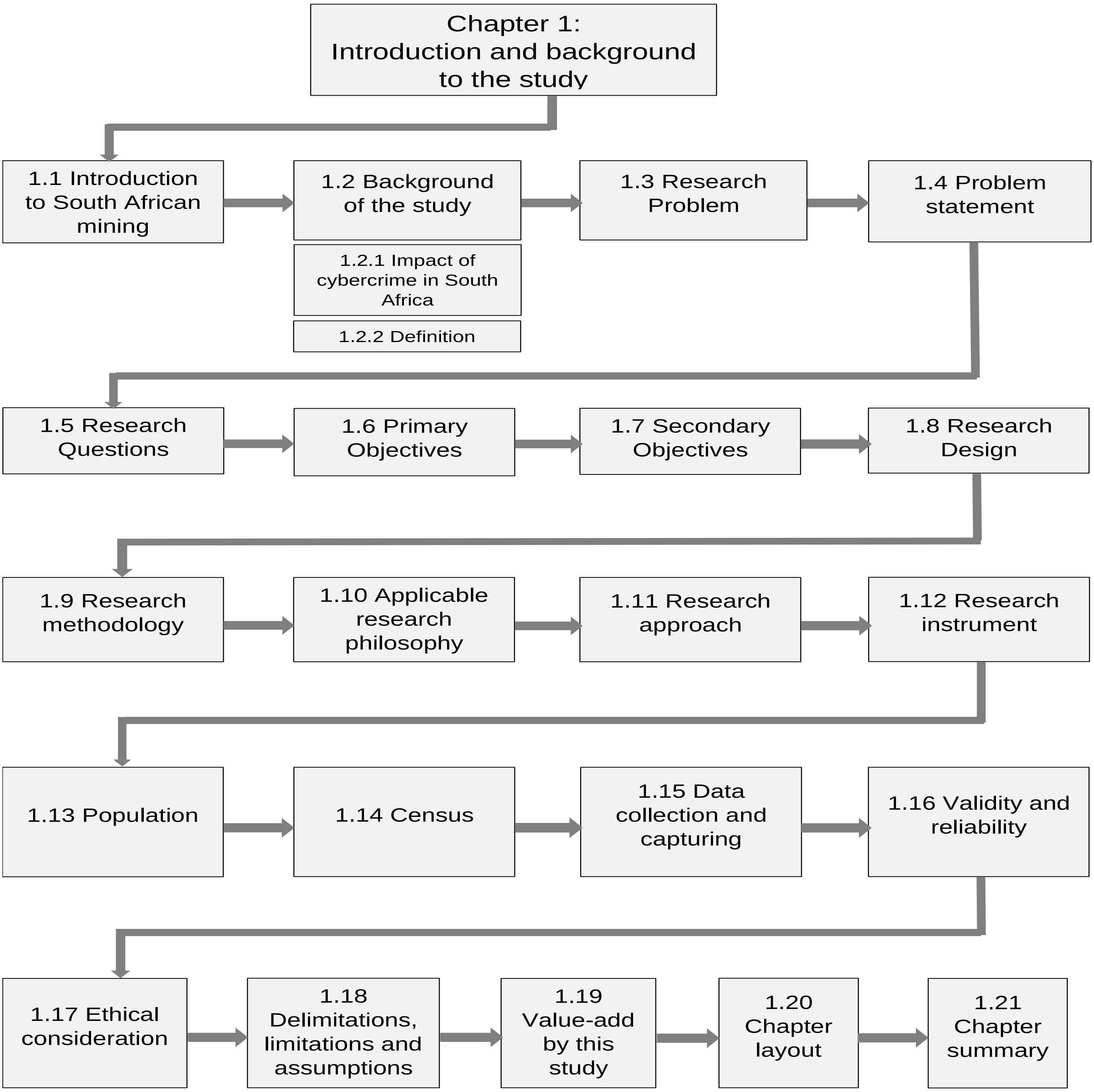
APT	Advanced Persistent Threats
AMSC	Amricam Superconductor Corporation
ARPA	Department of Defence’s Advanced Research Projects Agency
BEE	Black Economic Empowerment
CERN	European Organization for Nuclear Research
CIA	Central Intelligence Agency
CIO	Chief Information Officer
CM	Chamber of Mines
CNN	Cable News Network
COMSA	Chamber of Mines of South Africa
CSIR	Council for Scientific and Industrial Research
DDoS	Distributed Denial of Service
DMR	Department of Mineral Resources
DST	Department of Science and Technology
EC3	European Cybercrime Centre
ECT Act	Electronic Communication and Transactions Act
EFA	Exploratory Factor Analysis
EFT	Electronic Fund Transfer
EMV Chip	Europay, MasterCard, Visa
FBI	Federal Bureau of Investigation
FNB	First National Bank

GDP	Gross Domestic Product
GEIT	Governance of Enterprise IT
ICT	Information and Communications Technologies
IDS	Intrusion Detection System
ISACA	Information Systems Audit and Control Association
ISCOR	Iron and Steel Corporation of South Africa
INTERPOL	International Criminal Police Organization
IoT	Internet of Things
ISF	Information Security Framework
ISMS	Information Security Management System
ISO	International Organisation for Standardisation
ISP	Internet Service Provider
IT	Information Technology
ITGI	Information Technology Governance Institute
ITRM	Information Technology Risk Management
J-Cat	Joint Cybercrime Action Taskforce
JSE	Johannesburg Securities Exchange
KMO	Kaiser-Meyer-Olkin Measure of Sampling Adequacy
MALWARE	Malicious Software
MES	Micro-Electromechanical Systems
MIT	Massachusetts Institute of Technology
MS	Microsoft
NASA	National Aeronautics and Space Administration

NIST	National Institute of Standards and Technology
OIT	Online Identity Theft
PCA	Principal Component Analysis
PGM	Platinum Group Metals
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POPI Act	Protection of Personal Information Act 4 of 2013
POS	Point of Sale
PwC	PricewaterhouseCoopers
SAMMRI	South African Minerals to Metals Research Institute
SIG	Special Interest Groups
SITA	State Information Technology Agency
SOX	Sarbanes-Oxley Act
SSA	State Security Agency
TCP/IP	Transmission Control Protocol/Internet Protocol
TIA	Technology Innovation Agency
UCLA	University of California, Los Angeles
WCC	White Collar Crime
WEF	World Economic Forum

CHAPTER 1: INTRODUCTION AND BACKGROUND TO THE STUDY

The chapter outlines a background of the study, research problem, research aim, and research objectives. This is followed by the research design, methodology, philosophy, approach, and instrument. The chapter is concluded by the research population sampling, data collection, capturing and analysis, validity, reliability, ethical consideration, delimitations, limitations, assumptions, and value add by this study.


Chapter 1: Introduction and background to the study
1.1 Introduction to South African mining
1.2 Background of the study
1.2.1 Impact of cybercrime in South Africa
1.2.2 Definition
1.3 Research Problem
1.4 Problem statement
1.5 Research Questions
1.6 Primary Objectives
1.7 Secondary Objectives
1.8 Research Design
1.9 Research methodology
1.10 Applicable research philosophy
1.11 Research approach
1.12 Research instrument
1.13 Population
1.14 Census
1.15 Data collection and capturing
1.16 Validity and reliability
1.17 Ethical consideration
1.18 Delimitations, limitations and assumptions
1.19 Value-add by this study
1.20 Chapter layout
1.21 Chapter summary

1.1 INTRODUCTION TO SOUTH AFRICAN MINING

The South African mining industry is valued as the fifth-largest contributor to the Gross Domestic Product (GDP) (The Chamber of Mines South Africa; 2013; South African Yearbook 2012/13. Mineral Resources). The South African Reserve Bank reported in their 2013 annual economic report that the mining industry contributed 5.7% (2013) and 5.1% (2012) to the GDP of South Africa. The annual report of the Johannesburg Securities Exchange (JSE) reported that at the end of 2011, the value of mining shares listed was R1.4 trillion, or 29% of the total value of the JSE. The South African mining industry is held in high regard, and in 2010 the Cabinet of South Africa earmarked the industry as a critical stimulator to grow the economy in the country.

It creates millions of jobs for South Africans and foreign nationals. As a result, the government keeps making resources available for the mining industry (Gordhan, 2012). The accomplishment of the mining industry is attributed to a high level of technical and production expertise, research, and development (Chamber of Mines of South Africa, 2013). Kearney (2012) states that the processing facilities in South African are world-class, making the industry a world leader of ground-breaking technologies, that enable low-grade superfine iron ore to be converted into high-quality iron units.

According to Paladion (2012), the mining industry is like other manufacturing industries that are data-intensive and vulnerable to cyber-threats as it deals with information about finance, enterprise strategies, business processes, product designs, shipping, inventory, etc. Paladion (2012) concludes that there is a need for reliable and accurate information and thus demands good information-security governance practices in the industry to protect the enterprises against information-security breaches. Van Grembergen, W. & De Haes (2012) state that enterprises need a well-designed information-system governance framework to mitigate any information security risks.

Cyber threats are a huge concern within the mining industry and have the potential to be amongst the top ten strategic risks of enterprises (Kosich, 2016; Elliot, 2014). Ernst & Young also expressed their concern when they reported in 2013 (Ernst & Young, 2013) that cyber-hacking and reports of the information security systems in the mining industry are being breached and developing as one of the top security risks. The South

African Minerals to Metals Research Institute (SAMMRI) believes that there are significant opportunities to define an Information Security Governance framework in the mineral processing sector to improve the efficiency of processes.

SAMMRI in 2014 pointed out that poor development and implementation of relevant technologies and lack of Information and Communication Technology (ICT) skills are challenges to the growth of the mining industry (SAMMRI, 2014). The Department of Science and Technology (DST) conducted a study in the year 2012 on the mining industry recommended the use of technology for faster growth. Sawada and Managi (2013) state that the recommendation by the DST is noteworthy because the information in mining is becoming essential as it enables mining enterprises to formulate sound policies, formulate strategies, plan future forecasts, make informed decisions and assist with providing real-time information.

The Information Technology Governance Institute (ITGI) in 2012 stated (Spremic, 2012) that enterprises are dealing with a global revolution in information governance that severely affects their information-management practices resulting in an urgent need to evaluate the information being protected when providing enabled services. A further concern raised by the ITGI is that current and newly defined laws on the retention and privacy of information, desperately need an approach to govern information to protect the most critical assets of an enterprise to guard against vulnerabilities and reputational damage. CNN states (CNN, 2015) that there are more than 317 million malicious software viruses and that 80% of large enterprises were targeted by cybercriminals.

Moreover, it was reported by CNN that the mining industry has become the most targeted sector. CNN cited an example and reported that hackers gained access to information about an energy enterprise and stole a draft document of a potentially profitable energy drilling spot. The hackers were arrested after trying to sell the information on the black market to stock traders. Symantec Corporation in 2013 reported that cybercrime continues to be increasing and has become a global concern. The total global cost to enterprises of cybercrime increased (US$113 billion; up from $110 billion) and the cost per individual victim increased on average ($298; up from $197).

Despite the mining industry investing heavily in employee safety, and rightfully so, it remains unclear whether the industry also safeguards sensitive information against internal or external computer crime (Kosich, 2016).

1.2 BACKGROUND OF THE STUDY

Information Systems are designed with a specific reference to information that is supported by communication networks, technical hardware, and computer software (Fazlidaa & Saidb, 2015). Moreover, information systems contribute immensely to social and economic improvements, aid enterprises to digitally collect, filter, process, create, distribute, retrieve and store data. Information systems aim to support top-level management with critical information management and strategic executive decision-making processes (Fazlidaa & Saidb, 2015). Thus, information systems can technically be defined as a set of interrelated computer components and systems that support strategic decision-making processes in enterprises.

Moreover, information systems aligns with the Information and Communication Technology (ICT) that an enterprise use in which people interact to support business processes and operations. The interconnectedness of the ICT environment resulted in the formation of the internet over the last 40 years (Maleh, Sahid & Belaissaoui, 2019). Moreover, the growth of the internet gave rise to the continuous evolution and innovation of computer technology and development. Cyberspace became the true highway for the global business environment, however as Maleh *et al*. (2019) points out there is no single governance structure, reporting authority, strategy, or banking credentials.

Moreover, cyberspace is a dynamic global environment, linking industries, and countries irrespective of size and location. The internet as a social experience, enables individuals to interact, exchange ideas, share information, provide social support, conduct business, create artistic media, play games, engage in discussion, etc. The only limitation is the speed by which information is exchanged through information infrastructure, communication bandwidth, and the technology being used. The world and globalisation became popular in the 1990s when the uses of the internet, networking, and digital communication were all growing rapidly, and the term cyberspace was able to represent the many new ideas and phenomena that were emerging (Maleh *et al.*, 2019).

The internet thus enabled fraudsters to commit information technology cyber crimes from anywhere in the world. This resulted in highly sophisticated and organised criminal syndicates establishing themselves all over the world. Recent studies as pointed out by Beck (2020) show that nearly 80% of South African businesses have been victims of some form of cyber fraud. Beck (2020) suggests that the only means to potentially stop these crimes is to proactively detect and prevent them before the information of the enterprise is compromised. Phahlamohlaka, Jansen van Vuuren, Leenen and Zaaiman (2014) state that the responsibility of a government is to provide, regulate, and maintain national security, which includes human security for its citizens.

Recent declarations from the UK and USA governments agree that governments need alignment and agree that the internet is part of the national critical infrastructure that needs to be safeguarded and protected (Scroxton, 2020). Although the South African government approved a draft National Cyber Security Policy Framework, the country still needs a national cybersecurity governance structure in order to effectively control and protect its cyber infrastructure (Phahlamohlaka *et al*., 2014). Whilst various structures have been established to address cybersecurity in South Africa, Phahlamohlaka *et al*. (2014) point out that these structures are inadequate, and the implementation of an information security governance framework is still in the very early stages.

Moreover, structures need to be in place to ensure security policy frameworks are governed and implemented effectively. An information security governance framework is a series of documented, agreed, and well-understood policies, procedures, and processes that define how information is managed in an enterprise (Phahlamohlaka *et al.*, 2014). Moreover, South Africa must define and develop a cyber security framework and implement it to improve national security levels regarding ICT risks and misuses. Based on South Africa’s constitution, the key national security imperatives must be aligned with the governing principle, which is principle 98 of the South African Constitution, which very clearly states that “National Security must reflect the resolve of South Africans as individuals and as a nation, to live as equals, to live in peace and harmony, to be free from fear and want, and to seek a better life" (Phahlamohlaka *et al.*, 2014).

Phahlamohlaka *et al*. (2014) also argue the philosophical position that the fundamental premise on which cybersecurity policies and frameworks are developed is an absolute necessity. Cyberspace is a socially constructed, man-made space with a national cross-cutting social dimension (Scroxton, 2020). Moreover, the realisation must be noted that any cybersecurity awareness or cyberspace framework initiatives cannot be regarded as full proof of technological protection in a socially constructed space. The Chamber of Mines South Africa (2013) state that South Africa is a global leader in mining and account for a substantial amount of world production reserves.

The discovery of high-quality diamonds and large amounts of gold deposits in the 19th century, resulted in South Africa emerging from an agricultural economy to a modern industrial economy (Brand South Africa, 2014). According to the Department of Mineral Resources (DMR) (2014), gold and diamond mining are key commodities that will improve economic growth and benefit the developing economy of South Africa. DMR further states that the mining industry plays a critical role as a foreign exchange earner; with gold accounting for more than one-third of total exports, whilst the South African diamond industry is the fourth-largest producer of diamonds globally.

As part of the Government's growth strategy, the Cabinet of South Africa in 2010 approved the minerals beneficiation strategy as a critical economic area to help stimulate local economic growth whilst creating more job opportunities. The modernisation of the South African mining industry relies on the internet and ICT to operate their businesses and global market interactions (Ula, Ismail & Sidek, 2011). Moreover, insider and outsider information security attacks and data breaches have caused global businesses to lose billions of rands and or dollars. Thus, there is a need according to (Ula *et al.*, 2011) that a proper framework to govern information security is in place to assist the mining industry to better manage their cybersecurity risks.

Given the growing vulnerability of information systems and in particular ICT environments, enterprises need to incorporate cybersecurity as part of an enterprise's corporate governance strategy (Bahl & Wali, 2014). In 2010, the mining sector employed just fewer than half a million people and with the aid of the new beneficiation policy, the sector helped to create 1.3 million job opportunities by 2012. The beneficiation strategy was specifically designed so that the mineral wealth of the country could benefit its citizens (South Africa Yearbook 2012/13). In the 2012 Budget Speech, the then Finance Minister, Mr. Pravin Gordhan announced that the government would be increasing resources by developing port and rail infrastructure as a crucial step to aid the mining industry with transportation (Republic of South Africa, 2012).

It is clear from Government's intervention that the mining industry is constantly looking at innovative ways and adapt to local and international conditions so that the industry remains the flagship of the South African economy.

1.2.1 Impact of cybercrime in South Africa

The King III Report (2010) states that Information Technology (IT) should form a fundamental strategic portfolio as part of the enterprises' risk management portfolio. The report further states that the executive board should be responsible for IT Governance, which in turn becomes the responsibility of management and supported by the risk and audit committees, who will implement, track, and evaluate significant investments in Information Technology and thus ensure that information assets are managed effectively. In 2013, *Ernst & Young Global* conducted a Global Information Security Survey (Ernst & Young, 2013d) and found almost 41% of the respondents from the mining industry experienced an increase in external cyber security threats.

This outcome was in the 12 months leading up to the survey, whilst 28% experienced an increase in internal cyber security threats over the same period. The report stated that it is clear that mining enterprises need to start paying special attention to their data and how it is protected, and also apply the same governance processes in which enterprises manage their massive mining operations and infrastructures. *Security SA* (2011) reported that a new cybercrime study estimated that UK enterprises are losing an estimate of £16.8 billion per annum from the cyber theft of corporate secrets, classified information, and intellectual property.

Eardley (2011) further reported that software and computer services top the list, losing £2.5 billion, which is then followed by financial service enterprises at £2.3 billion, followed by pharmaceuticals and biotech at £1.8 billion, electronics and electrical equipment at £1.7 billion and mining at some £1.6 billion. Symantec Corporation, which is a global information security enterprise, released the Norton report after conducting a cybercrime survey in 24 countries in 2013. As part of their findings (Symantec Corporation, 2013) the report indicated South Africa rated third behind Russia and China in terms of cybercrime victims and stated that cybercrime has become a silent global digital epidemic.

Ernst & Young Global (2013) stated that 53% of Canadian enterprises included in a study, indicated that they had increased their security budget in 2013 after 29% of them reported an increase in cybersecurity incidents in 2012. Mining IQ reported in 2011 (Softpedia News, 2016 – was Mining IQ. Cyber Security, 2011) that Rio Tinto, an Australian mining enterprise, experienced cyber-attacks which resulted in its Singapore offices being unable to operate as it was offline for four days. The report further states that BHP Billiton, also an Australian mining enterprise, was the victim of a hacking attack while preparing a takeover bid of Rio Tinto.

The lack of cybersecurity expertise in South Africa is a national emergency and of huge concern (Von Solms, 2014; Parliament of the Republic of South Africa, 2017). Von Solms (2014) further states that cybersecurity expertise internationally and in South Africa is urgently needed, as the demand for cyber-expertise is twelve times more than that of ICT in general, which in itself is at a premium. South Africa cannot secure its cyberspace, including its critical information infrastructures, without such expertise. Von Solms (2014) cites several cases in South Africa where electronic fund transfer (EFT) fraud was committed as personal credentials were abused, which allowed unauthorised IT access and fraudulent activities.

An example of fraudulent activities committed in South Africa was, the Department of Water Affairs were defrauded in June 2011 of R2.84 million because user passwords were compromised. The Blue IQ's CEO was linked to R450 000 in fraudulent activities and claimed password theft in September 2009; the KwaZulu-Natal Provincial Government reported that R769 million was fraudulently pilfered in April 2010; the South Africa Social Security Agency (SASSA) said internal employees compromised user passwords and diverted an undisclosed amount of funds in March 2010; and the Mpumalanga Education Department were defrauded of R5.5 million in October 2009.

Von Solms (in Rasool, 2012) reports that EFT fraud is on the rise in all sectors of enterprises and highlighted an example when in 2012 cybercriminals accessed and illegally transferred R42 million into mule accounts after hacking into the ICT systems of the South African Postbank. During the delivery of the Government's State Security Agency (SSA) budget vote speech in 2015, Minister David Mahlobo of State Security advised that the South African government has been constantly criticised for the absence of decisive policies and governance processes over the growing problem of cybercrime, which cost the country over R5.8 billion in 2014. (Department of State Security, 2015.)

The Minister reported that cybersecurity has been overlooked by Government but has been prioritised and committed that the SSA would accelerate the enhancement of institutional cybersecurity capacity, finalise the national cybersecurity policy, present the Cybersecurity Bill before Cabinet, and socialise the SSA's cybersecurity awareness campaign.

1.2.2 Definition

This section defines key terms in this study. These key definitions are demonstrated in table 1.1 below.

Table 1.1: Definitions of key terms

Term	Definition
Governance of ICT	Governance of ICT is concerned about two elements, namely the value that IT contribute to the business and align strategically to business objectives, and the mitigation of ICT risks to manage its accountability to the enterprise. (Information Systems Audit and Control Association (ISACA), 2010)
ICT Governance Framework	Is a formal method of bedding down the corporate model to align and deliver business strategy, whereby it measures the performance, manages enterprise risk, and establishes a corporate culture with ethical standards (Dodds, 2012).
Information Security	Information security is a process whereby confidentiality, integrity, and availability of information is protected and persevered (ISO/IEC 27000 standard, 2014; revised 2018).
Cybercrime	A term for any illegal cyber activity that use a computer system as its primary means of committing criminal cyber activities (Rouse, 2012). A crime with which a computer system is the object of the crime or used as a tool to commit a cyber-criminal offense (Janssen, 2015).

	A cyber offence that involves the use of electronic communication equipment or information systems that include any device, or the use of the Internet, or any other technological method to commit this criminal activity. (The Law Society of South Africa, 2019).
	Cybercrime is an increasing area of crime as more cyber criminals are abusing the speed, convenience, and anonymity that the Internet offers to commit a diverse range of criminal activities that know no physical or virtual borders. (International Police Criminal Organisation (INTERPOL), 2015).
IT Governance	IT Governance is about authority – how decisions are made, who gets to make them, and who's accountable for them; management is about responsibility for delivering to meet these expectations. (Gartner Research Group, 2015).
	IT Governance is the responsibility of the board of directors and executive management. Forms an integral part of enterprise governance, the leadership and enterprise structure and processes to ensure that the enterprise's IT department sustains and extends the enterprise's strategies and objectives. (ISACA, 2010).

1.3 RESEARCH PROBLEM

The South African political, socio-economic and cultural factors have been dominated by mining, given that for so many years, this industry has been the flagship of the economy in South Africa (Baxter, 2016). South Africa remains one of the leading global producers of platinum. Baxter (2016) states that the success of the mining industry can be attributed to the high level of the industries' technical and mineral production expertise, including its commitment to an extensive program to research and development of mining activities. Mining enterprises in South Africa are constantly vulnerable to cyber theft as criminals are particularly interested in stealing corporate information as a reference to operational information (Eardley, 2011).

Moreover, according to Eardley (2011) mining enterprises based in the UK lost £1.6 billion because of cyber-criminal activities. A report by Ernst & Young Global Limited (2013) supports the concern of cybercrime by indicating that mining enterprises are facing an alarming rise of cyber-attacks, as they rely more on the Internet when automating equipment to run mines remotely. Mining enterprises need to have firm cybersecurity processes in place to protect the information assets of an enterprise. (Valli, 2012). According to Mazumdar, Barik and Sengupta (2010), because of global connectivity through the Internet, information security threats are no longer just confined to a particular industry or region, they are universal.

Consequently, enterprises must have comprehensive plans to deal with information systems security attacks (Valacich & Schneider, 2013). South African mining enterprises indicated at the mining indaba that modernising of the industry has started which is cautioned by (Chauke, 2019). Moreover, Chauke (2019) points out that the adoption of new leading-edge automation information technology, could result in severe threats to the safety of humans and their operations if they fail to adequately protect their ICT infrastructure against cyber-attacks. Chauke (2019) further states that mining enterprises in South Africa are set to embrace the next generation of technology, being the Fourth Industrial Revolution (4IR) with a view to reduce cost and increase production.

The view of Bergen (2019) corroborates with the findings of (Ernst & Young, 2019) who points out that 54 percent of mining enterprises experienced a significant increase in cybersecurity incidents in 2019. Automation is a double-edged sword, and mining operations need to make cyber security their top priority (Bergen, 2019). Moreover, based on the collective focus of cybersecurity by scholars (Bergen, 2019; Phahlamohlaka *et al*., 2014; Bahl & Wali, 2014), this study aims to identify and highlight cybersecurity benefits, challenges, types, victims of cybercrime and thus propose an information security governance framework which can be referenced in chapter 3.

1.4 PROBLEM STATEMENT

The South African mining industry remains one of the leading producers of most global minerals (Baxter, 2016). Moreover, because mining enterprises enjoy a high level of technical and mineral production expertise, the classified information and intellectual property of a mining enterprise remains under constant cybersecurity threats (Eardley, 2011). Thus, with the introduction of automation and modernisation in mining, enterprises are experiencing an alarming rate of cybercriminal activities and violations. Moreover, mining enterprises constantly face cyber threats from environmental activists as not everyone is pro-mining (Valli, 2012). However, it should be noted that it is not only South African mines who are experiencing cyber-security threats, but global mining enterprises as well (Eardley, 2011). Bergen (2019) corroborates with the findings of (Ernst & Young, 2019) who points out that 54 percent of mining enterprises experienced a significant increase in cybersecurity incidents in 2019.

The ICT environments of mining operations that are built on a foundation of industry-specific cybersecurity governance are also exposed to cyber risk, financial losses, threats to human health and life and even see the complete shutdown of mining operations (Bergen, 2019). This study focussed on the collective views of many scholars, who state that cybersecurity threats in the mining industry and the world at large is of serious concern especially with the evolution of the Fourth Industrial Revolution (4IR) (Bergen, 2019; Phahlamohlaka *et al*., 2014; Bahl & Wali, 2014; Ernst & Young, 2019). Thus, this study aims to propose an information security governance framework for enterprises, that can be used by cyber security administrators in parallel with their current ICT information security governance structures. Moreover, this study will review auditable control measures and policies and align it with the proposed cybersecurity governance framework. The “Research questions” and “Secondary objectives” addresses the Primary Objectives.

1.5 RESEARCH QUESTIONS

This study aimed to answer the following questions:

- What formal IT governance practices do enterprises in the South African mining industry use?
- What type of access control processes are in place?
- Do enterprises have information security policies in place?
- What auditable control measures do enterprises have in place?

1.6 PRIMARY OBJECTIVES

The primary objective of this study was to investigate auditable control measures and policies in order to propose an information security governance framework for the mining industry of South Africa.

1.7 SECONDARY OBJECTIVES

The secondary objectives of this study were:

- To determine if IT governance practices are used by enterprises in the mining industry.
- To identify the types of access control processes put in place by enterprises in the mining industry.
- To establish if information security policies are implemented within South African mining enterprises.
- To analyse auditable control measures used by enterprises in the South African mining industry.

1.8 RESEARCH DESIGN

This study was quantitative and descriptive in nature. This study aimed to quantify data and generalise the results from the from an information security administrator representing each of the sixty-two (62) mining enterprises in the South African mining industry (Van der Stroep & Johnson, 2010). This study used a web-based questionnaire to collect and generate statistical numerical data (Hair, Celsi, Money, Page & Samouel, 2011). Hair *et al*. (2011) state that research design provides the researcher a basic roadmap when undertaking a research study. Moreover, the research design needs to make available the appropriate information based on the research questions and hypotheses as this will guide the researcher to formulate a study design.

1.9 RESEARCH METHODOLOGY

Research methodology is a procedure that allows a researcher to collect, analyse and interpret data in order to achieve the research aims and objectives (Leedy & Ormrod, 2010). According to Hair *et al.* (2011), each study dictates the kind of research methodology the researcher should use to underpin the work and methods that will be available to the researcher to collect data. For the purpose of this study, a self-administered, well-structured questionnaire was used to gather data from information-security administrators in the mining industry of South Africa. Quinlan (2011) states that questionnaires are structured as this will ensure that each of the respondents is presented with the same, simple to understand, clear, concise, and precise questions which ensure that the responses are answered correctly. Close-ended questions were used since the research is quantitative in nature (Myers, 2013).

1.10 APPLICABLE RESEARCH PHILOSOPHY

There are several research philosophies, namely epistemology, ontology, interpretivism and positivism. Whilst the research findings in positivism studies are only descriptive and was subsequently selected to be the preferred philosophical method adopted for this study (Denscombe, 2010). Moreover, positivism is the objective of social research which is to determine the patterns and consistencies of the social world, by using scientific methods to good effect in natural sciences. Positivism relates to the philosophical stance of the natural scientist and is very similar to epistemology (Saunders, Lewis & Thornhill, 2012).

The positivist researcher uses a methodical approach that is independent of the content and context of the inquiry (Remenyi, Williams, Money & Swartz, 1998). This view suggests a structured methodical approach to facilitate the research, and that the researcher will be engaging an observable social reality by which the final outcome might be law-like generalisations (Saunders *et al.,* 2012). Moreover, a positivist paradigm emphasises quantifiable observations with possible statistical analysis, as in the current study. Positivism suggests the use of quantitative research methods, the search for causality and determinism (Collins, 2010), is viewed as a suitable philosophy to guide the research design.

Collins (2010) informs that because the researcher is independent of the research with no human interests within the study, the research findings in positivism philosophy studies are only descriptive and are thus regarded as the preferred philosophical position adopted for this study.

1.11 RESEARCH APPROACH

There are three approaches to research namely: deductive, inductive, and abductive research approaches (Bryman & Bell, 2015). This study adopted a deductive research approach which Myers (2010) defines as “an approach that explores a known theory or phenomenon and then tests if that theory is effective in given circumstances.” According to Saunders *et al*. (2012), research projects will make use of the deductive research approach allowing the researcher to define a theoretical or conceptual framework that will be consequently tested using research data. With deductive research, the research has a well-defined objective with the research question(s), however, the researcher does begin with any predefined theories (Saunders *et al.,* 2012).

This study adopted a deductive research approach which Myers (2010) describes as an approach that explores a known theory or phenomenon, and then tests if that theory is effective in all given circumstances. As the deductive research approach was the prevalent view for this study, other types of research philosophies were less accepted.

1.12 RESEARCH INSTRUMENT

A structured, self-administered web-based questionnaire was used to gather data from information security administrators. Due to the quantitative and descriptive nature of the research, the questionnaire used closed-ended questions. Questionnaires are often used for descriptive or explanatory research. Gill and Johnson (2010) define descriptive research as a “research approach that is undertaken by using attitude and opinion questionnaires that will allow the researcher to classify and describe the variability in different phenomena”.

1.13 POPULATION

Information security administrators in the South African mining information security industry were selected as the population for this study. Saunders *et al.* (2012) define a population “as the complete set of cases or group members upon which a research study will be based”. The market capitalisation of listed mining enterprises and its Information, Communication and Technology (ICT) infrastructure footprint in South Africa were the determining parameter in the research population and census.

The mining enterprises that were included in this study are those enterprises that complied with the following criteria: a) listed mining enterprises on the Johannesburg Stock Exchange (JSE); b) are members of the Chamber of Mines of South Africa (COMSA); and c) have legal mining licences with the Department of Mineral Resources (DMR). The aggregate number of mining enterprises in the South African mining industry consists of 62 listed mining enterprises, with a combined market capitalisation value of approximately R791 billion. The information security administrator representing each of the 62 mining enterprises in the South African mining industry participated in this study.

1.14 CENSUS

A census was used for this study, as it enabled the use of informed decisions to select scenarios that best provided the answer to the research questions (Cohen, Manion & Morrison, 2011; Hair *et al.,* 2011). For the purpose of this study, the emphasis was on the total number of enterprises in the South African mining industry as units of interest. This study required individuals with skills and practical experience in Information Security (IS) in the mining industry of South Africa. For this reason, the information security administrator representing each of the sixty-two (62) mining enterprises participated in this study.

1.15 DATA COLLECTION AND CAPTURING

A web-based, well-defined questionnaire was used to collect primary data from the information security administrators in the mining industry of South Africa. The web-based questionnaire was hosted by SurveyMonkey (www.surveymonkey.com) which is a Web-based survey enterprise that facilitates online surveys. This study used the census method to collect data from the research participants. According to Hair *et al.* (2011), census refers to the quantitative research method, in which all members of the population are enumerated. Census implies complete enumeration of the study participants. Census is a well-organised procedure to gather, record and analyse information about the population (Cohen *et al.,* 2011; Hair *et al.,* 2011).

Thus, based on the census research method, the entire population group to collect research data relates to this study. However, census essentially relate to the statistical collection of data across various areas and sectors relating to a particular subject matter or enquiry. The questionnaire was sent to an information security administrator who represented each of the 62 mining enterprises that have been identified in the census population group. These administrators were identified from listed enterprises on the Johannesburg Stock Exchange (JSE), all members of the Chamber of Mines of South Africa (COMSA) that have legal mining licences with the Department of Mineral Resources (DMR).

In this study, data was analysed as per table 1.2 below.

Research Objectives	Research Questions	Data Analysis Technique
To determine if IT governance practices are used by enterprises in the mining industry	What formal IT governance practices do enterprises in the South African mining industry use?	The data analysis in this study was quantitative and descriptive in nature as it references the basic transformation of research data, which define the essential characteristics such as tendency, distribution, and variability (Zikmund *et al*., 2013). This study used the Cronbach's alpha to measure internal consistency reliability. The validity and reliability of the research instrument was tested by using exploratory factor analysis (EFA). The Kaiser-Meyer-Olkin Measure of Sampling Adequacy (KMO) and Bartlett's Test of Sphericity was used as a statistic in this study to see if the proportion of variance in the variables could be caused by underlying factors. The scree plot was used in multivariate statistics which is a line plot of the eigenvalues of factors or principal components in the analysis to determine the number of factors to retain in the EFA or principal components to keep in the principal component analysis (PCA). (Ledesma, Valero-Mora & Macbeth, 2015). The rotation component matrix assisted the analysis of this study to determine what the components represent in a correlated matrix (Sheth, 2018).
To identify the types of access control processes put in place by enterprises in the mining industry	What type of access control processes is in place?	
To establish if information security policies are implemented within South African mining enterprises	Do enterprises have information security policies in place?	
To analyse auditable control measures used by enterprises in the South African mining industry	What auditable control measures do enterprises have in place?	

Table 1.2: Data analysis techniques (table was defined by the student)

1.16 VALIDITY AND RELIABILITY

The validity of a research instrument refers to the extent to which the tool measures what it should be measuring (Leedy & Ormrod, 2010). This study used Exploratory Factor Analysis (EFA) to validate the research results; as stated by Ruscio and Roche (2012), EFA results are used routinely when developing and validating research assessment instruments. Moreover, EFA evaluates the design validity of a scale or research instrument which was used to test the validity and reliability analysis of this study. Yu and Richardson (2015) state that EFA is a statistical technique that improves the reliability of the scale as it identifies inappropriate items that can then be removed. For this reason, this study used EFA to evaluate the research instrument.

The reliability of a measurement instrument is defined by Quinlan (2011) as “the extent to which a measurement instrument yields consistent results when the characteristic being measured has not changed”. Rubin and Babbie (2011) define reliability as “a matter of whether a specific technique is applied repeatedly to the same object and yield the same result each time”. *Cronbach’s alpha* is regarded as the most common way to assess reliability (Van der Stoep & Johnson, 2009). The coefficient of Cronbach’s alpha varies from 0 to 1, and a value of 0.6 or less normally indicates unsatisfactory internal consistency reliability (Malhotra, 2004). For the purpose of this study, Crobach's alpha was used to measure internal consistency reliability. This is done to assess whether the various items that make up the measure, are internally consistent (Rubin & Babbie, 2011).

1.17 ETHICAL CONSIDERATION

This study aligned to the Policy on Research Ethics of the University of South Africa (UNISA, 2012), which is the “Policy on research ethics contents of September 2016”. Creswell and Plano Clark (2011) support the research policy of UNISA, by stating that the ethical behaviour of research is very likely to be guided and adhered to by the university’s code of ethics policy or ethical guidelines. Respondents were advised that their participation in this study is voluntary, that there were no penalties for refusal to participate and they can decide whether to participate or decline. They were advised of the possible risks as well as the benefits of the research and their participation is free.

The purpose of the study as well as an explanation about the selection process of the participants and the procedures that were followed were shared with participants. Participants in this study were not compensated. There was no foreseeable harm, only minor and reasonably foreseeable discomfort (none of unusual nature), and invasion of privacy to participants of this study (Institutional Review Board [IRB] Guidebook, 2018). The participants were informed about the methods which would be used to protect anonymity and confidentiality. An informed consent form was issued to the participants to gain their consent to participate in the research. Participants were informed about their freedom to withdraw at any given time from being a participant in the research, before submitting the completed questionnaire (Fouka & Mantzorou, 2011).

1.18 DELIMITATIONS, LIMITATIONS AND ASSUMPTIONS

This study was delimited to the following:

- Mining industry of South Africa at a given point in time.
- The study cannot be generalised to other countries or industries.

The following limitations formed part of this study:

- Information security administrators at each of the mining enterprises are very busy professionals, and might not have been available to participate in the survey.
- Time and money were not always readily available since it was consumed by this study. However, it was efficiently spent whilst doing this study.

The following assumptions guided this study:

- Due to rapid change in ICT, it was difficult to cover all aspects of information security and governance in the literature.
- Honesty takes a considerable amount of time and effort to validate the answers given by each participant. Thus, the researcher assumed honest responses were provided by each participant.

1.19 VALUE-ADD BY THIS STUDY

The outcome of this study may assist enterprises within the mining industry of South Africa to kerb and prevent information security breaches. It may help mining enterprises to review their current policies and measure them against the recommendations from this study. Moreover, government and enterprises in other industries may also gain insight into information security breaches and preventive measures.

This study aimed to determine if enterprises in the mining industry of South Africa have a well-defined information systems security governance framework to mitigate any information security risks and vulnerabilities. To achieve this aim, the study established methods that enterprises in the South African mining industry use to protect sensitive and classified information in their ICT environments, which is critical for enterprises to achieve their strategic business objectives and attain growth opportunities.

1.20 CHAPTER LAYOUT

Chapter 1: Introduction and background to the study: This chapter defines the problem statement, research objectives, research design and methodology, research instrument, data collection, analysis, ethical consideration, chapter layout, research budget, and research schedule.

Chapters 2: Cybersecurity and governance: The literature review include an extensive review on how critical information security (IS) is in the South African mining sector, the management of Information Systems, Technology, Security and Compliance, Risk Management of information, Data governance, and a suggested design of a Security Information Framework model, together with the reasons for devising the model and an explanation of its importance.

Chapter 3: The South African Mining Industry and the proposed Information Security Governance Framework: This chapter discusses the mining industry of South Africa. The chapter also covers the characteristics of the proposed information security governance framework.

Chapter 4: Research Methodology: This chapter discusses the methodology used for the purpose of this study.

Chapter 5: Research Results: The chapter covers the analysis and interpretation of the findings in the study and thus produces a clear and comprehensible presentation of the research results.

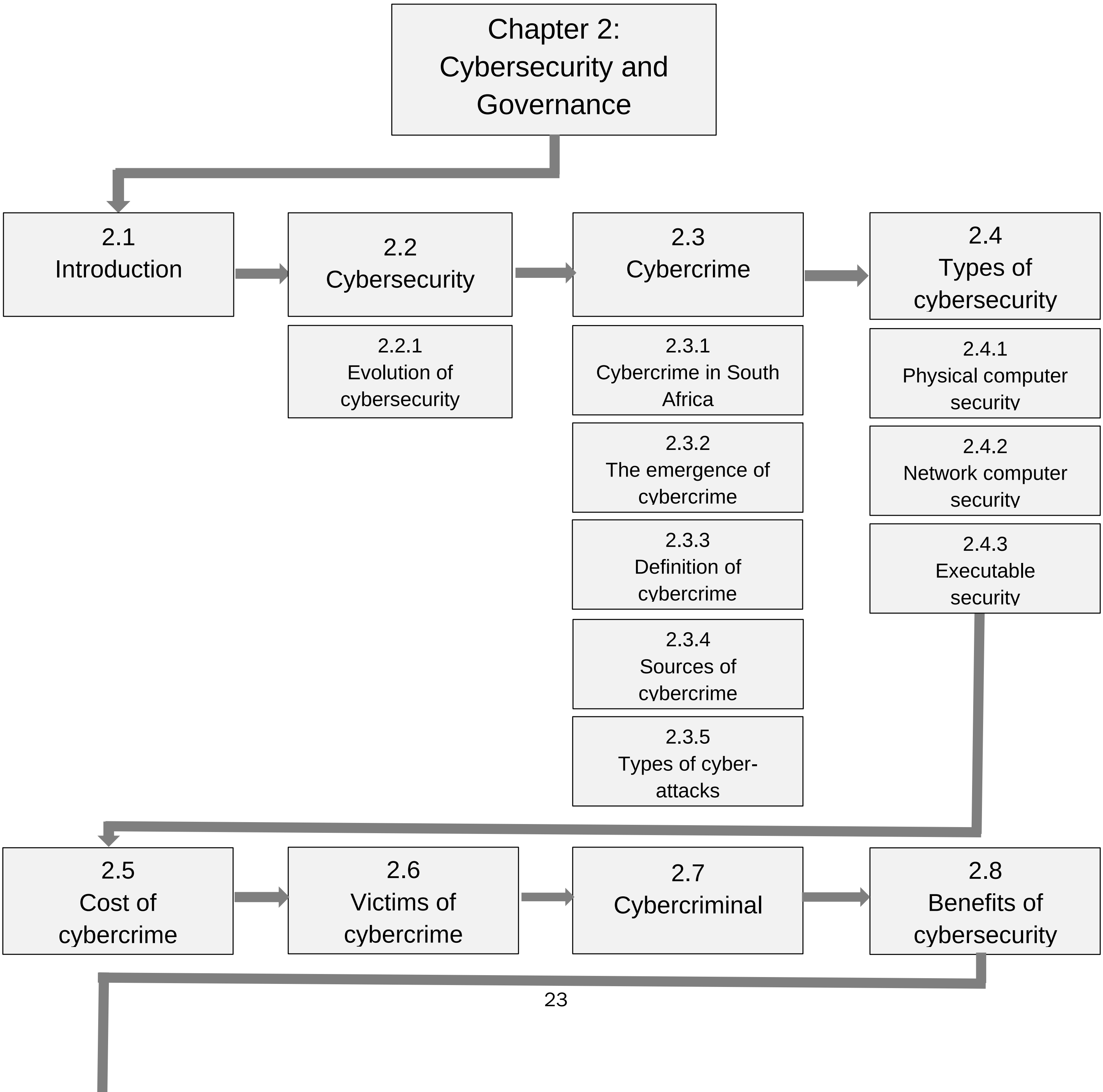
Chapter 6: Conclusions and Recommendations: The chapter draws conclusions based on the research aims, objectives, and findings of the research. Furthermore, research recommendations are offered, and future research is proposed.

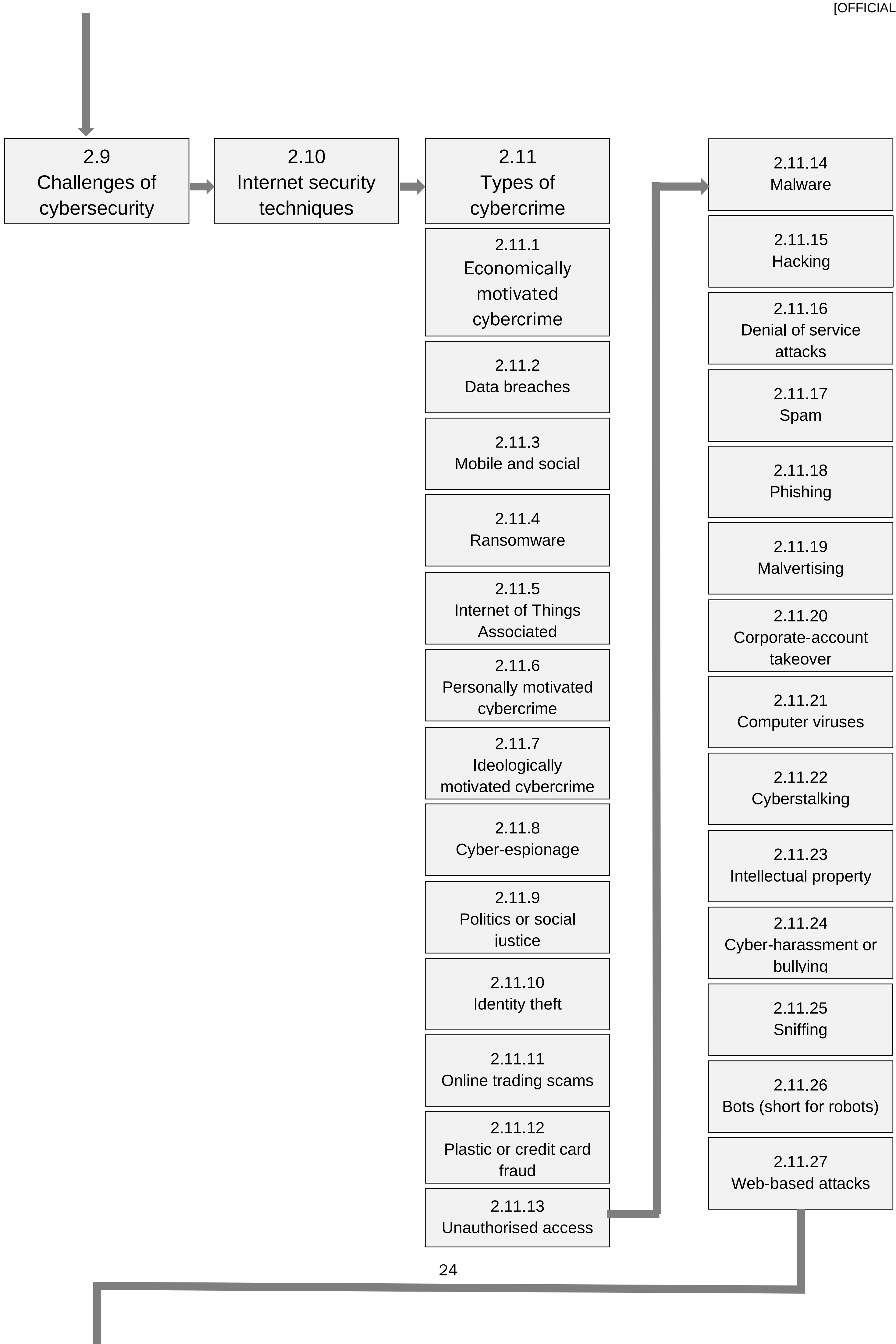
1.21 CHAPTER SUMMARY

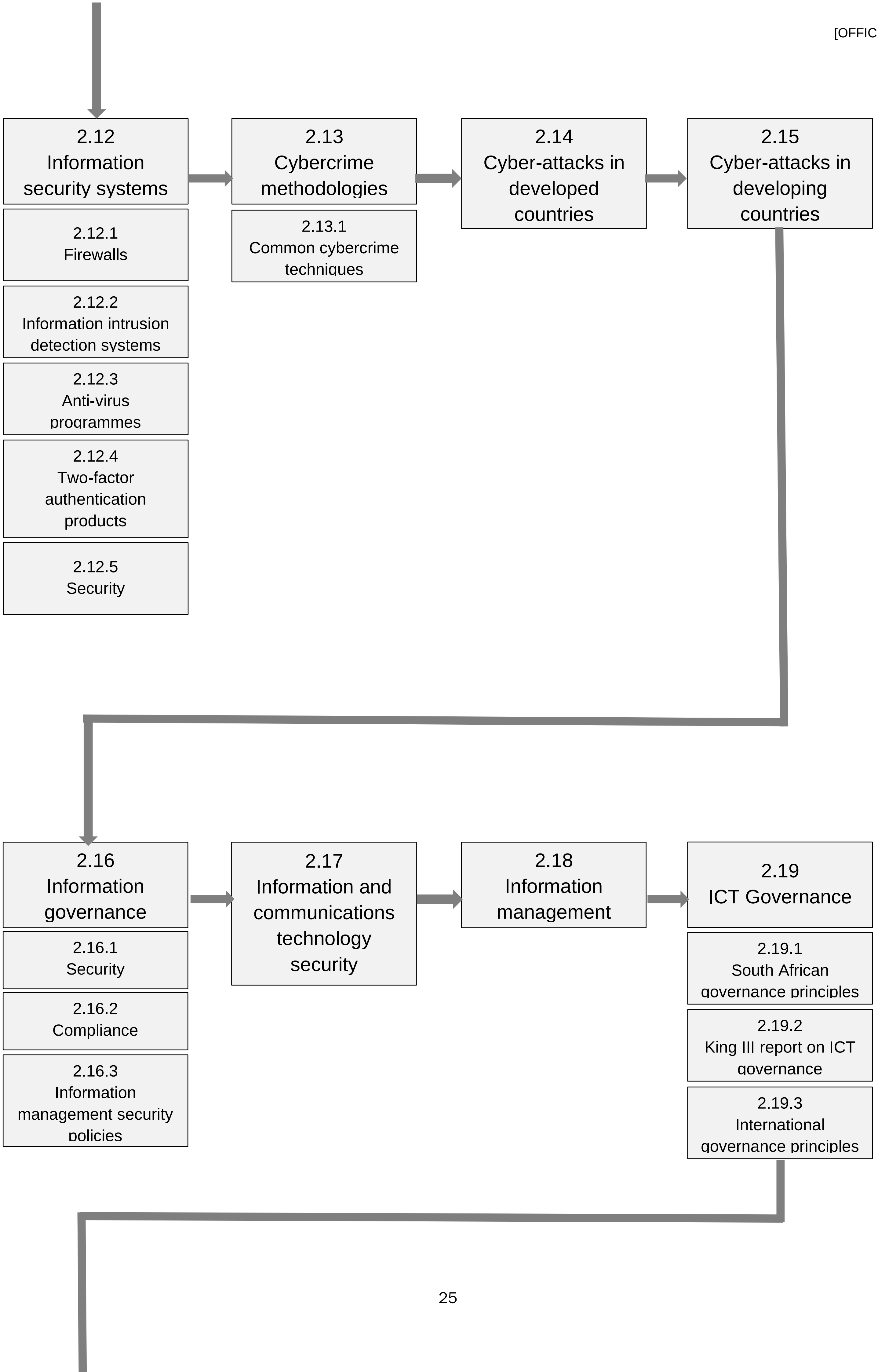
The mining industry of South Africa forms a critical path to the economy of the country. However, each of the mining enterprises contributes meaningfully to ensure the sustainability of the economy. All the enterprises within the mining industry have their ICT environments connected to a larger global network, which exposes them to cybercrime. This study aimed to review information security vulnerabilities that expose these enterprises to cybercriminals. Thus, the study collected data on the governance classified information and propose information security recommendations to these enterprises. Chapter 2 provides a detailed review of cybersecurity and governance.

CHAPTER 2: CYBERSECURITY AND GOVERNANCE

Cybersecurity and governance underpin the success of securing personal and classified information of enterprises. This chapter provides a comprehensive discussion of cybersecurity which includes the benefits, challenges, types, costs, and victims of cybercrime. It reviews the history of the Internet, characteristics of a cybercriminal, methodologies of cybercrime, cyber-attacks on developed and developing countries. It concludes by reviewing the governance of information, communication and telecommunication, information governance and South African and international governance principles, and conclude by reviewing risk management of information.


Chapter 2: Cybersecurity and Governance
2.1 Introduction
2.2 Cybersecurity
2.2.1 Evolution of cybersecurity
2.3 Cybercrime
2.3.1 Cybercrime in South Africa
2.3.2 The emergence of cybercrime
2.3.3 Definition of cybercrime
2.3.4 Sources of cybercrime
2.3.5 Types of cyber-attacks
2.4 Types of cybersecurity
2.4.1 Physical computer security
2.4.2 Network computer security
2.4.3 Executable security
2.5 Cost of cybercrime
2.6 Victims of cybercrime
2.7 Cybercriminal
2.8 Benefits of cybersecurity


2.9
Challenges of cybersecurity
2.10
Internet security techniques
2.11
Types of cybercrime
2.11.1
Economically motivated cybercrime
2.11.2
Data breaches
2.11.3
Mobile and social
2.11.4
Ransomware
2.11.5
Internet of Things Associated
2.11.6
Personally motivated cybercrime
2.11.7
Ideologically motivated cybercrime
2.11.8
Cyber-espionage
2.11.9
Politics or social justice
2.11.10
Identity theft
2.11.11
Online trading scams
2.11.12
Plastic or credit card fraud
2.11.13
Unauthorised access
2.11.14
Malware
2.11.15
Hacking
2.11.16
Denial of service attacks
2.11.17
Spam
2.11.18
Phishing
2.11.19
Malvertising
2.11.20
Corporate-account takeover
2.11.21
Computer viruses
2.11.22
Cyberstalking
2.11.23
Intellectual property
2.11.24
Cyber-harassment or bullying
2.11.25
Sniffing
2.11.26
Bots (short for robots)
2.11.27
Web-based attacks



2.12
Information security systems

2.12.1
Firewalls

2.12.2
Information intrusion detection systems

2.12.3
Anti-virus programmes

2.12.4
Two-factor authentication products

2.12.5
Security

2.13
Cybercrime methodologies

2.13.1
Common cybercrime techniques

2.14
Cyber-attacks in developed countries

2.15
Cyber-attacks in developing countries

2.16
Information governance

2.16.1
Security

2.16.2
Compliance

2.16.3
Information management security policies

2.17
Information and communications technology security

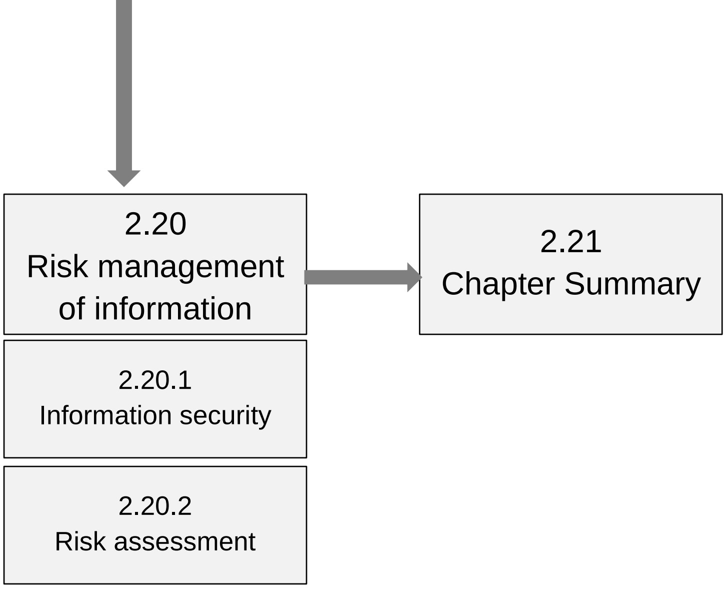
2.18
Information management

2.19
ICT Governance

2.19.1
South African governance principles

2.19.2
King III report on ICT governance

2.19.3
International governance principles



2.1 INTRODUCTION

Information and communications technologies (ICT) have become essential to the modern lifestyle. ICTs represent in today’s global economy what industrial machinery represented as supporting infrastructure during the Industrial Revolution (Moore, 2011). Moreover, ICT has revolutionised working behaviour, transformed the global economy and irreversibly changed and shaped modern society. The information security of a nation’s online activities depends on various stakeholders who provides ICT support services (Klimburg, 2012). The stakeholders include daily and business users of public and private communication services from Internet Service Provider (ISP) who provide and support the ICT infrastructure.

Furthermore, the ISPs manage the daily communication support services, by ensuring the security of a nation’s information and data assets. Klimburg (2012) further states that successful national cybersecurity strategies must consider all relevant stakeholders, their areas of responsibilities and the support that they require to provide them with the necessary support and expertise that they need to successfully perform their duties. This view is supported by the South African authorities when it tabled the Cybercrime and Cybersecurity Bill in the National Assembly of South Africa (Michalson, 2015).

Von Solms (2014) states, the *South African Cybercrimes and Cybersecurity Bill* defines a vast number of cybercrimes and suggests a wide range of penalties for infractions of these criminal activities. In theory, according to Von Solms (2014), the bill is a step in the right direction for South Africa, which makes the country more cyber-secure. Von Solms (2014) further states that more enterprises in South Africa have been victims of cybercrime and have spent large amounts of money on cybersecurity. Moreover, in 2014, South Africa experienced more cyber-attacks than any other country on the African continent, and financial losses through cybercrime amounted to about R5 billion.

Fryer (2015), in IT News Africa (2015), supports this view by stating that South Africa experience the most cyber-attacks on the African continent. Moreover, cybercrime has become a serious concern in South Africa, which is ranked third on a global list of cyber-victims, with Russia ranked first and China second. The Protection of Personal Information Act, No. 4 of 2013 (POPI) was promulgated and signed into law in November 2013, which seeks to regulate the processing of personal information (Government Gazette Number 37067, 2013). The POPI Act defines processing as anything to do with personal information, which includes the collection, unlawful usage, storage, dissemination without consent, modification or destruction of information; whether such information is managed automatically, electronically or manually processed.

The revised Protection of Personal Information Act (often called the POPI Act or POPIA) was presented to parliament on 19 November 2013. The commencement date of the act was proclaimed by the President of South Africa on 1 July 2020 (POPIA, 2020). The Act applies to promote the protection of personal information processed by public and private bodies.

The POPIA Act recognises that:

- Section 14 of the Constitution of the Republic of South Africa, 1996, provides that everyone has the right to privacy.
- The right to privacy includes a right to protection against the unlawful collection, retention, dissemination, and use of personal information.
- The State must respect, protect, promote, and fulfil the rights in the Bill of Rights.

The Act bear in mind consonant with the constitutional values of democracy and openness, the need for economic and social progress, within the framework of the information society, requires the removal of unnecessary impediments to the free flow of information, including personal information. The Act regulates, in harmony with international standards, the processing of personal information by public and private bodies in a manner that gives effect to the right to privacy subject to justifiable limitations that are aimed at protecting other rights and important interests. The South African cyber-laws have been improved in dealing with threats in cyberspace as there is a notion that the country faces a major cyber-threat challenge (Alfreds, 2015).

Klimburg (2012) states that national cybersecurity cannot be regarded as merely a sectoral responsibility; it involves a coordinated and collaborative effort from all concerned stakeholders to help guard against cybercrime. Moreover, the national cybersecurity policies are limited to within the borders of national sovereignty. Klimburg (2012) further states that these cybersecurity policies address an environment of cybercriminals that has a total disregard for national boundaries. Cybersecurity is an international problem and concern, that requires international cooperation to successfully maintain and secure critical information globally (Choucri, 2012). Richet (2015) states that the procedures to address cyber-threats is proposed by several stakeholders which include political, technological, legal, private sector or the military.

2.2 CYBERSECURITY

The term cyberspace is used to describe computer systems and services that are interconnected to the Internet through telecommunications and computer network infrastructures (Moore, 2011). Moreover, modern society depends on the timely service, adequate and confidential performance of cyberspace. Cybersecurity is critical to society, businesses, and governments because it aspires to ensure that cyberspace is always available as expected, even if there is a cyber-attack (Bayuk, Healey, Rohmeyer, Sachs, Schmidt & Weiss, 2012). Cybersecurity cannot be seen as just a pure computer system security issue, according to Bayuk *et al.* (2012), instead, cybersecurity has become a national security policy matter.

Moreover, the unlawful use of cyberspace could hamper an economy, the health of society, safety, and a country’s national security activities. Hathaway and Klimburg

(2012) emphasis ICT infrastructure and state global society have become dependent on ICT infrastructure; and cyber threats against the availability of the very same ICT infrastructure, the integrity and confidentiality of classified information have serious implications for the functioning of societies, businesses, and governments. Brenner (2012) states that ICT systems have managed to change the way enterprises provide services, how society communicate with one another, how enterprises make strategic decisions and especially the way people understand each other and interact globally.

Furthermore, many of the changes we witness today is a result of the convergence of significant, interrelated computer networks, mobile communication, large data transmissions and ever-evolving social networks. While each of these changes is independently significant, Brenner (2012) states that when taken in combination, these shifts have a pervasive impact on the enterprise in the digital world in which cybersecurity risks cannot be ignored. Cybersecurity, if ignored according to Yar (2013), has the potential to cause reputational damage to an enterprise’s brand, intellectual property, classified business data and financial information.

The ever-presence of cyber security risks is changing how many enterprises approach cybersecurity, which makes it more important for security experts and business leaders to form a closer partnership to formulate a strategy to mitigate cybersecurity risks (Yar, 2013). Cybersecurity is critical to the success of a business and encompasses the protection of critical ICT systems and enterprise information from malicious cyber-threats (Vacca, 2013).

2.2.1 Evolution of cybersecurity

Cybersecurity has evolved as an established information security discipline to protect interconnected computer systems and ICT infrastructures, with a focus to safeguard valuable classified business information stored on those systems from cyber-criminals who want to obtain, corrupt, destroy or commit fraud (Brodie, 2014). Moreover, cybersecurity has quickly evolved from a technological discipline to a strategic imperative for businesses and governments (Geers, 2011). It can also be said, according to Geers (2011), that globalisation and the birth of the internet have given society, enterprises and nations across the world, incredible new technical power, based on the constant development and usage of ICT technology.

Carter and Zheng (2015) state that cybercrime is an evolving industry globally and imposes significant costs on enterprises that fail to implement adequate ICT security safeguards. However, according to Carter and Zheng (2015), regulators are taking notice of the increased and emerging risks of cyber-threats and are constantly looking at imposing implicit requirements on enterprises and governments to secure their ICT environments in the name of operational assurance, data protection, and accurate reporting. It is within the backdrop of cybersecurity that the technological revolution concept of cybersecurity came into existence (Devi & Rather 2016).

Furthermore, the term "cybersecurity" refers to the securing of information, communication and technology and focuses on protecting interconnected computers, devices, programmes, data networks and data from unauthorised or unintended access and destruction of business information. Clarke and Knake (2012) state that cybersecurity is critical in the design of information and communications technology and Internet services. Therefore, it becomes essential for each country's information security and economic well-being to enhance cybersecurity in protecting critical information technology infrastructures. Clarke and Knake (2012) state that cybersecurity is as old as cyberspace, which makes it as old as computers. However, the actual importance of cybersecurity had not been realised until the Internet was made available to the public.

2.3 CYBERCRIME

Cybercrime is committed by cybercriminals or hackers in cyberspace. The word or term cyberspace can be defined in several ways, especially by IT professionals and lexicographers who tried to give meaning to the term (Oluga, Ahmad, Alnagrat, Oluwatosin, Sawad & Mukta, 2014). Cyberspace, according to Oluga *et al.* (2014) can be an imaginary world, where information is shared between computers. Cyberspace is sometimes referred to as a web of private *cum* public interconnected computers (Oluga *et al.,* 2014). Cyberspace according to Trim and Upton (2013) essentially refers to the virtual space of interconnected computer systems. According to Oluga *et al.* (2014), cyberspace is a computer-technology invented world.

Cyberspace comprises many real-world activities which are similar to the physical world, which explains why the two are closely related (Langer, 2011). Based on this background, Langer (2011) states that the world of cyberspace is viewed as a virtual world. The numerical number of cyberspace users has seen continual growth across the world (Shakarian, Shakarian & Ruef, 2013). The growth of cyberspace provided a multitude of benefits; however, these benefits are now faced with cybercrime (Shakarian *et al.*, 2013). Moreover, this unfortunate criminal activity in cyberspace has the potential for societies, nations, and businesses to lose confidence in using the benefits that cyberspace has to offer.

Kshetri (2010) states that the permeation of various cyber-criminal acts as in human society is equally happening in the digital or internet world of cyberspace. The term *cybercrime* is otherwise regarded as computer-crime, internet-crime or web-crime and has attracted various definitions or interpretations by those who have shown an interest in this area of study (Kshetri, 2010). There are nearly as many terms to describe cybercrime as there are actual cybercrimes. It can further be stated that initial descriptions of the term included “computer crime”, “computer-related crime” or “crime by computer” (Bernik, 2014). Furthermore, new terms, “high-technology” or “information-age” crime was added to the lexicon as digital technology matured.

Then, according to Nemati (2014), the advent of the Internet gave rise to terms such as “cybercrime” and “Internet” or “Net” crime. Nemati (2014) further state that because technology is used in committing these crimes. Grigsby (2014) states that this regulatory body was established to enforce cybercrime laws thus ensuring the successful prosecution of cybercriminals. This body successfully established a broad consensus as to what the terms of cybercrime encompass (Cevidalli & Austen, 2010). Kshetri (2010), defines cybercrime and states that “cybercrime is defined as a criminal activity in which computers are the primary tools of committing an offence or violating laws, rules or regulations”.

This definition of cybercrime is very similar to that of Holt and Bossler (2016), and Gad (2014), who state that “cybercrime refers to a criminal offence that involves a computer as the object to commit a crime”.

2.3.1 Cybercrime in South Africa

A research report by Accenture (2019) states that as the use of technology, the Internet and smartphones grows in South Africa, so does the cyber-attack surface. The report further states that in 2019, South Africa saw a cross-industry spike of cyberattacks. A South African security intelligence company, iDefense indicates that South Africa has the third most cybercrime victims worldwide, losing about R2,2 billion a year. Accenture (2019) state that one of the reasons identified indicate that there is low investment in cybersecurity and immature cybercrime legislation which makes South Africa a target.

Moreover, according to the Accenture report (2019), as an increasing proportion of the South African population begins connecting to the Internet for the first time, their inexperience paired with increased exposure to the Internet, is a combination that cybercriminals try to exploit. Yamout (2020) states that South Africa is starting to experience network attacks which are used through methods like “phishing” emails. Cybercriminals scan the South African internet looking for vulnerable computer servers that are exposed (Yamout, 2020). Moreover, email threats in South Africa increased by 56% between April and May 2020. Mpuru and Kgoale (2019) identify emerging trends and insights of cybercrime in South Africa:

February 2019: A South African energy supplier suffers two security breaches in quick succession.

July 2019: Ransomware infects a service provider of pre-paid electric power, leaving customers without access to power.

September 2019: One of South Africa’s largest Internet Service Providers (ISP) suffers a Distributed Denial of Service (DDoS) attack lasting two days.

October 2019: Several South African Banks, as well as financial institutions in Singapore and Scandinavia, suffer DDoS attacks resulting in a loss of service.

The following facts and figures taken over 12 months in South Africa in 2019 indicate the scale of the problem, (Accenture, 2020).

- 22% in malware (malicious software) attacks in South Africa in the first quarter of 2019 compared to the first quarter of 2018, which translates to just under 577 attempted attacks per hour.

- 79% Card-not-present (CNP) fraud on South African-issued credit cards, making it the leading contributor to gross fraud losses in the country.

- 100% Increase in mobile banking application fraud.

Cybercriminals may perceive South African enterprises as potentially having lower cybersecurity defensive barriers than those found in developed economies (Mpuru & Kgoale, 2019). Moreover, these cybercriminals may also think they face a lower chance of incurring consequences for their malicious activity. That's because as pointed out by Mpuru and Kgoale (2019), there is low investment in cyber security and the development of cybercrime legislation in South Africa.

Mohapeloa (2019) state that cyber-attacks are after all just another form of theft, but more importantly as pointed out by Mohapeloa (2019) is that South Africa has a Cybersecurity hub that can be accessed on https://www.cybersecurityhub.gov.za. . Moreover, the hub provides information that creates awareness on cybersecurity as well as information that encourages South African citizens and enterprises to interact securely on the internet. Cybercrime incidents can also be reported through the cybersecurity hub Mohapeloa (2019).

2.3.2 The emergence of cybercrime

More and more businesses are trading online, whilst personal information is rapidly being migrated and shared in digital format on globally interconnected computer technology platforms. As a result of the data migration, the risks from cyber-attacks has increasingly become a reality. Cyber-hackers pursue financial gain by committing cyber-criminal activities to defraud unsuspecting members of the public and enterprises, whilst competitors also steal intellectual property or disrupt businesses to gain a competitive advantage (Bailey, Del Miglio & Richter, 2014). White (2014) states that it should be no surprise that there is an increase in cybersecurity occurrences as data breached progressively increased.

This view is supported by Kelly (2015) who states that there is a surge in the typical indicators of targeted attacks in today's information and communication technology environment. PricewaterhouseCoopers (PwC) researched the global state of information security, 2018 (Chesley, 2016), and responses were gathered from about 9 700 Information Technology experts and Business professionals. The research was undertaken in 154 countries on information security incidents, which occurred between 2014 and 2015. Furthermore, the researchers concluded that undetected information security occurrences increased to 66% year-on-year since 2009, and in 2014 the number of cyber security occurrences increased to 42.8 million globally, which is 48% higher than 2013 at an average amount of 117 338 security occurrences daily.

Furthermore, according to Chesley (2016), the financial impact also increased and was up 34% from the previous year, which was 2014, and the total amount of enterprises that reported losses greater than $20 million annually, almost doubled.

2.3.3 Definition of cybercrime

Williams (2014) defines cybercrime as "any crime that involves a computer and a network". In some instances, the computer may have been used to commit the crime, whilst it could also have been the target of the crime. Cybercrime is not a legal term and as such, lends itself to a certain degree of contextual variability (Broadhurst, Grabosky, Alazab & Chon, 2014) Moreover, cybercrime can also include technical crimes that are exclusively facilitated by technology. Any criminal activity that is committed via the Internet is regarded as cybercrime (Snow, 2012). Akhgar, Staniforth and Bosco (2012), simply define cybercrime as "any criminal activity that involves a computer and a network" and net crime as "the criminal exploitation of computer and network infrastructure on the Internet".

However, Mercer (2016) states that cybercrime is the term that was adopted at the Convention on Cybercrime of the Council of Europe, ETS No. 185 (also known as the Budapest Convention on Cybercrime). Moreover, according to Mercer (2016) "The Council of Europe's Convention on Cybercrime" was designed to address the jurisdictional issues posed by the evolution of the Internet. However, understanding cybercrime add value as it raises awareness and the impact it has on society, governments, and businesses. Moreover, the awareness results in prevention initiatives being formalised to limit and prevent cybercrime attacks.

2.3.4 Sources of cybercrime

Vacca and Rudolf (2011) state that humans tend to participate in criminal activities when the activity provides a high return, and the risk is low. Cybercriminals calculate the risk versus the benefit and once they have calculated that the criminal activity is profitable, they continue to commit fraudulent activities by hacking into computer systems for financial gain. Ellis (2014) states that the principal sources of cybercrime are either internal or external cyber-threats, of which examples of external threats include, but is not limited to, financially motivated hacker groups, economic espionage or cyberwarfare, whilst internal threats could include disgruntled or corrupt employees, departing employees or negligence.

Schneier (2014) cautions businesses against seeing hackers as the biggest concern, whilst underestimating the risk from organised crime syndicates as serious threats. It is therefore important and could be difficult to develop an effective mitigating plan against cybercrime without a proper understanding of the potential sources of cyber-attacks (Schneier, 2014). Finklea and Theohary (2015) state that computer crime can be classified by the extent of the damage or type of harm it caused, the geographic location where cybercrime was committed, the target, and the perpetrator. Moskowitz (2014) states that computer intrusions originate from anywhere globally and target both private and public institutions.

Private cyber-attacks are directed towards corporate ICT infrastructures, whilst public cyber-attacks include government computer services. Brewster, Kemp, Galehbakhtiari and Akhgar (2015) state that the Internet is seen as a platform for criminal activities such as cybercrime, cyberterrorism, and cyberwarfare to be performed by cybercriminals. Ellis (2014) states that the Internet is a vital source of information as it contains vast quantities of data such as personal, business, and personal financial data, sensitive or classified information and research data, etc. However, despite the range of opportunities and the potential it offers, the Internet has a dark underbelly that criminal groups see as a new avenue to exploit and perform criminal activities.

A major and increasing concern of this “dark side” of the Internet, is the growing amount of cybercrime and cyberterrorism, which are criminal activities that we hear about more often, especially since these attacks have catastrophic implications. Ellis (2014) further states that an added dimension of cyber-related criminal activities must be viewed as cyberwarfare and described by Manoske (2013) as the activity to conduct cyber-attacks to commit espionage, sabotage or to conduct cyber-attacks on a target’s strategic and tactical resources. There are popular images that society have of a cybercriminal, being the intimidating Russian cyber hacker in a quest for financial gain, or more recently the Chinese cyber hacker.

Wall (2012) regards these assumptions of cybercriminals as misleading, and state that offenders arise from many different nations and countries, whilst their motivation to commit cybercrime is diverse, although their quest for financial gain appears dominate this criminal activity (Wall, 2012).

2.3.5 Types of cyber-attacks

Senior corporate executives, senior government officials, scholars and academics have become aware that cybercrime present concerns regarding the financial and regulatory losses that arise from cyber-attacks (Sugarman, 2014). For this study, the following definitions were identified to understand cyber-attacks better:

- Any unlawful criminal activity that undermines the functionality of an interconnected network environment that compromises the political or national security stability of a country (Hathaway, Crootof, Levitz, Nix, Nowlan, Perdue & Spiegel, 2012).

- The deliberate cyber-criminal activity or activities to deface, degrade or destroy computer programmes, sensitive or classified information on interconnected computer systems (Hathaway et al., 2012)

- Cyber-criminal activities that affect the operations of an ICT environment, either offensively or defensively, with the intention to modify, delete, destroy, corrupt, or revoke access to computer data, software or information for: (a) propaganda and/or (b) partially or totally disrupting the operational activities of the targeted computer system or data network, and related ICT infrastructure; and/or (c) causing physical damage to an ICT environment, computer data center or physical network infrastructure (Roscini, 2014).

- The exploitation and unauthorised access of cyberspace to access and manipulate classified information, disrupting computer networks, and stealing both data and money electronically (Uma & Padmavathi, 2013).

According to Kapur, Dhupia and Gupta (2014), cyber-attacks consist of a range of illegal digital activities that is targeted at enterprises with the intention of causing harm and instability to their ICT environment. Cyber-attacks by their very nature are multi-dimensional and complex (Kapur *et al.,* 2014). Although enterprises understand the need to safeguard and secure their ICT infrastructures, intruders have often found innovative ways to exploit new loopholes in ICT systems and the governance processes of their targets (Charney, 2016).

2.4 TYPES OF CYBERSECURITY

Computer information security experts recognise three different types of ICT security, mainly, *physical security, network security,* and *executable security* (Akhgar & Brewster, 2016). However, according to Akhgar and Brewster (2016), each type has different risk and implementation profile which is discussed below.

2.4.1 Physical computer security

Kumar (2011) states that physical computer security is the most rudimentary type of computer security and the simplest to understand. In short, Akhgar and Brewster (2016) state that if you have physical access to the computer, you control it. Moreover, user passwords, and other computer protection software can't stop an attacker if he/she can access the computer device. According to Andreasson (2012), computer-hosting enterprises started prioritising physical security at their data centres and employ guards, using sophisticated access control measures and surveillance cameras to monitor their ICT environments. However, Andreasson (2012) cautions that most computer users disregard physical security completely.

Furthermore, these devices are handed to repair technicians who have full access to their private and sensitive information. Andreasson (2012) also raises concern and states that the same negligence applies to physical external hard drives. Moreover, users store private and sensitive information on their computers and then leave them unattended without any computer protection software installed on them to protect their information. Kumar (2011) states that it is recommended to configure the computer to lock by itself after a few minutes of inactivity. It can also be stated according to Kumar (2011) that computer security software protects computers, whilst network security is the security control measure that is implemented that enable the protection of interconnected computers.

2.4.2 Network computer security

Beal (2016) defines “a computer network as simply an infrastructure of interconnected computers”. A network security system essentially consists of secure protection layers which host multiple components, including system monitoring and security software (Beal, 2016). Components according to Beal (2016) is often configured with network security, anti-virus and anti-spyware protection software, firewalls, intrusion prevention and protection hardware systems and virtual private networks to provide secure access to an ICT environment.

Moreover, all the security components interact collaboratively to increase and improve the overall information security of an ICT network. It is known that a computer firewall is an essential piece of ICT security, which is essentially a device that enables network security by filtering and blocking unauthorised network access to an ICT environment (Felix, Joseph & Ghorbhani, 2012). Many enterprises incorporate both computer systems and network security to ensure the highest level of information protection (Johnson, 2015).

2.4.3 Executable security

Executable security is also known as anti-virus security (Ablon, Libicki & Golay, 2014). A system user who is requested to set up a computer system to run a program or set it up so that it executes automatically at a certain time should be prevented to do this, as this action could result in the computer system executing a malicious virus program (Ablon *et al.,* 2014). All names of executable files ending in ".exe" is a programme when that executes when opened. Ablon *et al.* (2014) state that when a user receives an email with a .exe file extension as an attachment, the user should always ensure that the files come from a trusted source, as it could contain a malicious virus code.

2.5 COSTS OF CYBERCRIME

Cybercrime may become one of the greatest threats to every enterprise in the world, are the words of Ginni Rometty, Chairman and CEO of IBM, Beale (2016). British insurance enterprise, Lloyd's, estimated that cyber-attacks financially cost businesses an estimated $400 billion a year, inclusive of direct damage to the business and post-attack disruption to the operations of the business (Morgan, 2016). These cyber-attacks have seen the growth for cyber insurance from enterprises over the last few years. This is evident as is the case in 2015 when the insurance industry underwrote cyber-attack insurance premiums to the value of $2.5 billion (Beale, 2016). The views of O'Callaghan (2015) and Antonopoulos (2016) is that many cyber-attacks go unreported, resulting in the impact of cybercrime being underestimated.

Antonopoulos (2016) states that cybercrimes have a bigger impact on the economy than most conventional crimes globally. According to the 2018 Pricewaterhouse Coopers' (PwC) biennial Global Economic Crime Survey, over 36% of the enterprises that were interviewed reported that they experienced one or more massive economic crimes. However, more than 30% of global enterprises have been victims of economic cybercrime, as reported during a survey of more than 6 000 respondents to PwC's Global Economic Crime Survey in 2016. Furthermore, the PwC survey (2016) reported that nearly 22% of the 6 000 respondents were subjected to losses of between $100 000 and $1 million; 14% of respondents were subjected to losses of more than $1 million, and 1% of respondents (primarily from North America and Asia-Pacific) reported losses in excess of $100 million.

These are substantial sums of money and are representative of a trend of rising costs of individual fraud as stated by the report. A report from security-software enterprise

McAfee (2014; Net Losses: Estimating the Global Cost of Cybercrime. Economic Impact of Cybercrime II), indicates that financial cybercrime has annually cost the global economic and financial markets about $445 billion. The financial losses of cybercrime has resulted in unplanned outages and disruptions to businesses from theft of intellectual property and financial data exceeding $160 billion. Furthermore, losses linked to personal information, such as stolen personal banking data, reached $150 billion in the same year.

The Ponemon Institute (2015) surveyed 252 enterprises in seven countries and reported on the global cost of cybercrime, which was the aim of their study. The study demonstrated a shift in focus as enterprises are committing additional funds to information and cybersecurity security to protect their ICT environments. The study further states that enterprises must understand and acknowledge that cybersecurity poses one of the biggest risk to their business and must have the economic and financial resilience to help them plan their security approach and investments.

The findings of the study are endorsed by Ponemon (2015) who states that cyber-attacks are constantly on the increase, both in frequency and severity, and enterprises needs to plan their financial and resource cover appropriately to mitigate against the consequences and disruptions of a cyber-attack.

Gandel (2015) reports that the threat of cybersecurity was a much-debated topic at the World Economic Forum, at the global gathering of CEOs, world leaders and other powerful nations in Davos, Switzerland. Morgan (2016) states that between 2013 to 2015 the cybercrime financial implications quadrupled, and the assumption is that there will be another quadrupling of cost from 2015 to 2019. As with any underground economy as pointed out by (Antonopoulos, 2016), it is difficult to estimate the financial cost of cybercrime as a global problem that has been challenging, as no accurate statistics and costs exist, as many of these crimes are never reported.

2.6 VICTIMS OF CYBERCRIME

Cybercrime has a direct effect on more than 431 million adult victims globally (Zapo, 2015). Moreover, Zapo (2015) states that since the Internet has become such an essential part of governments, businesses, and in the lives of millions of people globally, cyberspace has become an ideal place for criminals to remain anonymous while they prey on their victims. Maiuro (2015) states that the Internet has become a great haven for cyber scammers and wrongdoers since it allows them to perform criminal activities while hiding behind a shield of digital anonymity. Furthermore, cybercrime affects society in several different ways, both online and in the offline world.

Bernik (2014) state that being a victim of cybercrime can have lengthy effects on private enterprises, countries, and the life of even individuals. The disruptive effects of successful a cyber-attack on an individual or an enterprise can have extensive implications, such as financial and intellectual property losses and can cause reputational damage, resulting in the loss of consumer confidence in enterprises and governments (Bernik, 2014). The damage caused by cybercrime can take years to resolve, so it is important that anyone who is connected to the Internet, protect himself or herself adequately to avoid becoming a victim of cybercrime.

The African continent is regarded as having one of the highest personal cybercrime victims in the world (Von Solms, 2014). Furthermore, from a cybercrime perspective, South Africa rates third after China and Russia. According to a report by the Federal Bureau of Investigation (FBI) in 2014, it states that in terms of impact to victims who suffered financial loss due to cybercrime, South Africa rates seventh (7th) by comparison of the top 50 complainant’s countries globally. Von Solms (2014) states that one of the reasons South Africa in particular, and African countries in general have been targeted, is because of the high transmission broadband Internet cables that have been placed on the east and west coasts of Africa.

According to a report by Symantec on security threats in 2016, it indicated that smartphones have become an increasingly attractive target for cybercriminals. Furthermore, these cybercriminals are targeting users’ cellular phones by downloading valuable data from their victims. Moreover, Android handsets are seen as the number one target, whilst in 2015 there was a suggestion of effective cyber-attacks on Apple handsets as well. Von Solms (2014) states that many South Africans, and to a larger extent people in Africa, are people exploring cyberspace for the first time via their mobile phones. It is further reported by a report of Symantec on security threats in 2016 that about 47% of South African smartphone users had experienced mobile cybercrime in 2015, compared to 38% globally in the same year.

These users, according to Von Solms (2014), never went through the personal computer generation and have no understanding of the risks when using their devices in cyberspace. Von Solms (2014) further warns that cybercrime victims will increase because of the aggressive marketing strategies of service providers of mobile handsets that are used by society as a means of transacting (Von Solms, 2014). Bernik (2014), states that all citizens, consumers of cyberspace, and employees should be cognisant of cyber threats and the remedial action that they can perform in the event of a cyber-attack as this will enable them to protect their own and the information of an enterprise and thus prevent them from becoming victims of cybercrime.

2.7 CYBERCRIMINAL

Identifying the type of cyber attacker is essential, as this will provide accurate details when the profile of a cybercriminal is created, which will then help to reduce cybercriminal activities when solutions are designed and implemented (Rogers, 2010). According to Rogers (2010), the listed six types of cybercriminals below, are generally identified as cybercriminals:

- Script kiddies: Cyber-attackers who essentially depend on existing tools, which have been created by other cyber criminals, for example, exploit computer programmes and scripts (Adams & Makramalla, 2015). These cyber-attackers are immature, and their primary motivation is to get recognition and perform mischievous acts (Aggarwal, Arora, Neha & Poonam et al., 2014; Rogers, 2010).

- Cyber-punks, (virus writers): Cyber-attackers who write virus code to exploit computer programmes for the sake of creating problems and gaining fame amongst their peers, and in the cyber-underworld (Adams & Makramalla, 2015). Furthermore, cybercriminals are motivated by being admired, recognised whilst having a total disregard for authority and/or social norms. These cyber-punks have a slight edge as they have generally more cyber-attacking skills than that of script-kiddies (Rogers, 2010) and attack ICT systems to cause disruption (Dogaru, 2012).

- Insiders: Cyber-attackers that are based within an enterprise that form part of a plan to attack and cause disruptions to the enterprise because of their authorised access (Adams & Makramalla, 2015). Because access is not assessed for authenticity, most attackers from within the enterprise have limited technical expertise (Williams, 2008). As such, these insiders become easy accomplices for criminal syndicates who influence them to commit cybercrime that will expose the computer systems of the enterprise from the inside (Parmar, 2013).

- Petty thieves: Cyber-attackers who commit online fraud such as identity theft and computer system data encryption crime for ransom, with only monetary reward in mind (Adams & Makramalla, 2015).

- Grey hats: Cyber-attackers who are a mix of black hats (i.e. malicious or illegal hackers) and white hats (i.e. hackers intending to improve cybersecurity). These attackers may attack computer systems to prove their cybercrime skill, or to identify vulnerabilities within a computer system, and may even alert the target to the vulnerability (Aggarwal et al., 2014; Bodhani, 2013; Adams & Makramalla, 2015). Grey hats are often highly skilled; however, they write a virus and hacking scripts that cyber-punks and script-kiddies typically use (Rogers, 2010).

- Professional criminals: Cyber-attackers who are hired to infiltrate systems and are known as cyber-mercenaries (Adams & Makramalla, 2015). Sometimes these cyber-attackers work on the instruction of competitor institutions to enter systems for financial gain (Dogaru, 2012). They operate in the most secretive environment and are governed by strict rules of anonymity so that they cannot be easily identified (Rogers, 2010).

For example, politically motivated cyber-attacks may be carried out by members of an extremist group who use cyberspace to spread propaganda, attack websites, and steal money to fund their activities. Generally, the intent of non-politically motivated attacks is normally for financial gain and is considered as cybercrime (Andreasson, 2012), however many cyber-attacks are motivated by deeply rooted socio-cultural issues (Gandhi, Sharma, Mahoney, Sousan, Zhu & Laplante, 2011). Han and Dongre (2014) state, and as shown in *Figure 2.1* below, indicate that cybercriminals can generally be considered as insiders or outsiders, meaning that they act from within an enterprise or attempt to attack the enterprise from the outside.

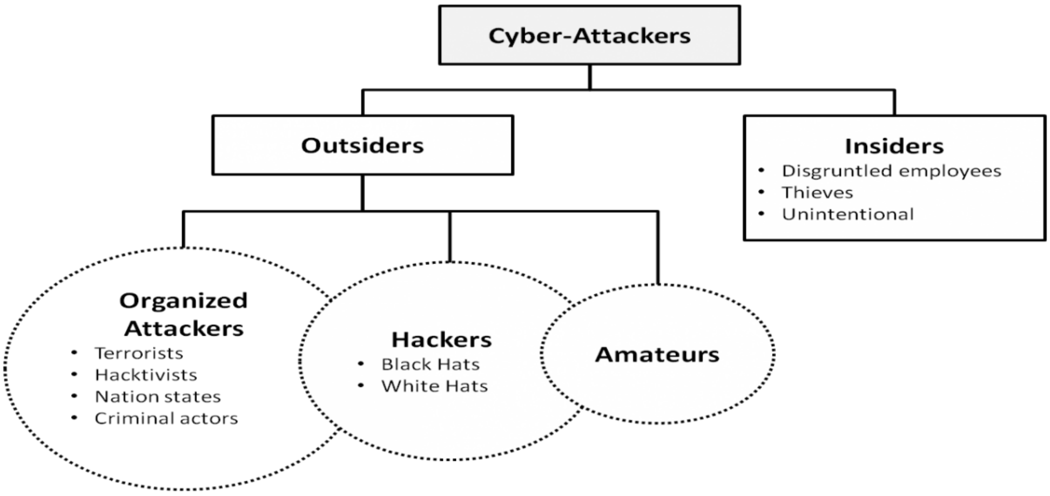


Figure 2.1: Categories of cyber-attackers (Source: Han & Dongre 2014)

The three basic categories of cyber-attacker regarded as insiders are: a) disgruntled employees, who may launch retaliatory attacks by compromising vulnerabilities of computer systems; b) financially motivated insiders, who may misuse enterprise funds by manipulating the ICT system for personal financial gain; and c) unintentional insiders, who may unwittingly facilitate attacks from the outside, but are essentially not the primary attackers (Han & Dongre, 2014).

Outsiders can be classified based on their cybercriminal enterprise, motives, and professional level, being organised attackers, hackers, and amateurs (Han & Dongre, 2014).

- Organised attackers include enterprises of terrorists, hacktivists, nation-states, and criminal actors. Terrorists are those who seek to make a political statement or attempt to inflict psychological damage, or cause destructive ICT damage to nation-states, to achieve their political gain or create fear in countries or the public (Grau & Kennedy, 2014).

- Hackers seek to make a political statement, and ICT destructive damage may be involved, but the motivation is primarily to raise awareness of their activities. Cyber-attackers are solely motivated by ideology and often include terrorist groups. These cyber-hackers are sometimes forced into activism by their strong psychological dispositions and beliefs, some hackers may become hacktivists and perceive their motives to commit hacking to be completely selfless (Adams & Makramalla, 2015).

- Amateurs are less-skilled hackers, also known as script-kiddies or noobs who often use existing hacking tools and instructions which is freely available on the Internet (Andress & Winterfeld, 2011). The motivation of amateur hackers may vary, as some hackers are simply curious or enjoy the challenge, whilst others may be seeking to build a reputation and demonstrate their skills to fulfil the entry criteria of a hacker group (Andress & Winterfeld, 2011). Despite their lower-level skills, these amateurs can cause a lot of damage or, after gaining enough experience, may eventually graduate to professional hacking.

Although these categories are presented as discrete groups, there can be some overlap or difficulty placing a given situation into a box, for example, a group of cybercriminals can act in a coordinated fashion, and in this sense could be considered organised attackers (Han & Dongre, 2014).

2.7.1 Characteristics of cybercriminals

Cybercriminals are drastically different from their general criminal counterparts, whose threatening presence and intimidating demeanour play key roles in the execution of their crimes (Rogers, 2010). Moreover, the remoteness of cybercriminals helps them commit cybercrimes that can be of equal or greater magnitude than traditional crimes and have the ability to hide their behaviour and crimes from their victims and members of law enforcement (Rogers, 2010). Adams and Makramalla (2015) state that cybercriminals are usually located internationally, which makes finding and extraditing them difficult. The intent for these cybercriminals is to commit any crime to cause physical or emotional harm to an individual, enterprise or state (McGuire, 2015).

Moreover, McGuire (2015) further states that it is impossible to construct one profile of the type of person who commits a cybercrime, just as it is impossible to make an accurate profile of all traffic-law violators. Furthermore, even within a particular category of cybercrime, the physiology, psychology, and motivation of each cybercriminal are different from every other. Physiology includes everything from how a single cell function, to what makes your nerve receptors work, and what happens to your muscles when you exercise; whilst psychology is the scientific study of the human mind and its functions, especially those affecting behaviour in a given context or the mental characteristics or attitude of a person or group (Oxford English Living Dictionary, 2016).

Nonetheless, some commonalities are evident of the typical cybercriminal (McGuire, 2015). That situation has changed, as the Internet has become an increasingly a pervasive social medium (Wori, 2014). Now, instead of being inspired by a need to prove their art, cybercriminals are often motivated by financial gain. Consequently, the old stereotypical image of the kid living on Skittles, while doing seventy-two-hour hacks, has been replaced by a much darker and more complex approach, which is well organised and much more focused on practising as a cybercriminal (Wori, 2014). The opportunities for financial gain from cybercrime have become lucrative resulting in established cybercriminal syndicates transitioning to businesses of electronic crime (Van der Meulen, 2015).

As a result, security experts generally agree that law enforcement must learn a lot more about the skill level, personality traits, and various methods of operation of computer criminals (Van der Meulen, 2015). Moreover, cybercriminals hide behind the virtual world of anonymity that the Internet provides. Therefore, it is essential to be able to understand what cybercriminals know, and more importantly, what motivates them (Morley, 2015). It can also be stated, according to Morley (2015), that cybercrimes and cybercriminals differ as much in motive, intent, and outcome as any type of physical criminal.

Behavioural analysis is a key factor to investigate why cybercrime is committed because enterprises are not going to solve computer security issues in isolation or by funding technology solutions with the intent of resolving this problem (Siegel, 2013). It is about understanding how people behave (Siegel, 2013). Cybercrime, which is typically anonymous and originates from a virtual world of computers on the Internet, present the unique behavioural characteristics of the cybercriminal is an invaluable help to the investigation. Shinder (2010) states that profiling a cybercriminal is all about generalisations but knowing the types of people that generally commit specific types of crime can be very helpful in catching and prosecuting the perpetrator of a specific criminal activity.

Moreover, investigators analyse the unique set of behaviours exhibited by the offender to reconstruct a profile of the criminal's distinguishing characteristics. Profiling assumes that the psychological mentality of every individual criminal is different, meaning that each perpetrator will behave differently. Edelbacher, Kratcoski and Dobovsek (2016) state that profiling helps an investigator "see" the person behind the crime. After a basic profile is constructed, which Tropina and Callanan (2015) describe as a description of a criminal's characteristics, is designed without knowing the identity of the suspected criminal, investigators can then compare the suspect's profile against different characteristics of a cybercriminal to further narrow their pool of suspects.

Most classes of crime, even cybercrimes, have a common method of operation (Edelbacher *et al.,* 2016), and these crimes exhibit distinctive individual behaviours that are a result of their unique psychological composition. Bernik (2014) states that to build a profile of a cybercriminal, it must be noted that some generalities apply in all characteristics of cybercriminals, but also caution that it is important to view these characteristics as probabilities, and not as absolute rules, as there are exceptions to each case. Chidambaram (2012) states that cybercriminals are more likely to operate independently are self-motivated aggressive loners who often are not team players and feel entitled to be a law unto themselves. Initially, cybercriminals tend to be counterculture that works alone and on the fringes of society in which they reside (Wori, 2014).

Shinder (2010), and Tropina and Callanan (2015) state that there are always exceptions to profiling, but most if not all cybercriminals display some or most of the following characteristics:

- High tolerance for risk or are thrill seekers.

- “Control freak” qualities, enjoy manipulating or “outsmarting” others.
- Motivated to commit cyber-crime – financial gain, emotionally strong, strong political or religious beliefs, or sometimes just bored.
- Have a minimal amount of being technical savvy, participate in high-risk activities such as committing cybercrime, who has at least some computer experience and use others' malicious code to commit cybercrime.
- Total disregard for the law or believe he/she is above the law and does not believe in rules or complying with the law because it is the law, but rather believe the law is unfair and can be broken. They believe because of their special computer skills and intelligence that they are above the law or that no rules exist in cyberspace.
- Live an active fantasy life and use the Internet to live their fantasies, and often develop an entirely new persona which they fake and use it online to both hide their identities and avoid detection.
- Risk-taker in nature, and often expends more energy for less practical returns in committing cyber-crimes than they would if they turned their efforts to more socially acceptable work. For some of these cybercriminals, it is the risk of getting caught, and the thrill of doing something illegal that makes the life of a cybercriminal attractive. Whilst for others, it is the false sense of control they get from manipulating or outwitting others. Although these two characteristics seem to be in contrast, they can coexist in the same person. The risk-taking element provides the “rush”, while evading detection, makes the cybercriminal feel safe and in control.
- Strong motivations, but the motivations might be wildly different. It takes time, energy, and a certain type of person to commit most crimes, whilst it takes extra effort and a certain level of skill to commit cybercrimes. Most cybercriminals are strongly motivated, from just wanting to have fun, to the need or desire for money, emotional impulses, political motives, or mental illness or psychiatric conditions.

Singer and Friedman (2014) state that forensic psychological profiling of criminals, if used for cybercriminals, that will be progressively useful in catching cyber offenders. Moreover, having a clear understanding of people's behaviour to understand their characteristic traits by forensic behavioural analysis would help develop a data bank of psychological signatures of all suspected persons which would help identify cybercriminals and pre-empt their moves. According to Ernst & Young (2014), a cyber hacker is a person who is highly skilled with the purpose to breach or bypassing Internet security or gaining unauthorised access to software without paying royalties.

Ernst & Young (2013) further state that mining enterprises are becoming far more reliant on integrated ICT systems in pursuit to improve productivity and reduce costs, however, this intent expose and make these enterprises vulnerable to cyber-attacks. Godin and Imbeau (2014) explain that common types of cybercrime include the theft of online banking details, sensitive information theft, personal identity theft, online predatory crimes, and unauthorised computer access. More serious crimes like cyberterrorism are also of significant concern. The idea of the International Criminal Police Organization (INTERPOL) was established in 1914 at the first International Criminal Police Congress, which was held in Monaco.

INTERPOL was officially created in 1923 as the International Criminal Police Commission, and the enterprise became known as INTERPOL in 1956. According to INTERPOL (2015), cybercrime is a fast-growing area of crime, whilst more criminals are exploiting the speed, convenience, and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual. INTERPOL (2015) states previously, cybercrime was committed mainly by individuals or small groups of cybercriminals, whilst in today’s technological environment, underworld criminal enterprises exist, who work with cybercriminal professionals to commit cybercrime, to fund other illegal cyber activities.

The cybercriminal networks are highly complex, and their objective is to commit crimes globally on an unprecedented scale. McClelland (2015), states that cybersecurity must be a top-tier national security priority for communities, enterprises, and countries. Moreover, the national security, economic prosperity and social wellbeing of the cyber community are critically dependent upon the availability, integrity and confidentiality of information and technology. Miller (2014) states that the cybercriminals behind the cyber-attacks are experts who remain hidden from traditional security as they are intelligent, resilient, highly motivated, trained and often well-funded by criminal enterprises in their persistence and efforts to break through an enterprise’s ICT defences.

2.8 BENEFITS OF CYBERSECURITY

Cybersecurity is now needed more than ever before because the ICT marketplace is essentially globalised and vulnerable to cybercrime (Akhgar & Brewster, 2016). There is a growing need to protect personal and classified information as the emergence of the Internet, has resulted in a growing need to protect personal information, business financial data, computer assets, as well as the national security of a country (Jabbour, 2016). During the cold war in 1982, the Central Intelligence Agency (CIA) of the United States planted malicious software code into the Siberian gas pipeline software system in Russia to cause it to malfunction. This malicious software code caused the pipeline to explode (Wilshusen, 2012).

In the information highway of the Internet, everyone is vulnerable, even the President of the United States was a victim of cybercrime (Dupont, 2013). Whilst campaigning for the presidency in 2008, suspected cybercriminals from China and Russia hacked the computers that were used in the campaign of both Barack Obama and John McCain, which compromised classified information such as campaign data (Dupont, 2013). According to McPhee and Bailetti (2013), even though India is emerging as one of the biggest global ICT service providers, it has been the victim of escaped cyber-attacks. In India, in July 2012, more than 10 000 people had their email accounts hacked, which included government officials.

Some of the email accounts hacked included the Prime Minister’s office, Minister of Defence, External Affairs, the Finance Ministry, and Intelligence Agencies. In 2014, according to Nelson (2016), eBay was the victim of an aggressive cyber-attack as hackers managed to steal personal information such as passwords, personal email addresses, physical addresses, customer phone numbers, etc. An information security report generated by Kaspersky antivirus enterprise (Dupont, 2013), points out that in

2013 the enterprise successfully managed to neutralise 5 188 740 554 cyber hacking attempts on ICT environments, personal computers, and mobile devices of unsuspected users.

Therefore, according to Dupont (2013), Nelson (2016) and Wilshusen (2012), it is of paramount importance to have cybersecurity in place to guard against these attacks. As stated by Gabel, Liard and Orzechowski (2015), we live in an increasingly computer interconnected world, that ranges from personal online banking to government ICT infrastructure, however protecting these networks and ICT environments against cyber-attacks is no longer an option, but mandatory. Furthermore, cyber risk is now definitely highly rated on the international agenda bringing fears that hacker attacks and other information security failures could compromise the global economy.

Gabel *et al.* (2015) state that the Global Risks 2015 Insight Report, published by the World Economic Forum (WEF) pointed out a stark cyber security warning, stating that: “90 percent of enterprises globally recognise they are insufficiently protected against cyber-attacks”. Julian (2014) states there is always a need for cybersecurity, whilst enterprises can take security protection precautions to reduce the probability of being hacked. Thompson (2015) states that cybercrime is real and becoming progressively complex and sophisticated, and the world is at a point in time to utilise its information security strategies to decisively deal with the impact of cyber threats and look at a fresh approach to mitigate against cybercrime.

Beissel (2016) states that the benefits of investing in cybersecurity results in risk mitigation. Security breaches and cyber hacking are potentially prevented when investing in cybersecurity, resulting in the reduction of breach costs. Furthermore, some of the benefits from cybersecurity investments can be financial, e.g. prevention of financial losses; or non-financial, e.g. protection of the enterprise’s reputation. Gabel *et al.* (2015) state that the cybersecurity benefits can form part of the list below:

- Protect computer networks and computer systems from unauthorised access.
- Improvement of business information security and consequently business continuity management. Information assets are not compromised.
- Improve the confidence of stake and shareholders in the ICT environment.

- Provide improved business recovery time objectives should an unplanned ICT outage occur.
- Protects ICT environments against viruses, virus worms, spyware, and other undesirable malicious programme code.
- Protects the ICT environment from being hacked by cybercriminals.
- Minimise unplanned computer outages and disruption, which could affect productivity.
- Provide privacy and protection to individual private information as well as enterprise or governmental information.

Wallace and Webber (2015) state that regulatory compliance is a major driver of cybersecurity initiatives. Although according to Wallace and Webber (2015), compliance does not guarantee a secure environment, it is an important first step in aiding both regulatory and internal enterprise policy. Moreover, according to Wallace and Webber (2015) cybersecurity regulatory compliance help enterprises and governments to prevent their ICT environments from being compromised, but a holistic cybersecurity regime should be implemented.

2.9 CHALLENGES OF CYBERSECURITY

Maintaining and ensuring sufficient information security measures, controls and solutions is by no means an easy task especially in the modern era of cybercrime (Ellyatt, 2015). Naggar (2015) states that cyber attackers are becoming more sophisticated in their approach and are now using advanced persistent threats (APT) to break into an enterprise’s secure environment. Many of the cybersecurity solutions that are available in the information security market, require security professionals with the necessary skill to build complex information security models to detect, recognise, remediate, and stop a sophisticated cyber-attack (Cowan, 2015).

The view of Cowan (2015) is that businesses essentially need sophisticated cybersecurity defence mechanisms to present opportunities to the information security enterprises to develop advanced and sophisticated cybersecurity solutions. The ever-increasing adoption rate of the Internet by society and businesses, with various use cases of digitally connected technologies according to McLellan (2015), brings with it an accelerated and complex computer environment, that presents its cybersecurity challenges. Ellyatt (2015) states that one of the biggest challenges of cybersecurity is that as soon as new cybersecurity policies are deployed by businesses or the implementation of cutting-edge cybersecurity tools, cyber hackers find innovative ways to circumvent those security barriers.

In fact, according to Ellyatt (2015), information technology lends itself to cybercrime innovation, which essentially means that Information Technology (IT) security professionals need to be vigilant of any new or existing cyber-threats. Nesbitt (2015) believe that the Internet of Things (IoT), which connects home appliances and vehicles to the Internet, will soon become the “Internet of Vulnerabilities”. Moreover, millions of cyber-hackers could hack into these unsuspecting interconnected systems as system security of these devices have been sacrificed for efficiency (Nesbitt, 2015). The IoT may present exciting business opportunities, however, society and businesses must be cognisant by ensuring that access is limited; secure and that sensitive data should always be encrypted (Drolet, 2016).

2.10 INTERNET SECURITY TECHNIQUES

The Internet age has created vast and ubiquitous databases of the personal information of corporations irrespective of size, government departments, medical records, vendor information, business partners, customers, banking information, student information etc. (Kaufmann, 2017). Therefore, as suggested by Kaufmann (2017) there is a need for internet security and how it is implemented must be balanced thoughtfully against the needs of the enterprise. Moreover, hackers’ continuously changing tactics, with a growing number of cybercriminals and the rapidly expanding and evolving technologies, make it challenging for cyber security experts and businesses to stay ahead of cybercriminals.

While it is impossible to eliminate all the risks of a cyber-attack or cybercrime, Edgar and Manz (2017) states that understanding how to prevent cybercrime is about bringing together an effective combination of technologies, best practices, and well-defined procedures to craft a solution that is best suited for the enterprise. Edgar and Manz (2017) state that fundamentally the vulnerabilities identified on the internet, need new security models and methods. Moreover, information security enterprises need to develop new methods when designing and engineering secure computer systems. Edgar and Manz (2017) state that when addressing cyber security for the longer term, it requires a vigorous sustainable process of fundamental research.

The sustainable process is essentially required to explore the science to develop the technologies necessary to design security tools into computing and networking systems and software. One element of a more realistic model for cyber security may be the principle of mutual suspicion, meaning that every component of a computer system or network is always suspicious of every other component, and access to data and other resources must be constantly authorised (Gordon, 2020). Moreover, generally, cyber security should be an integral part of the design process for any large, complex computer system or network infrastructure. Cybercrime prevention is not a one-size-fits-all approach; enterprises are different in size and have different needs, threats, risk tolerances, vulnerabilities, and capabilities.

With increasing reports of enterprises and the public becoming targets and victims of cybercrime, Edgar and Manz (2017); Kaufmann (2017); Gordon (2020) recommends the list below of cybercrime prevention techniques, however, this list is not exhaustive or limited to these recommendations:

- *Layers of Defense*

Implement layers of defense, starting with the outmost layer of physical security, followed by management-level procedures and policies, firewalls and architecture, security updates and antivirus solutions.

- *Least-privilege principle*

Apply the least-privilege principle, where information and access are limited to a need-to-know basis.

- *Network hardening*

Implement network hardening measures, ensuring patch management is adequate and proactively reviewed.

- *Segregation and protocol-aware filtering*

Implement segregation and protocol-aware filtering techniques to protect against cyber threats that might affect critical systems.

- *Removable device policy*

Implement a sound removable device policy with provisions to ensure all USBs are encrypted and scanned for viruses before being used with other devices.

- *Business continuity plans*

Design business continuity plans, identify key personnel and establish processes from both technical and business perspectives to prevent the negative impact of a cyber-attack from causing any further damage when trying to recover business operations.

- *Third-party providers*

Vetting of third-party providers is essential to ensure they are cyber security compliance

- *Awareness briefings*

Arrange frequent awareness briefings and training programmes to educate all employees on cyber security best practices.

- *Be mindful of which website URL is visited:*

Keep an eye on the URL you are clicking on. Always look for secure URL’s with the https address – the suffix ‘s’ indicates secure. Ensure the internet security product includes functionality to secure online transactions on licks with unfamiliar looking URL’s.

- *Protect children on the Internet*

Parents are required to protect their children from cybercriminals and install software products that filter undesirable content from their children.

- *Ensure Internet security software is current – update it regularly*

Ensure the latest security is always installed and up to date.

- *Lock or log off your computer when stepping away*.

Ensure that no one will have access to your information.

- *Go offline when an Internet connection is not required.*

If your computer is always connected, it increases the chances that hackers can access your computer.

- *Take advantage of security settings.*

On your smartphone, tablet, or computer, use PINs or passcodes to protect your device from being accessed.

- *Consider sharing less online*

Do not share personal information easily with unverified Internet users as this could lead to cybercriminals having access to your information.

- *Use strong passwords*

Use different user IDs / password combinations for different accounts and avoid writing them down. Make passwords complex by combining letters, numbers, special characters and changing passwords regularly.

- *Secure your computer*

Activate the firewall that comes with the Operating System as the first line of defense. Firewalls block connections to unknown or bogus sites and will keep out viruses and hackers.

- *Use anti-virus / malware software*

Prevent viruses from infecting your computer by installing and regularly updating anti-virus software.

- *Block spyware attacks*

Prevent spyware from infiltrating your computer by installing and updating anti-spyware software.

- *Be social-media savvy*

Ensure that your social networking profiles (e.g., Facebook, Twitter, YouTube, WhatsApp etc) are set to private. Be careful what you post online, once it’s on the Internet, it’s there forever.

- *Protect your data – use encryption*

Use encryption when sharing sensitive files such as tax returns, bank statements and detail, financial records etc.

- *Backup data regularly*

Make regular backups of all important data. Store it at a different location and make use of cloud storage.

- *Secure wireless network*

Wi-Fi (wireless) networks are vulnerable to intrusion if they are not properly secured. Review and modify default password and settings. Public Wi-Fi's (known as Hotspots) are also vulnerable. Avoid conducting financial or corporate transactions on these networks.

- *Protect your e-identity*

Be cautious when sharing personal information on the Internet. Make sure that websites are secure (e.g., when making online purchases) and that privacy settings are enabled.

Whilst the above list on Internet security techniques and preventative strategies is not exhaustive, it could be considered by business and their users. Moreover, it is suggested that business adopt relevant technical standards that are suitable to their enterprise to establish a relatively high protection level of security. The recommended Internet security techniques are useful to individuals who have personal computers.

According to Lee (2014), the Internet is the world's most popular interconnected computer network, which started as an academic research project in 1969 and was transitioned to a global commercial network in the 1990s. Radu, Chenou and Weber (2014) state, that the World Wide Web (www) being the Internet, is a popular commercial and research platform, which was designed by Timothy Berners-Lee in 1991. The backbone that hosts the Internet consists of wide-area computer networks, mostly network towers and fibre-optic cables that are connected between data centers and consumers (Beal, 2016). The creation of the web according to Radu *et al.* (2014), in the mid-1990s, saw enterprises such as Google, Yahoo and Amazon building profitable web-based businesses.

Osborne (2015) states, that the Internet has made society information-dependent in both their professional and personal lives. The Internet, together with the Information Communication Technology (ICT) that underpins it, is a crucial national resource for governments around the world and has become a key driver of socio-economic growth and economic development (Dean, DiGrande, Field & Zillenberg, 2012). As a result, governments and businesses have embraced the Internet and the potential of ICT to generate revenue (Klimburg, 2012). Tolica, Senrani and Gorica (2015), state that the economic, technological, and socio-political benefits of the Internet are at risk if services offered is not secure, protected and always available.

2.11 TYPES OF CYBERCRIME

There is a wide range of cybercriminals, according to (McGuire, 2013), ranging from highly organised criminal enterprises to individual cybercriminals to state-sponsored groups. A comprehensive understanding of the types of cybercrime is essential in building effective defences against cybercrime. Today, the key types of threats committed by attackers, include, but are not limited to, the list below as cybercrime is an evolving practice of criminality (McGuire, 2013):

2.11.1 Economically motivated cybercrime

Mercer (2016) states that, as with any crime, it is always concluded that cybercrime involves money as a major motivating factor for many cybercriminals. This is especially true because the dangers of criminal activities are less obvious when cyber-criminals hide behind a virtual network (Mercer, 2016). Moreover, the perception of cybercriminals is that cybercrime is low risk with very high financial reward. This perception encourages cybercriminals to participate in malicious software, phishing, identity theft and fraudulently money scamming attacks (Mercer, 2016).

2.11.2 Data breaches

Symantec (2016) report that in 2013, more than 550 million personal identity information was exploited due to data breaches which are expected to soon exceed 1 billion, and this equates to almost 1 out of every 7 people globally, or about 1 in 3 Internet users. McGuire (2015) endorses this view and states that data breaches of personal information are becoming increasingly extensive, for example intellectual property, trade and business agreements between enterprises, have become the target, not just credit-card data as it was with previous cyber-criminal activities.

2.11.3 Mobile and social

Symantec (2016) states that social media is a key area where cyber threats are proliferating as cyber attackers collect personal data about an individual's interest via social networks which are then used to target their victims via emails in a more convincing manner. Mitchell (2016) states that an extensive range of mobile devices are being used today, which are always switched on, and most of the time network-connected and consequently pose well-known threats from cybercriminals.

2.11.4 Ransomware

Cybercriminal demands payment to decrypt software after installing malicious software on a computer that locks and encrypt the information on the victim's computer. Ransomware is installed on a computer connected network and then encrypts sensitive or critical information by using public-key encryption, which is different from most cyber hacking tools, like malicious software, this encryption key remains on the hacker's computer (Symantec, 2016). The victims of ransomware are then requested to pay large sums of money, using cryptocurrency to receive a private key to decrypt their software. Ransomware is becoming increasingly popular amongst cybercriminals and according to Symantec (2016), it observed an increase of 500% month-on-month in Ransomware incidents.

2.11.5 Internet of Things associated

The IoT is a system of interconnected computing devices, mechanical and digital machines, objects, or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction (Marsan, 2015). Moreover, a Thing on the Internet of Things can be a person with a heart monitor implant, an automobile that has built-in sensors to alert the driver when the tyre pressure is low can transfer data over a network. The IoT evolved from the convergence of wireless technologies, micro-electromechanical systems (MES), microservices and the Internet (Marsan, 2015).

McGuire (2015) points out that to be effective in combating IoT cyber-attacks, cyber security developers must form part of the design of the software products when these products are developed, and not installed later as an afterthought. Van der Meulen (2015) states that the hype of IoT is not unsupported, as there are enough evidence to support the success of the “Internet of Things” in the coming years. According to Van der Meulen (2015), it is estimated that there will be at least a 30% increase in the number of Internet-connected devices in 2016, as compared to 2015 with 6.4 billion IoT devices entering the realm of the Internet of things. The number is expected to increase further to 26 billion by 2020.

The new normal going into the future, according to Kobie (2015), is going to be, that “any object that can be connected will be connected by the IoT”. Van der Meulen (2015) states that as with any evolving technology, there are challenges, which make the viability of IoT doubtful. Furthermore, security is one of the major concerns of experts who believe virtually endless connected devices and information sharing can severely compromise one’s security and well-being. Unlike other hacking episodes which compromise online data and privacy, IoT devices can open a gateway for an entire network to be hacked.

Samani (2016), states that the 2016 Internet Organised Crime Threat Assessment (IOCTA) by the European crime agency Europol, warns that the IoT creates new types of security risks and cyber threats in critical-infrastructure control systems. Samani (2016) also warns that the public can expect to see more targeted attacks on existing and emerging IoT infrastructures. Moreover, these attacks will include new forms of blackmailing and extortion schemes, for example, ransomware for smart cars or homes, data theft and new types of botnets. Samani (2016) identifies three key IoT security challenges:

- A trillion points of vulnerability: Every single device and sensor in the IoT represents a potential security risk. The enterprise cannot confidently state that the new devices have control measures in place to preserve the confidentiality of data collected and the integrity of the data sent (Samani, 2016). Santillan (2015) states at the French graduate and research center in communication systems, Eurecom, researched an estimated 32 000 firmware images from potential IoT device manufacturers and 38 vulnerabilities across 123 products were discovered, including poor software encryption and vulnerable backdoors that could allow unauthorised access to the devices. The manufacturers of these devices include Xerox, Bosch, Philips, Samsung LG, and Belkin.

- Trust and data integrity: Corporate systems will be flooded with data from all areas of connected sensors in the IoT (Samani, 2016). However, an enterprise cannot confirm with confidence that the data has not been compromised or interfered with. Researchers, according to Samani (2016), have successfully demonstrated that smart meters which are widely used in Spain, can be hacked to under-report energy use. However, with the IoT, the security capability does not exist in many of the devices, which will suddenly become connected without any protection.

- Data collection, protection, and privacy: The vision for the IoT is to make the lives of consumers easier and boost the efficiency and productivity of businesses and employees (Salim, 2015). The data collected will help society make smarter decisions; however, this will also have an impact on privacy expectations. Furthermore, according to Salim (2015), if data collected by connected devices is compromised, it will undermine trust in the IoT. Trust, according to Salim (2015), is the foundation of the IoT and that needs to be underpinned by security and privacy as a society to reap the benefits of the connected world.

Consumers, software developers and service providers need to clearly understand the ICT security issues associated with the different devices, which provide IoT solutions (Salim, 2015). However, if security and privacy factors were kept intact, it would not be an unattainable goal, though it will be tricky.

2.11.6 Personally motivated cybercrime

Cybercriminals are all humans, and their crimes are often driven by personal emotions and vendettas (Paganini, 2013). The motivation to commit cybercrime ranges from a disgruntled or unhappy employee who knowingly installs a malicious virus on office computers, or an unhappy student who will compromise any legal website just to demonstrate that he/she can create a sense of achievement.

2.11.7 Ideologically motivated cybercrime

Paganini (2013) reports that after financial institutions like Visa, MasterCard and PayPal refused to let debit or credit cardholders contribute to the controversial non-profitable website WikiLeaks, the "hacktivist" group *Anonymous* coordinated a series of robotic cyber-attacks on the ICT infrastructure of these financial institutions, which rendered their computer servers inaccessible to Internet users. These kinds of cyber-attacks are conducted for perceived ethical, ideological, or moral reasons, which damages or disable computer equipment and/or network infrastructures to express grievances against individuals, corporations, enterprises, or even national governments (Paganini, 2013).

2.11.8 Cyber-espionage

Sutherland (2016) state that espionage is generally associated with a sovereign state or large enterprises experiencing cyber-attacks aimed at gathering classified information from a victim. Sutherland (2016) further indicates that espionage was always seen as an activity of individuals who physically penetrated or compromised vulnerabilities within a targeted enterprise, however, this has changed to a craft that is more technological than physical.

This is all possible as ICT storage infrastructures now store information electronically that was once kept in an enterprise manual paper ledgers, blueprints, and papers, (Sutherland, 2016). Cyber espionage is an underground criminal activity whereby attackers plan to avoid being detected, at least until they achieve their primary objective (Rubenstein, 2014). Moreover, these cybercriminals are among the most persistent of cyber attackers and often continue to attack different vectors, even after they have been detected.

These cybercriminals exit the computer systems and in doing so, they cover their digital footprint or attempt to retain access through a vulnerable backdoor that they create for later use. If they succeed with their hacking and successfully cover their footprint, the hacked enterprise might never know that its security defences have been compromised (Rubenstein, 2014). Cyber espionage is very similar to traditional forms of industrial espionage, as cyber-hackers gain unauthorised access to confidential or classified information. Cyber-espionage is committed for various reasons, that include intelligence-gathering purposes, financial gain, or a combination of both (Finklea & Theohary, 2015).

2.11.9 Politics or social justice

Politically motivated cyber attackers mainly seek to acquire classified government or political information by sabotaging this information, especially in times of heightened military tensions or conflict (Sutherland, 2016).

2.11.10 Identity theft

The theft of an individual’s identity happens when a cybercriminal gains unauthorised access to personal information, such as full names, residential addresses, dates of birth, banking account details, personal photographs, medical records, personal information about family members, etc. so that money can be stolen or other financial gain or criminal benefits that can be used against the victim (Moore & Edwards, 2014). This view is endorsed by Nemati (2014) who states that the theft of a person’s identity is a criminal act whereby criminals obtain sensitive information about a person unlawfully, and then use this information to commit fraudulent activities.

According to Moore and Edwards (2014), personal information can be used by cybercriminals to apply for credit or other facilities, such as opening a bank account, creating fake personal identity documents or using the information maliciously. Identity theft of personal information and fraud is regarded as one of the most common types of cybercrime (Van der Meulen, 2014). Moreover, the term identity theft is used when a person impersonates another person, to commit financial fraud for personal gain. This online crime usually transpires on the Internet which is referred to as Online Identity Theft (OIT). The most common sources where identity information of victims are stolen is from websites of government and financial institutions (Nemati, 2014).

2.11.11 Online trading scams

Online trading scams involve cyber scammers that target unsuspecting individuals who buy, sell or trade stock on the Internet (Dicks, 2012). According to Dicks (2012), online trading scammers may:

- Advertise day-to-day products for sale at very cheap prices, and once payment is finalised the products are never delivered.

- The scammer will pay an additional amount for goods, more than the advertised amount, then come up with an excuse for the overpayment of the goods. The buyer will then request that the excess amount be repaid to the scammer/seller party before the seller realises that it was a fraudulent activity.

- Take advantage of charity enterprises by impersonating and requesting donations.

- Claim that your personal computer is infected with a virus and has been compromised, and then request to access your computer remotely to resolve the issue.

- Attract individuals with offers for “free” goods and request the unsuspecting individual to subscribe to mobile premium services.

Moreover, there are a large amount of different online and internet scams, which aim to cheat unsuspecting individuals and social media users.

2.11.12 Plastic or credit card fraud

Plastic card or credit-card fraud is defined as the unauthorised use of “plastic”, credit or debit cards, or obtaining the card numbers unlawfully for personal monetary gain (Newman & Clarke, 2011). This type of cybercrime essentially involves cybercriminals who use stolen credit or debit card details at automatic teller machines and retailers in countries that have not yet upgraded to Europay, MasterCard, Visa (EMV Chip) and personal identification number (PIN) (Newman & Clarke, 2011). There are several means that fraudsters use to obtain card details, such as phishing for personal information, skimming, sending spam e-mails, or hacking an enterprise’s information database.

2.11.13 Unauthorised access

Unauthorised access is when a cyber hacker gains unauthorised access to a computer system of an unsuspecting owner (Newman & Clarke, 2011). Once the criminals have compromised a victim’s email, banking, or personal information, they can have the ability to reset user passwords, or to prevent the unsuspecting victim from legitimately accessing his/her accounts lawfully (Newman & Clarke, 2011).

2.11.14 Malware

“Malware” is a term that is used to describe different types of malicious software programs (malware) and often include viruses, computer worms, spyware software and trojans (Sloan & Warner, 2014). Moreover, cybercriminals normally use malicious software (or malware) that is installed on a victim’s computer to monitor and capture their online activity and later perform fraudulent activities on the computer system. In fact, according to Sloan and Warner (2014), malware is often downloaded to a user’s computer and activated when an unsuspecting victim inadvertently executes an infected electronic mail attachment or click on a suspicious web link imbedded in an electronic mail.

Furthermore, malware can also be used to steal sensitive or classified information, usernames, passwords, or other information, that is then forwarded to a cyber syndicate to commit cybercrime. Malware is a malicious program code that has evolved into stealthy, complex arsenals that are used by experienced cybercriminals and novice identity thieves to commit cybercrime (Khanse, 2014). Spyware – spyware is a general term used to describe computer software that performs certain unauthorised behaviours on a computer (Khanse, 2014). Khanse (2014) states that spyware is often associated with software that displays advertisements (called adware) and is used to track personal or classified information.

However, it does not mean all software that provides online advertisements is bad. Managing spyware on a computer can be extremely difficult because most spyware is designed so that it cannot be removed easily. Furthermore, other kinds of spyware typically amend software programs on a computer and cause the computers to slow down in performance or crash. These programmes generally change a user’s web browser's home page, or search engine page, or even add additional components to the browser that the user does not need or want. The software is designed in such a way that makes it difficult for the user to reset the settings back to the way it was before spyware was installed (Khanse, 2014; Chen, 2014).

Viruses – According to Khanse (2014), viruses are small computer programs that are designed to replicate themselves on a victim’s computer and unknowingly spread to other computers. Some viruses are relatively benign, whilst other viruses are malign, that causes computer programs to fail or execute incorrectly, and may even destroy or corrupt valid files, while also formatting the hard disk of a computer. When a hard disk is reformatted, it essentially wipes all the information from the hard disk.

Worms – Instead of infecting a relatively small number of files on the computer, it infects the entire computer rapidly (Khan, 2013). Furthermore, a computer worm is a self-contained program or set of computer programs that can spread functional copies of itself on a network or its segments to other computer systems, usually via network connections.

Trojans are malicious software that disguises itself as software that the user may want to use or install; however, the Trojan horse then performs malicious actions by typically allowing backdoor access to the computer (Khan, 2013). In computing terms, a Trojan horse is a software program that appears harmless, but is, in fact, malicious (Rouse, 2016). Moreover, cybercriminals have always used Trojan horses as a trick for end-users to unknowingly install malicious software.

Typically, the malicious programming is hidden within an innocent-looking email attachment or free programme, such as a game. When the user downloads the Trojan horse, the malware that is hidden inside is also downloaded. Once inside the computing device, the malicious code can execute whatever task the attacker designed it to carry out (Rouse, 2016).

2.11.15 Hacking

Hacking is one of the most widely used cybercriminal activities that cyber hackers use to gain unauthorised access to computer systems to steal, change or destroy the information or install malicious software without the knowledge or consent of the victims (Ellis, 2014). The clear-cut definition of hacking is “the unauthorised access and subsequent use of other people's computer systems” (Ellis, 2014). However, the word *hacker* did not have the negative connotation as it has today. Sloan and Warner (2014) explain that the hacker attacks are carried out in several phases, which starts with information gathering, scanning the environment, and finally gaining unlawful access to a target system.

The information-gathering process involves obtaining information unlawfully in an ICT environment. The cybercriminal will expose the security vulnerability by obtaining information about the target environment before proceeding to hack it (Sloan & Warner, 2014). Hackers may be perceived as benign explorers, malicious intruders, or computer trespassers (Shakarian, Shakarian & Ruef, 2013). In some cases, hacking is not a malicious activity according to Grau and Kennedy (2014), and they state that a *white hat* hacker is someone who uncovers weaknesses and vulnerabilities in computer and network systems to contribute to improving the ICT environment, often with permission or as part of a contract with the owners.

2.11.16 Denial of service or distributed denial of service attacks

A denial-of-service attack floods a computer or website with data, which cause an overload to the bandwidth of a network or computer system and force into a hung state before the ICT environment malfunction (Dicks, 2012). Unlike hacking or malware, it generally does not involve access to the computer system. According to Nemati (2014), a distributed denial of service (DDoS) attack is an attack on normal functioning services by broadcasting a flood of data traffic from multiple computer systems, intending to compromise a computer network.

Cevidalli and Austen (2016) state that Denial of Service (DoS) attacks flood a computer server with thousands or millions of page requests that originate from bot-infected computers around the globe. When these computers are widely distributed, the ensuing shutdown is termed a *Distributed Denial of Service (DDoS)* and can result in serious losses. Moreover, many major enterprises have suffered such attacks, requiring them to take expensive preventive measures and extend their backup services.

2.11.17 Spam

Spam is associated with electronic junk mail which (Ellis, 2014) points out as unsolicited messages sent to a victim via electronic mail, text messages or instant messages without the recipient’s knowledge or consent. Moreover, spam messages often contain offers of free goods or “prizes”, cheap products, promises of wealth or similar offers. The recipient of these emails might be asked to pay a joining fee to a service, to buy something to “win” a prize, or to call or text a telephone number (calls made to these numbers are charged at premium rates), which is essentially unwanted emails and messages that the recipient doesn’t need. Spamming is unsolicited or unwanted email that is generally used for advertising via electronic mail (email).

Furthermore, according to Chen (2014), although email spam is the most common form of spamming, other spamming methods do exist, for example, mobile phone-messaging spam and Instant Messaging spam. Spamming involves sending nearly identical messages to thousands (or millions) of recipients. Spammers make use of software robots, called spambots to get valid email addresses from enterprise websites, blogs, and newsgroups. Spam messages normally have a fake origin address, which is randomly generated by a computer program, so that the author of the message from where the message originates is not easily discovered (Chen, 2014). Moreover, spam messages are always sent with fake return email addresses, which is then referred to as junk mail.

2.11.18 Phishing

Phishing is a way that criminals use to trick unsuspecting people into giving out their personal or financial details (Bullock, Haddow & Coppola, 2013). Phishing messages are sent to victims in a disguised format as a legitimate electronic message from a business. Moreover, phishing is an unlawful process whereby cybercriminals offer a reward to the recipient to solicit personal information that cybercriminals later use for unlawful activities. According to Rouse (2016), state that a phishing attacker masquerades as a legitimate business to convince victims to provide banking account details, personal user identification, user passwords or credit card details.

Phishing is popular with cybercriminals, as it is far easier to trick someone into clicking a malicious link in a seemingly legitimate email, than trying to break through a computer's defences (Rouse, 2016). Although some phishing emails are poorly written and fake, sophisticated cyber criminals employ the techniques of professional marketers to identify the most effective types of messages (Rouse, 2016). Furthermore, Rouse (2016) describes spear-phishing methods as follows:

Spear-phishing attacks are directed at specific individuals or enterprises, while incidents that specifically target senior executives within an enterprise are termed whaling attacks. Those preparing spear phishing campaign research their victims in detail to create a more genuine message, by using information relevant or specific to a target, which increases the chances of the attack being successful. Phishers use social networking and other sources of information to gather background information about the victim's personal history, interests, and activities. Targeted attacks and advanced persistent threats (APTs) typically start with a spear-phishing email containing a malicious link or an attachment.

2.11.19 Malvertising

Malvertising according to Murray (2013) is a process whereby users unwittingly download malicious program code by merely clicking on an advertisement on a website that is infected with a virus. Moreover, the websites are innocent, and these cybercriminals insert malicious and infected adverts on legitimate websites that are unbeknown to the webmasters or the owners of the website. However, in other cases, as pointed out by Murray (2013), the cyber criminals show clean advertisements for a period and then replace them with malverts so that the website owner or webmaster does not suspect any criminal activity when these advertisements are embedded on the web page. Malvertising is rapidly on the rise in becoming a cybercrime tool to be used by cybercriminals (Murray, 2013).

2.11.20 Corporate-account takeover

The emergence of a new cybercrime method was identified in 2008, known as, corporate account takeover (Murray, 2013). A huge concern, according to Murray (2013) is that this type of cybercrime put financial constraints on corporations and is believed to be the stealthiest type of cyber-attack. Cybercriminals perform this activity covertly to obtain an entity’s financial banking credentials, then use computer software programs to capture one of the corporate’s computers remotely, and finally siphon funds from the corporation’s bank account, which often amount to millions of dollars.

2.11.21 Computer viruses

Zimmer (2012) defines computer viruses “as computer software programs that, when executed, install copies of the program code onto hard drives of the computer without the consent of the user”. As warned by Zimmer (2012), when creating a computer virus and distributing it to unsuspecting victims it is regarded as cybercrime. Moreover, the virus may steal disk space, access personal and sensitive information, corrupt data on the computer or send information out to other computer users' personal contacts. The two most common ways for a virus to infect a computer is by way of an email attachment or the copying of files (Zimmer, 2012).

In some cases, if the virus is opened by a computer on a system network, such as the place of employment of the user, the virus can immediately spread throughout the network without needing to be sent via email. Computer viruses can be removed from the user's infected computer system using specialised software, and in some cases, they are not removed, and a total rebuild of the computer system or environment is needed (Dicks, 2012). It must be noted, according to Dicks (2012), that cyber criminals who cause computer inoperability or gain unauthorised access to a security-protected computer system can face imprisonment and be ordered the payment of financial losses suffered by an individual or enterprise.

2.11.22 Cyberstalking

Cyberstalking is defined as "the use of the Internet or technology to stalk or harass a person, an enterprise or a specific group" (Maiuro, 2015). There are many ways in which cyberstalking becomes a cybercrime as it includes monitoring their victim's activity in real-time, i.e. while the user is working on their computer or mobile device. Cyberstalking is regarded as a crime when it is performed with repeated threatening and harassment behaviour or monitoring a person's activity by an individual without authorisation (Maiuro, 2015). An example of cyberstalking would be to put a recording or monitoring device on a victim's computer or a smartphone to save every keystroke they make so that the stalker can obtain information. Another example would be to repeatedly post derogatory or personal information about a victim on web pages or social media, despite being warned not to do so. Maiuro (2015) also notes that cyberstalking can lead to imprisonment.

2.11.23 Intellectual property

Murray (2013) state that intellectual property, include commercial copyrighted materials such as music, movies and books. However, it must be noted according to (Murray, 2013) that music producers rate high on the list of victims, whilst commercial entities that hold copyrights or patents also need to remain vigilant. According to Murray (2013), intellectual property theft is a complex issue to combat when carried out by state-sponsored hacking countries, especially China. More commonly, according to Murray (2013), cybercriminals illegally download entertainment intellectual property, such as movies, music, and books, and then use it without payment or sell it for a profit, meaning non-compliance with copyright laws. Ellis (2014) states that music is purchased legitimately and re-sold many times unlawfully on a website. This is done by loading the CD/DVD online in digital format, which is a breach of copyright laws (Ellis, 2014).

2.11.24 Cyber-harassment or bullying

Cyber-harassment or bullying is the use of automated information and communication tool such as electronic mail, instant messaging, text messages, blogs, mobile phones, and defamatory websites to harass an individual by attacking the persons persona. (Foody, Samara & Carlbring, 2015). During a physical confrontation, there is an endpoint, but when the hecklings and humiliation is directed to a child, its torture, and never stops (Foody *et al.,* 2015). Moreover, cyber-bullying that include taunts, insults, and constant harassment on social media and or electronic text messages has become widespread among the youth, and in some cases results in undesirable tragic consequences, and Foody *et al.* (2015) points out that cyber-harassment and bullying have affected every education institution in every country.

2.11.25 Sniffing

A *sniffer* is a computer program used to eavesdrop and generally legally used by government surveillance agencies or by telecommunication enterprises to identify network bottlenecks, however it is also used by cybercriminals to obtain proprietary information. *Email wiretaps* are small computer programs that are hidden in an email message and allow subsequent messages forwarded by the recipient with the original message to be monitored and tracked (Tarakanov, 2016).

2.11.26 Bots (short for robots)

Bots could be malicious computer program covertly installed on computers that are connected to the Internet. Moreover, unknown to their owners, these computers can then be controlled by third parties. Collections of these computers (botnets) are commonly used for Denial of Service (DoS) attacks (Cevidalli & Austen, 2016).

2.11.27 Web-based attacks

Typically involve techniques that redirect the Internet browser to malicious World Wide Web sites (Ashford, 2014). Furthermore, web threats and malware are malicious software programmes that are designed to target users when they are online, using the Internet. These threats can appear in many forms, including viruses, spam, phishing, spyware, and other versions of cybercrime (Williams, 2014). Moreover, these browser-based threats include a range of malicious software programmes that are designed to infect a victim’s computer or steal sensitive data.

2.12 INFORMATION SECURITY SYSTEMS

Computers and digital devices have become essential to enterprises that have increasingly become a target for cyber-attacks. Enterprises or individuals who wants to use a computing device with confidence must first be assured that the device is not compromised in any way and that all communications will be secure (Bourgeois & Bourgeois, 2014). Information security systems are measures taken to reduce information security risks, such as information breaches, data theft, and unauthorised changes to digital information or information systems. Information security systems are controls intended to help in protecting the availability, confidentiality, and integrity of data (Garcia, 2019). Moreover, these information security systems are devices and software intended to strengthen cybersecurity.

2.12.1 Firewalls

A firewall is a network security device that grants or rejects network access to traffic flows between an untrusted zone (e.g. the Internet) and a trusted zone (e.g. a private or corporate network). The firewall acts as the demarcation point or “traffic cop” in the network, as all communication should flow through it, and it is where traffic is granted or rejected access. Firewalls enforce access controls through a positive control model, which states that only traffic defined in the firewall policy is allowed onto the network; all other traffic is denied (known as “default deny”) (Zeltser, 2015). Firewalls, information intrusion detection systems, antivirus programmes and two-factor authentication products are just some of the tools available to assist in protecting an enterprise network and information (Zeltser, 2015).

2.12.2 Information Intrusion Detection Systems

An Intrusion Detection System (IDS) is a network security technology solution originally built for detecting vulnerability exploits against a target application or computer (Zeltser, 2015). Moreover, IDS need only to detect threats, and as such is placed out-of-band on the network infrastructure, meaning that it is not in the true, real-time communication path between the sender and receiver of information. IDS was originally developed this way because at the time the depth of analysis required for intrusion detection could not be performed at a speed that could keep pace with components on the direct communications path of the network infrastructure. The IDS monitor traffic and reports its results to an administrator but cannot automatically take action to prevent a detected exploit from taking over the system (Zeltser, 2015). Attackers are capable of exploiting vulnerabilities very quickly, once they enter the network, rendering the IDS an inadequate deployment as a prevention device (Rouse, 2015).

2.12.3 Anti-virus programmes

An anti-virus software program has the ability to scan files and to identify and eliminate computer software viruses and other resident malicious software (malware) (Zeltser, 2015). Anti-virus program software typically uses two different techniques to accomplish this, namely:

- Perform system scan to find known viruses through a virus dictionary installed on the computer.
- Identify suspicious behaviour from any computer software program, which might be seen as a suspicious computer virus.

Most commercial-off-the-shelf anti-virus software uses both of the above approaches, with an emphasis on the virus dictionary approach (Zeltser, 2015).

2.12.4 Two-factor authentication products

Two-factor authentication is a security authentication process in which the user is challenged to be authenticated in two stages; one is generally a physical token, such as a token card; and the other is typically a password that must be memorised, such as a security identification code. In this context, the two factors involved are sometimes spoken of as something you *have*, and something you *know* (Vacca, 2013). A common example of two-factor authentication is a bank card: the card itself is the physical item and the personal identification number (PIN) is the data that is linked to it (Rouse, 2015).

2.12.5 Security

Security is a process and as such no tool can be “set and forget”, essentially affirming that all security products are only as secure as the people who configure and maintain them, and thus highly skilled security professionals should be tasked to manage an enterprises ICT environment (Vacca, 2013). The area of information security is based on protecting assets in general. Information security (IS) is concerned with protecting information in all forms, whether written, spoken, electronic, graphical, or using other methods of communication. However, network security is concerned with protecting data, hardware, and software on a computer network, which is essentially the ICT environment (Rhodes-Ousley, 2013).

Moreover, the practice of information security is all about reducing risks to assets, to acceptable levels by using a layered, comprehensive approach, so that all risks are mitigated and controlled even when one control fails. The field of information security constantly evolves, but the basis of good security practices has not changed throughout history. Goodrich and Tamassia (2014) state that enterprises implement information-security measures to solve specific business security problems and produce results that are consistent with clearly identified business requirements, tangible business benefits by reducing costs and creating new revenue opportunities.

It can thus be stated according to Goodrich and Tamassia (2014) that the security and maintenance of information improve revenue growth whilst controlling losses. Moreover, a good information security programme is used to manage proactive security efforts whilst policies and procedures are used to manage reactive security efforts. Together, a well-designed security strategy and tactics results in an effective, efficient, business-driven security programme. Moreover, information security programme implementations are often weak because of inadequate skilled and technical resources, commitment, and time and funding.

2.13 CYBERCRIME METHODOLOGIES

Cybercriminal activity on the Internet is pervasive and increasingly sophisticated (Roberts, Indermaur & Spiranovic, 2013). Moreover, attackers use a variety of methods to commit cybercrimes, to cause harm using the Internet. Furthermore, in order to protect information against this ever-evolving discipline essentially mean an understanding of the different types of cyber-attacks, but also identifying methods to prevent becoming a victim of cybercrime. Some of the approaches used to commit cybercrime are discussed below.

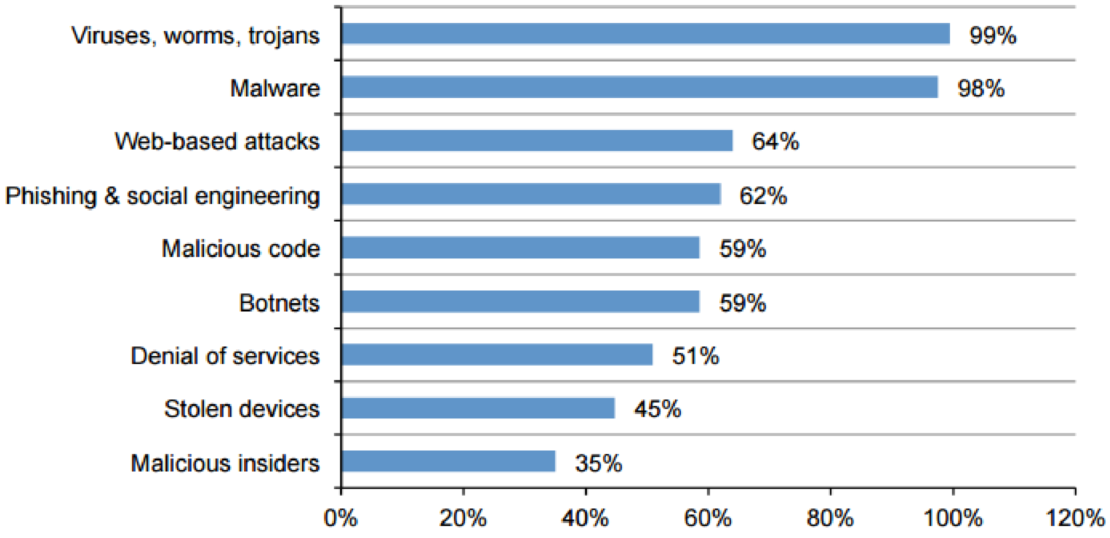
2.13.1 Common cybercrime techniques

Houck, Crispino and McAdam (2012) state that the organised criminal community targets credit-card and banking personal information of unsuspecting banking clients who transact using the Internet. The sale of this information to counterfeiters of credit, debit card and travel documents have proven to be extremely lucrative (Houck *et al.,* 2012). These cybercriminals use software designed to extract this sensitive information, for example, Trojan horses, viruses, and worms, which according to Houck *et al.* (2012) fall into a similar malicious software category. Moreover, this software is computer programs that are designed to infect computers or replicate themselves onto a computer of unsuspecting users; however, each program operates very differently.

An important difference between computer viruses and worms is that computer viruses require an active host software program or an already infected and active operating system in order for viruses to execute, and consequently causes harm and infect other executable files or documents, while worms are stand-alone malicious programs that can self-replicate and mutate via computer networks, without any intervention (Griffiths, 2015). Moreover, the costliest cybercrimes in 2015 were those carried out by malicious cybercriminals who committed DoS and malicious web-based cyber-attacks (DoS, or a Denial-of-Service attack, is an attack that flood a website with Internet traffic that causes it to go into a non-responsive state).

The global financial services and energy sectors were affected by DoS attacks, resulting in an annual average cost of $13.5 and $12.8 million respectively (Griffiths, 2015). Mehan (2014) states that in the decade of the rapid growth of information sharing, the Internet was enabled with an enormous growth of information, which resulted in information security as a global concern. However, the growing concern about cybercrime and the erosion of personal privacy have governments and agencies around the world discussing the need for international action and legislation to seek the right standards to implement, to improve cybersecurity.

Figure 2.2 below reviews nine different cyber-attack vectors as the source of the methodology of cybercrime, as per the Ponemon Report on Cybercrime in 2015. A benchmark of 252 enterprises that experienced a total of 477 discernible cyber-attacks. The list below shows that the number of successful cyber-attacks experienced by firms has progressively increased. Figure 2.2 Types of cyber-attacks experienced by 252 benchmarked enterprises



Source: 2015 Cost of cybercrime study: Ponemon 2015 Cost of Cyber Crime Global 2015

The figure summarises, in percentages, the types of cyber-attack methods that participating enterprises experienced. Virtually all enterprises experienced cyber-attacks concerning computer viruses, worms and/or Trojans and malicious software over the four-week benchmark period; 64% experienced web-based cyber-attacks and 62% experienced phishing and social engineering cyber-attacks. Most enterprises also experienced malicious code and botnets (both 59%) and denial of service attacks (51%). Only 35% of enterprises say a malicious insider was the source of the cybercrime.

2.14 CYBER-ATTACKS IN DEVELOPED COUNTRIES

Granville (2015) reports that many cases of cyber-attacks are ever-increasing, which is why US President Obama recently proposed a sharp budget increase on cybersecurity, to $14billion. According to Granville (2015), some of the major cyber-attacks on the United States businesses community include, but is not limited to the brief list of enterprises below:

A health-insurer enterprise, which is based in Washington State, reported that medical details of about 11 million members have been affected by a cyber-attack in 2015. Hackers gained access to the enterprise's computers on May 5, 2015, and the breach was not discovered until January 29, 2016. The breach exposed members' names, dates of birth, social security numbers, mailing and email addresses, phone numbers and bank account details. In November 2014, a huge cyber-attack was launched on Sony Pictures essentially clearing data of several internal data centres, resulting in the cancellation of the theatrical release of "The Interview", a comedy about the fictional assassination of the North Korean leader Kim Jong-un.

During this cyber-attack, confidential contracts, salary details, film budgets, and entire film data were leaked. Between July and August 2014, the computer and data networks of JPMorgan Chase were infiltrated in a series of coordinated, sophisticated cyber-attacks that extracted large amounts of data, including banking account information. The banking account information of about 83 million households and small businesses were compromised, and authorities determined that the same hackers tried to gain access to the information systems of at least twelve other financial institutions. In December 2013, Target, a retail enterprise in the United States, experienced one of the largest cyber-attacks ever experienced by a retail enterprise.

Harvey (2014) reports that hackers stole credit and debit card records of more than 40 million customers, as well as the personal information of more than 70 million people. The Target breach was caused by malware (malicious software), which was installed on the enterprise's networks and data centre storage components, the malware was then used to extract sensitive and confidential information of their customers. When the breach was made public, the enterprise sales suffered major losses and its profit margins for that quarter declined by 46%. The enterprise agreed to pay $10 million in response to a lawsuit brought by shoppers, which was affected by the breach. Harvey (2014) reports that the biggest bank heist in history was the $480m Bitcoin cyber-heist.

Bitcoin which is a viable currency also suffered reputational damage and later filed for bankruptcy in response to the digital robbery that has been labelled as the world's biggest cyber-heist in history (Peterson, 2016). Bitcoin customers can buy goods anonymously in online marketplaces that are registered to use the virtual currency which is also a practice to evade sales tax and currency controls. Bitcoin is a unique solution whereby an enterprise called MtGox provides a way to convert official currencies such as ZAR and dollars into virtual coins, called Bitcoins. According to Peterson (2016) of the Washington Post, hackers caused a power outage in the Ukraine, which researchers say is signalling a potentially troubling new escalation in digital attacks.

Peterson (2016) states that this is the first incident where an attack caused a power outage and has always been a scenario that has been worrying for years because it causes major disruptions to all industries and government sectors. The blackout left a large region without power, which was caused by a computer virus that disconnected electrical substations from the power grid. In this case, the hackers used malware, named BlackEnergy that wiped files off the central computer systems causing them to shut down. Ashford (2014) reported that the theft of banking and credit card information from the Mandarin Oriental Hotel group highlighted the security risk and vulnerabilities of legacy point of sale (POS) systems.

The hotel group confirmed banking and credit card information was stolen from an “isolated number” of payment card systems at their European and US hotels after the enterprise’s ICT and network infrastructure was hacked. Moreover, the Hilton Hotel group was scammed by a similar attack, as was Starwood Hotels, which owns Sheraton and Westin, the Trump Hotel Collection, Hard Rock’s Las Vegas Hotel & Casino, the Las Vegas Sands Casino, and FireKeepers Casino and Hotel. Donnelly (2015) reports that IT security firm FireEye claims to have uncovered a decade-long cyber-espionage campaign against firms in Southeast Asia and India.

Furthermore, the Chinese government has been accused of being involved in a decade-long cyber-espionage campaign aimed at stealing classified information from enterprises in Southeast Asia and India (Donnelly, 2015). The declaration was made in a report by IT security firm FireEye, whose research team named the perpetrators as APT30 and claimed they have been actively involved in procuring political, economic and military data from enterprises in the aforementioned regions since 2005. Wilson (2015) reported that a cybercriminal gang used distributed denial of service (DDoS) attacks to extort bitcoins from their victims since July 2014, ramped up operations despite a monetary reward of $26,000 for their successful prosecution, according to Arbor Networks.

Ashford (2014) states that the cybercriminal gang, calling itself DD4BC (DDoS for Bitcoin), has been rapidly increasing the frequency and scope of its DDoS extortion attempts, shifting from targeting Bitcoin exchanges to online casinos and betting shops, and most recently, prominent financial institutions in the US, Europe, Asia, Australia and New Zealand. According to Ashford (2014), the fastest growing fraudulent activity is the purchasing of airline tickets online, using stolen credit-card details, resulting in estimated losses of €1 billion to the global airline industry. Police successfully arrested 130 suspects in connection with this type of cyber fraudulent activities at 140 airports around the world during an international law-enforcement operation.

The operation was aimed at combating online fraud and was conducted in collaboration with the global airline and travel agencies as well as credit card institutions. More than 60 airlines and 45 countries were involved in the sting operation, which took place at over 80 airports across the world. According to Oerting (2014), the operation was called Operation Onymous and was coordinated from Europol's European Cybercrime Centre (EC3) in The Hague, and supported by the UK-led Joint Cybercrime Action Taskforce (J-Cat). Police in Bulgaria, the Czech Republic, Finland, France, Germany, Hungary, Ireland, Latvia, Lithuania, Sweden, Luxembourg, Netherlands, Romania, Spain, Switzerland, and the UK were involved in Operation Onymous. While enterprises will never be able to make cybercrime go away, there is a lot that can be done to reduce the risk to the business (Oerting, 2014).

2.15 CYBER-ATTACKS IN DEVELOPING COUNTRIES

Rasool (2012) reported that the South African Post Office Bank, which forms part of the South African Post Office, experienced the biggest cybercrime in South Africa to-date when losing R42 million to cybercriminals. Frank (2015) states that South Africa has become a very attractive target for cyber-attacks as it is a regional hub on the African continent for the banking industry and host the headquarters of most enterprises, compared to the rest of Africa. Some of the South African cybercrime activities are mentioned below. Rondganger (2007) reported as far back as 2007 the increase in cybercrime in South Africa in that the Scorpions exposed a multimillion-rand online bank-hacking syndicate when the mastermind of this scam was arrested.

The cybercriminal agreed to a plea-bargain with the state, and the 30-year-old Kempton Park man was sentenced to eight years in jail; this was after he confessed to committing a range of online fraudulent activities that amounted to millions of rands. His first successful hack was against a First National Bank (FNB) client using sophisticated software programs to glean people's sensitive banking login details. He was able to transfer R9.8 million from an enterprise's bank account into multiple host accounts, which he set up. Balancing Act Africa News reported in January 2016, that a hacker successfully hacked into 53 South African websites in less than an hour. The person or group of persons succeeded in destroying all the websites within half an hour.

The State Information Technology Agency (SITA) reported in 2015 that it suffered a massive cyber-attack in which its online computer servers were accessed over the Internet and confidential data leaked. The leaked information contained a database with records of full names, usernames, electronic mail addresses, encrypted passwords, physical addresses, phone, and fax numbers of SITA officials. A second database, which was accessed, contained electronic mail addresses and phone numbers of the South African Government officials, including parliamentarians. Amir (2016) reported that anonymous cyber-hackers breached a South African portal that hosts jobs for locals and the accessed personal information of 33 000 job seekers.

These cyber-attacks are committed by an online activist group that call itself Operation Africa (Amir, 2016). This group opposes corruption, injustice, child abuse and child labour and targets ICT infrastructures in African governments such as Ethiopia, Sudan, South Sudan, South Africa, Tanzania, Rwanda, Uganda, and Zimbabwe as they believe these countries are guilty of these activities. Van Heerden (2016) reports that the cybercriminal gang that made off with R300 million from Standard Bank in Japan, was not a new phenomenon or even the modus-operandi that was used. Standard Bank, Africa's largest bank by assets, confirmed reports that it is South

African banking operations were the victim of a sophisticated, coordinated fraud incident.

According to the bank, the fraud involved the withdrawal of cash using a small number of fictitious cards at various ATMs in Japan. Japan police suspect that a group of more than 100 people extracted the money from ATMs, which were located in Tokyo and 16 prefectures, or about three hours on 15 May 2016. They targeted 1 400 ATMs in convenience stores and made about 14 000 transactions. Van Heerden (2016) believes the cybercrime ring consists of lots of people and could have been done through phishing or any other technique, or through third parties. Tamarkin (2015) states that Internet penetration is showing progressive growth in Africa and around the world.

According to Tamarkin (2015), the International Telecommunication Union indicated that by the end of 2014 there would be about 3 billion Internet users of which two-thirds will be coming from the developing world. Moreover, in Africa, almost 20% of the population will have Internet access by the end of 2014, up from 10% in 2010. Much of this growth has been fuelled by a dramatic increase in the use of mobile technology, particularly in Africa. Tamarkin (2015) conclude that African states that fail to adequately address the evolving cybercrime problem will consequently limit their economic growth as well as compromise national security.

2.16 INFORMATION GOVERNANCE

Information governance (IG), is the set of multi-disciplinary structures, policies, procedures, processes, and controls implemented to manage information at an enterprise level, supporting an enterprise's immediate and future regulatory, legal, risk, environmental and operational requirements (Ledergerber & Knouff, 2012). Furthermore, IG provides enterprises and individuals with the assurance that personal information is managed legally, securely, efficiently, and effectively, to provide the best possible care. Moreover, IG enables enterprises to put in place procedures and processes for their corporate information that support the efficient location and retrieval of corporate records where and when needed, to meet requests for information and assist compliance with Corporate Governance standards.

MacLennan (2014) states that that the objective of IG is to provide a governance control framework for an enterprise's information, based on its business value and associated risk. Moreover, if IG is applied appropriately, it can provide a mechanism to generate fast, high-quality information to assist leaders in making strategic business decisions. In addition, it can provide customers, regulators, and auditors with an overview of how the data has been collected, managed, transferred, stored and/or destroyed. Smallwood (2014) states that IG is a super discipline that has emerged because of new, tightened legislation that governs businesses against external cyber threats such as hacking, data breaches and cyber-attacks on the information.

However, IG was designed in recognition that multiple overlapping business disciplines were needed to address the current information management challenges in an increasingly regulated and litigated business environment. Furthermore, IG is a subset of Corporate Governance, and include key concepts from records management, content management, ICT and data governance, information security, data privacy, risk management, litigation readiness, regulatory compliance, long-term digital preservation, and even business intelligence. This also means that IG includes related technology and discipline subcategories, such as document management, enterprise search, knowledge management and business continuity, and disaster recovery (Smallwood, 2014).

Blair (2015) states that IG is a new approach to managing information. It builds upon and adapts disciplines like records management and retention, archiving, business analytics, and ICT governance to create an integrated model for harnessing and controlling enterprise information. The ultimate purpose of IG is to help enterprises maximise the value of information while minimising its risks and costs.

2.16.1 Security

Information security defines the level of information protection of an enterprise's assets, and the security controls that are defined and applied, to achieve a desired level of confidentiality, integrity, and availability of information assets (Buecker, Amado, Druker, Lorenz, Muehlenbrock & Tan, 2010). Wechsler (2015) supports this view by stating that most governments start their national-security strategies by describing the importance of "securing information" implementing "computer security" or articulating the need for “information assurance”. These terms are often used interchangeably and contain common-core tenets of protecting and preserving the confidentiality, integrity, and availability of information.

Information security (IS) focuses on data regardless of the form the data may take, either electronic, print or other forms, whilst Computer Security usually seeks to ensure the availability and correct operation of a computer system without concern for the information stored or processed by the computer. Information assurance is a superset of information security and deals with the underlying principles of assessing what information should be protected. Effectively, all three terms are often used interchangeably, even if they address slightly different viewpoints (confidentiality, integrity and availability). Most unauthorised actions that affect any of the three core tenets or information security attributes are considered a crime in most countries (Buecker *et al.,* 2010).

2.16.2 Compliance

According to Buecker *et al.* (2010), security control measures are usually defined in a security policy framework, whilst information security governance (ISG) compliance is understood as the process that protects the operations of an enterprise to meet the requirements that are defined in the Information Management security policies, which consolidate legal and regulatory obligations and management direction. Moreover, information security compliance management requires the ability to identify compliance criteria and to assess, analyse, consolidate, and report on the previous, current, and expectable compliance status of security controls.

Shostack (2014) supports this view, but with caution states that information security (IS) is a pervasive business requirement and that enterprises cannot get it wrong. However, if it is not managed properly, an enterprise could suffer on several levels, including loss of revenue, criminal liability, reputational damage, as well as customer dissatisfaction. Moreover, while most enterprises appreciate the importance of ensuring that information is treated with confidentiality, integrity, and prescribed availability, it must be stated that information security governance (ISG) and compliance is one of the most challenging disciplines to understand, implement and maintain.

2.16.3 Information management security policies

According to Wechsler (2015), volumes have been written about securing information resources, whilst many enterprises do not have effective data-security policies. However, the way to achieve effective data security is to have an effective security policy, and more specifically, an effective security policy that is tailored for an enterprise's data protection challenges. Korzeniowski (2016) states that an information security policy covers more than just technical infrastructure and that every enterprise’s information security strategy is to protect its information from unauthorised access. Therefore, according to Korzeniowski (2016), an IM security policy should include employees that need to be educated on how to protect the enterprise’s information assets.

It is therefore necessary, according to Korzeniowski (2016), that employees fully understand and is familiar with the enterprises’ IM security policy. Johnson (2015) defines information security (IS) “as the act to protect information and the ICT systems that store and process it”. Moreover, this protection is necessary against the risk that would lead to unauthorised access, usage, disclosure, disruption, modification, or destruction of information. Johnson (2015) states that information needs to be protected and a well-structured information management (IM) security policy will ensure the protection of information in any location and in any form. IM security policies should cover every threat of the ICT system and include the protection of people, information, and physical assets (Johnson, 2015).

Chapple (2016) states that policies must set rules for users, define consequences of violations, and minimise risk to the enterprise. However, enforcement will depend on the clarity of roles and responsibilities defined in the policies. Chapple (2016) further states that enterprises need to hold people accountable for adherence to policies, because if it is unclear and identify who is accountable, then a policy becomes unenforceable. It is important to implement an enterprise Group IM security policy as this can reduce the time and effort an enterprise’s technical support staff spends in resolving security-related issues (Chapple, 2016).

2.17 INFORMATION AND COMMUNICATIONS TECHNOLOGY SECURITY

Information and Communications Technology (ICT) has become a central part of modern life (Hughes, 2015). Moreover, it has transformed the way that information is shared, accessed, distributed and the way society communicates using social media. ICT is the overarching term that includes any communication device or application, encompassing radio, television, mobiles devices, computer and network hardware and software, satellite systems, videoconferencing, and distance learning (Hughes, 2015). ICT is a composite term, which represents three important concepts, that needs to be explained, to have a better understanding (Kalloniatis, 2012). Rouse (2016) breaks down and describes ICT as follows:

- *Information*: This can mean many things to many people, depending on the context. When scientifically defined, information is processed data, which aids decision-making. Furthermore, information is any useful fact, quantity or value that can be expressed uniquely with accuracy.

- *Communication*: Refers to the transfer or exchange of digital information using technology. Communication is a technical system that transmits information or data from one place to another or from one person to another. Society use communication technology tools like phones, computers, electronic mail, fax, text-messaging tools etc. to stay in touch with friends and family. Businesses use communication technology tools to facilitate the flow of information in a workplace, assist businesses with strategic decision making and serve the communication needs and requests of the enterprise.

- *Technology:* Technology is the application of science to solve problems. Moreover, technology and science are different subjects, however, it complements each other to accomplish a specific task or solve a particular problem. Technology is dynamic, as it constantly evolves according to the needs and demands of society and businesses. Moskowitz (2014) states that the world has moved from the industrial revolution to the information age.

> Moreover, during the industrial age, enterprises with large sums of capital had the funds to acquire expensive technological tools to gain a competitive advantage, whilst small businesses had less potential because they could not afford expensive manufacturing or processing technological tools. Furthermore, the advancement in technology benefitted small businesses to gain a position in highly competitive markets.

After the Industrial Revolution and with the start of the Information Age, the development and proliferation of electronically communicated information accelerated economic and social changes across all areas of human activity worldwide (Morley, 2015). According to Morley (2015), the information age meant that ICT became one of the driving forces of globalisation with unprecedented opportunities for enterprises to survive in the new global economy. Rouse (2016) defines ICT as "an umbrella term that includes any communication device or software application, encompassing: radio, television, cellular phones, computer and network hardware and software, satellite systems, videoconferencing, etc".

Wechsler (2015) states that ICT is similar to Information Technology (IT), but focuses primarily on communication technologies, which includes the Internet, wireless networks, cellular phones, and other technical communication mediums. According to Riley (2016), ICTs are constantly evolving, and it is difficult to stay abreast with the momentum of digital technology. A good way to think about ICT is to consider all the benefits of digital technology that help individuals, businesses and enterprises that use information (Riley, 2016). Bourgeois (2014) states that ICT is concerned with the storage, retrieval, manipulation, transmission, or receipt of digital data. Furthermore, in the last few decades, ICT has provided society and businesses with a vast array of new communication and technology capabilities.

For example, people can communicate with each other in real-time and in different countries using technologies such as instant messaging, video-conferencing and social networking websites. Rouse (2016) states that the European Commission is concerned with the inability of ICT to create greater access to information and communication in less-developed countries to benefit those communities. Many developed countries have well-established enterprises for the promotion of ICTs, which exacerbate the economic gap between technologically developed countries and less-developed countries. Lichem (2016) states that the United Nations have a key role to play by helping to overcome and bridge the digital divide which is facing humankind.

The importance of open, accessible, and relevant communications for fostering national development, social fulfilment, and human dignity, is undeniable (Lichem, 2016). Moreover, the more communicated a society is, the more opportunities it will generate. However, according to Lichem (2016), the key to the contemporary equation lies in widespread digital connectivity, which means upgrading information and communication technologies (ICTs) in the developing world to the level already enjoyed by most developed countries. Jardine (2015) states, the real meaning of bridging the digital divide is not just an issue of resources and technologies, nor of computer hardware and software. However, it is a matter of wise priorities, good policies, intelligent leadership, transparent decision, and population involvement. However, there are challenges, which are immense, and final success depends on a variety of actors and factors, which include national and local governments, public enterprises and private enterprises, technical improvements, as well as political will and freedom.

2.18 INFORMATION MANAGEMENT

Information is data that has been processed and interpreted to be meaningful (Ogiela & Ogiela, 2014). Moreover, we live in an information age as pointed out by Ogiela and Ogiela (2014) which essentially means that huge resources are applied to the technology, that stores and transmit digital information. Baan (2013) states that Information Management should be viewed as a conscious process by which information is collected and then used to aid in strategic business decision making at all levels within an enterprise. Furthermore, information management is as much about paper-based systems or even human voice-based systems, as it is about technology-based systems.

However, Baan (2013) states that technology provides an important supporting role in good information management and should be viewed as the infrastructure that supports information management, rather than the complete answer to information management. Baan (2013) further states that enterprises that use technology to help deliver information management should involve employees to interact with information, rather than how they interact with technology. Kumar (2013) advocates an integrated approach of all stakeholders to manage an enterprise's information. Kumar (2013) strongly believes in the aspect of inclusiveness and states that Information Management and Information Technology are supporting elements in business, functional and production planning.

Information management should not be undertaken in isolation, as an enterprise needs to have a high level of information management competence if it is to be successful. McWay and Rhia (2014) state that the aim to manage information is to ensure that information that has been identified as being useful to the enterprise can be accessed at the right time, in the right place, in the right formats and by the right people. Aspects to be considered in this context are (McWay & Rhia, 2014):

- *Right time (availability):* When is information available and how soon after creation should the information be made available? Do employees have the correct access properties to information to help them with their decision-making process and is the information available "just-in-time"?

- *Right place:* How well is the information stored and is it accessible in repositories? Is the information stored in hard copy and/or in electronic repositories?

- *Right format:* How do employees prefer to receive information? In hard copy, or electronic format? Is the information up to date and does the enterprise have an information-archiving policy?

- *Right people:* Do the employees have the right skills to be able to use the information effectively? Which employee roles are particularly information intensive? What information security issues must be considered for all employees, to be given access to the information?

McWay and Rhia (2014) state that enterprises must ensure that all business information is safe, regardless of the format. Furthermore, employees should have the tools to access information efficiently and in meaningful formats. Information management involves and requires a clear understanding, at appropriate levels of the enterprise, whilst ICT are tools are used to facilitate information management (Franks, 2013). Significant technological breakthroughs have increased accessibility to new channels of communication, sometimes so much that an enterprise can be said to be “drowning in information” (Franks, 2013). Moreover, the concern and negativity around information lie in the fact that it is “soft” and therefore not easy to manage.

Franks (2013) concludes by stating that at the heart of a good information management (IM) strategy is the need to treat information as an asset and to manage it just like other assets. Singer and Friedman (2014) state, that good information management (IM) is essential for ICT governance, which forms a cornerstone in corporate governance. An integral part of the ICT governance is underpinned by information security governance (ISG), and in particular pertaining to the sensitive and personal information of an enterprise (Singer & Friedman, 2014). Goodrich and Tamassia (2014) state that compliance assurance seeks to validate that the enterprise has implemented adequate security controls to satisfy the many government regulations and auditing regulatory standards.

Klimburg (2013) states that information stored on computers needs to be protected and secured, to protect the integrity and reliability of this information, whilst from a legal perspective; enterprises need to avoid being sued by internal or external parties.

2.19 ICT GOVERNANCE

Good governance requires some form of regulation, but as Ribiere and Worasinchai (2013) advise that information regulation has problems that explains the importance of professional behaviour in ICT. Furthermore, corporate governance has been noted as having come to the fore after some spectacular corporate collapses, while corporate ICT governance is concerned with the role of ICT within the corporation. Weckert and Lucas (2013) state that corporate governance of ICT is the system by which the current and future use of ICT is directed and controlled. Furthermore, corporate governance directs the plans for the use of ICT to support the enterprise and monitor the process to achieve its business objectives.

Ribiere and Worasinchai (2013) define ICT governance as a subset of the discipline that is referred to as corporate governance but is focused on information and ICT assets. Weckert and Lucas (2013) define ICT governance as a collection of principles and practices that guide the correct application and delivery of ICT services. ICT governance provides strategic direction for the use of technology in enterprises (Pande & Van der Wiede, 2012). The overall objective of the ICT governance and control processes is to establish a complete set of managerial and technical control behaviour that will ensure reliable monitoring and control of ICT operations (Kohnke, Shoemaker & Sigler, 2016).

Moreover, Kohnke *et al.* (2016) believe that ICT governance is a strategic governance issue, rather than a technical concern. With the exponential growth of security breaches, the effective use of ICT governance and enterprise-wide frameworks to guide the implementation of integrated security controls is critical in order to mitigate data theft (Kohnke *et al.,* 2016). ICT security can not continue to be seen as a technical issue, according to Mellado (2013), but it is a process that involves the entire enterprise. Furthermore, it is largely

been accepted that ICT security needs to be recognised and reach governance level, so that senior corporate executives and the executive board of directors understand the cyber risks and have the confidence and assurance that these risks are being properly and continuously managed.

Mellado (2013) further states that ICT governance need the support of an enterprise's leadership, structures and processes to ensure that the enterprise's ICT have a sustainable solution that extends the enterprise's strategies and objectives. ICT governance forms part of corporate governance and it cannot be considered as an isolation discipline, but in coordination with other governance structures (Brown & Marsden, 2013). Furthermore, it is linked to other enterprises' key assets, like financial, human or physical, so that it is included in the same decision-making processes.

Brown and Marsden (2013) further state that ICT governance is the strategic business alignment, so that maximum business value and security is achieved through the development, maintenance and support of effective ICT control, accountability, performance and risk management. ICT has become an essential element of every business, and according to Baum and Mahizhnan (2014), it has shown the potential of offering new opportunities to obtain competitive advantages and increase productivity. It is therefore according to Baum and Mahizhnan (2014) of paramount importance to have an effective governance structure of ICT in place, to achieve enterprise goals.

2.19.1 South African governance principles

Enterprises are aware of these requirements and obligations, hence the reason for the development of the King III Report on Corporate Governance which became effective in South Africa in March 2010 (Michalson, 2010). Moreover, the King III Report was designed amongst other controls to make enterprises aware that the guidelines in the King III Report may a guiding principle to highlight security controls, to protect its information assets and their enterprises. Michalson (2010) further states that the principle on which the King III Report has been written is in accordance with "comply or explain". Michalson (2010) further states that the evolution of the South African Information Security Law, is essentially an emerging area of the law that governs all of an enterprise's information-security obligations.

The three areas of the South African Information Security Law, which is the, King III Report on Corporate Governance for South Africa, the Electronic Communication and Transactions (ECT) Act (Act 25 of 2002), and the Protection of Personal Information (POPI) Act (Act 4 of 2013). These three guidelines for South African enterprises and consumers are defined as follows:

- *King III Report on Corporate Governance* recommends that the executive board of directors should ensure that information resources of an enterprise is managed in a controlled manner, that includes the protection of information in the Information Security (IS) sections of the Report.

- *Electronic Communication and Transactions (ECT) Act (Act 25 of 2002)* provided a control framework for the security public key infrastructure (PKI); recommended and imbedded the need for consistent software electronic signatures; provided the security to transact online and highlighted and identified several cybercrimes to be subscribed into the law of South African.

- *Protection of Personal Information (POPI) Act (Act 4 of 2013)* presented and provided appropriate and reasonable technical direction to South African enterprises on how to manage security protection measures of personal information.

2.19.2 King III Report on ICT governance

According to Deegan (2016), the King III Report was released on 1 September 2009, which came into effect on 1 March 2010. Furthermore, the King III Report represents a significant momentous achievement in the evolution of corporate governance in South Africa and gave rise to significant opportunities for enterprises that embrace its principles. The King III Report became a guiding principle for South Africa based on the anticipated trends in international governance. Rizzo (2016) states that Information Technology (IT) in the King III report articulate the role and responsibilities of the executive board of directors in support of IT governance.

Furthermore, the recommendation of the King III Report is extensive and would require additional resources, management, and time with directors to address and manage IT governance and the related procedures and practices. The risk committee should ensure that IT risks are adequately addressed and mitigated to ensure appropriate assurance on controls. The audit committee should consider IT in relation to financial reporting and the going concern. Rizzo (2016) concludes by stating that the King III Report is an aspiring governance report, which with good intention would take enterprises in South Africa an extended period to formalise and achieve the recommended governance control processes and best-practice principles. Enterprises need to be mindful that the application of the recommendations would require them to balance the implementation cost and the benefits that will be realised and be meaningful to all stakeholders.

2.19.3 International governance principles

The United States of America formalised a major part of the country's ICT governance in an Act, known as the Sarbanes-Oxley Act (SOX) (Maleske, 2012). However, this is a statutory rule known as "comply or else", which has legal implications for non-compliance. Roman (2014) states that policy guidelines, standards operating procedures, government legislations and industry best practices, such as the King III Report on Corporate Governance and Sarbanes-Oxley (SOX), have been designed to assist enterprises to have a clear understanding of their governance responsibilities among executive board members, businesses, and Information Management (IM) managers.

These guidelines, standards and governance processes have been formalised by government statutory committees to support enterprises in complying with the laws or governance standards (Roman, 2014). National cybersecurity is a critical and strategic component of information security, whilst Klimburg (2012) points out that the national cybersecurity governance processes should play a crucial role in deterring cyber-crime. This strategy informs that appropriate governance legislation must be adopted to guard against the abuse of ICT environment security procedures for the benefit of cybercriminal activities with the aim to disrupt the integrity of critical national ICT infrastructures (Klimburg, 2012).

This activity according to Klimburg (2012) is a shared responsibility by all security stakeholders (Government, corporates, and citizens) which require a collaborative effort to prevent, prepare, respond, and recover an ICT environment. Moreover, to formulate and implement a national cyber security framework requires a comprehensive approach (Roman, 2014). Thus, according to Roman (2014) to develop and supporting a national cybersecurity strategy forms a vital component in the fight against cybercrime.

2.20 RISK MANAGEMENT OF INFORMATION

A generic definition of risk management is "the assessment and mitigation of potential risks that are a threat to a business, whatever their source or origin" (Mackey, 2011).

Moreover, in order to discuss the risk of managing information, it is necessary to explain the meaning of the three main risk management concepts, namely: risk has the potential that can lead to an undesirable outcome of loss of a chosen activity; whilst a threat has the potential to cause an undesirable impact on a system; which can further be defined as an undesirable event that may cause harm to the information of an enterprise.

Moreover, vulnerability is described as a weakness in system procedures, information security, internal controls and other weaknesses that can be exploited to bypass security and unauthorised access to information. It can thus be stated, according to Mackey (2011), that vulnerability signifies any weakness, act or statement that has the capability to exploit the information about an asset by a threat. However, risk management of information is a process consisting of identifying vulnerabilities and threats to the information resources used by an enterprise. Kouns and Minoli (2010) concur by stating that Information Technology Risk Management (ITRM) is concerned about the possibility of compromise and/or the potential loss of classified information, which have reached critical levels in many enterprises over the last few years.

Moreover, cyber-attacks continue to be a source of significant concern to enterprises of all types, and therefore, potential damage and/or potential incapacitation of information assets have become fundamental business continuity issues. Furthermore, a vulnerability or weakness is a lack of security, which may be exploited by a cyber threat, causing harm to the information systems, which can be a computer software flaw that permits exogenous agents to use a computer system without authorisation. Kouns and Minoli (2010) further state that there is a definite need to protect the enterprise from random, malicious, or planned cyber-attacks on its ICT assets.

Moreover, it is critical, therefore, for enterprises to develop ready-to-go technological and human resources within the enterprise to manage vulnerabilities and events that are likely to affect the enterprise. Stroie and Rusu (2011) recommend that enterprises establish risk management or risk assessment teams that will evaluate and identify potential risks that could ensue from vulnerable events by ensuring that risk mitigation solutions are in place. Cybersecurity threats are a constant and evolving risk to an enterprise’s ability to ensure its strategic objectives deliver core business functions. In fact, failing to secure information can result in significant long-term financial loss to the affected enterprise, and substantial loss in confidence and consumer trust in the reputation of a brand.

Stroie and Rusu (2011) further state that cybersecurity should move from being in the ambit of the ICT professionals to that of the Executive and Board of the enterprise, where its consideration and mitigation can be commensurate with the risk posed. It is clear from the statement of Stroie and Rusu (2011) that the traditional approach to cybersecurity which is to build walls (firewalls and antivirus software), while still necessary, is no longer sufficient.

Stroie and Rusu (2011) recommend that a holistic cybersecurity risk management approach across the enterprise, its ICT environment, and the wider business environment is required. Kouns and Minoli (2010) state that risk management for information systems is a process, which essentially means it is a series of coordinated activities that should not be seen as a once-off activity, but instead, enterprise risks must be monitored, reviewed, and treated continually. The process requires several inputs to analyse risks to generate a risk-treatment and management plan as output. However, to mitigate the identified information risks, Khosrow-Pour (2015) states that enterprises are presented with a practical challenge on how to manage and run an efficient and effective information security programme.

Moreover, consistently is required to identify high-level protection, and in turn, how to identify risk events, assesses the risk and mitigate or manage the ICT environment to reduce risk events. Moreover, information security risk management is the process of reducing risk, which should be a process that is well defined, and repeatable sequences of activities of which Khosrow-Pour (2015) recommend that five processes should be followed to mitigate information security risk. The processes identified by Khosrow-Pour (2015) include, but is not limited to:

- The ongoing identification of threats, vulnerabilities, or risk events, which affect the set of ICT assets owned by the enterprise. Furthermore, risk mitigation involves identifying risk mitigation options, then choosing an identified risk option to implement. The team designated to manage the risk need to work collaboratively with the relevant individuals to make appropriate recommendations to leadership.

- *The assessment or analysis of risks* – risk assessment, often called risk analysis is a critical step at the beginning of an information security project as it sets the foundation for information security in an enterprise. However, the importance of each risk needs to be assessed so that the most appropriate ways could be implemented to avoid security incidents.

- *Plan on how to mitigate the risk findings* – risk mitigation involves taking the necessary precautions to eliminate or reduce the probability of compromising the confidentiality and integrity of valuable classified information to an acceptable level.

- *Implement the risk mitigation plan* – there are essentially three steps to a risk mitigation plan, namely, identify the risk, choose to accept the risk if it is low and implement risk-mitigating options.

- *Accept the risk* – an enterprise may choose to simply accept the risk if the risk is considered low. Should the cost be high to accept the risk, or higher than transferring or limiting it, then the enterprise may choose not to accept the risk. The enterprise should then review an option to transfer or limit the risk.

- *Transfer the risk* – when the risk is transferred, it is shared with a third party, part or the entire risk. This is essentially regarded as the use of insurance. Third parties provide insurance for enterprises, by agreeing for the risk to be transferred. The insurer will then compensate the information owner is full for damage of a particular risk. In some cases, the option of transferring the risk may not be possible or the liability of the risk may be too high to ensure.

- *Limit the risk* – when a risk of a particular asset is high, and cannot be transferred, then the risk should be limited in part or in full. The process involves the identification of possible threats to a certain asset, identifying, researching, or designing an acceptable control measure to mitigate the threat. To limit risks, such as a virus outbreak, spam and/or unauthorised access, the enterprise may decide to purchase antivirus software to potentially reduce the impact of these risks.

Risk limiting involves the control of access to an enterprise’s ICT environment, by installing tools such as antivirus or anti-spam software, including a firewall to manage unauthorised access. It is essential to educate employees to be mindful of information security as this will also help to reduce risk. Suppliers of Information computer systems or software would provide free software security patch updates and, in most instances, provide software tools to perform automatic security patch updates to these systems.

- *Avoid the risk* – It is difficult to provide a universal answer to confirm if it is possible to avoid risk because every risk situation is different. Risk avoidance is typically in place to protect critical business assets. Some examples of risk avoidance include to initiating a system backup of information or disconnecting critical computers from the Internet to operate in isolation.
- *Evaluate the mitigations* – implementing the risk-mitigating plan involves deploying the risk plan that has been chosen. As previously defined, the possible plan includes to accepting, transferring, limiting, or avoiding the risk. This essentially means that each information asset will have a risk plan assigned to it to mitigate the potential risk. Implementing the chosen plan, will involve certain procedures and/or new controls to be followed. Thus, limiting the risk by adopting control measures is the most used scenario to protect critical information systems.

To continually evaluate and manage the implemented risk mitigation plan, will involve continual monitoring to ensure the level of risk is kept to a minimum. Moreover, to achieve a business continuity strategy and ensure information security protection against malicious cyber-attacks, the enterprise must have a clear top-down understanding of its ICT supported business operations (Khosrow-Pour, 2015). Furthermore, a clear fundamental and comprehensive understanding of the risk must be in place to manage and have a strong risk mitigation plan in place.

2.20.1 Information Security

The view of Humphreys (2013), who regards an Information Security Framework (ISF) as a framework that ensures compliance to an Information Security Management System (ISMS) standard, is an effective way to manage IT within an enterprise. Moreover, unfortunately, ISMS is not an easy standard to implement and is generally complex, however, this standard will ensure governance compliance. Humphreys (2013) further states that it is extremely important to comply with an ISMS standard and recommends that enterprises adopt a framework to adopt standards gradually to avoid failing with the implementation of an ISMS standardisation project.

Granneman (2013) defines an ISF as “a series of documented and accepted processes that are used to define policies and procedures with the implementation, and on-going support and management of information security control processes in an enterprise’s ICT environment”. Furthermore, these frameworks are essentially a “blueprint” for designing an information security programme to manage risk and reduce security vulnerabilities. Granneman (2013) recommends that ICT security professionals could use these formalised frameworks to design and prioritise the activities required to build ICT security solutions in an enterprise.

However, information security has a critical role to play in supporting the enablement of ICT activities of the enterprise, whilst a key component to help understand the process and technical competent features of ISMS, such as ISO 27001, is to use a framework to deploy the components of ISO 27001 in a phased approach. Moreover, frameworks are often customised to guide and help resolve specific IS-problems (Granneman, 2013). The International Organisation for Standardisation (ISO), in ISO 2015 and ISO 27000 as a family of standards, help ensure that information assets are secured, whilst these standards guide enterprises on how to manage the security of these standards.

ISO 27000 is regarded as the most popular standard of the ISO family for Information Systems in that it provides system governance requirements. (Granneman, 2013). Humphreys (2013) states that cyber-threats present a constant cyber security threat that affects global governments and enterprise, whilst the proliferation of these threats are on the rise as cybercriminals focus on improving their skills. Moreover, this problem requires an international solution in the form of ISO 27001, as it will provide a management framework to assess cyber risks. Humphreys (2013) recommends that enterprises conduct an information security assessment to comply with an ISMS standard such as ISO 27001.

Mackey (2011) states that risk assessment frameworks establish the meaning of terms so that it is widely understood. In 2014, the National Institute of Standards and Technology (NIST) introduced a framework for Improving Critical Infrastructure for enterprises that offer a standardised framework to manage cybersecurity activities and reduce cyber risk (Coraggio, Rogers & Hilgeman, 2014). Moreover, the National Institute of Standards and Technology (NIST) in the United States provides best practices documentation by gathering an extensive list of information security standards. The NIST security framework reference to improve critical infrastructure in cybersecurity is referred to as a security policy of the United States (Metivier, 2016).

Furthermore, this policy was designed to enhance and improve the cyber security governance and resilience of the country's critical ICT infrastructures. Coraggio *et al.* (2014) state that as part of the profile development process, enterprises should determine the optimal method for assessing their environments. Guinn (2014) states that the NIST framework target those enterprises that operate critical in-house ICT infrastructure; adoption of this framework may prove to advantage businesses across all industries. The NIST framework comprises a risk-based consolidation of guidelines and standards that could help enterprises improve cybersecurity when implemented.

The benefits and importance of a cybersecurity framework are well worth adopting for enterprises in various industries, which will help in improving cyber risk-based security. Greene (2014) states that the guiding principles of a cybersecurity framework are collaboration to share information and improve cybersecurity practices and threat intelligence. The best security minds in the world have contributed to researching, evaluating, and publishing security frameworks (Greene, 2014). An IS framework as stated by Greene (2014), is a collective term given to guide topics that are related to information systems security and governance, predominantly regarding the implementation planning, managing risk and auditing of overall information security practices.

Moreover, Greene (2014) states that the two most widely used frameworks globally are the Information Security Framework (ISF) and National Institute of Standards and Technology (NIST), created in the United States and the Information-Security Management System offered by the ISO. When these governance frameworks coexist, an enterprise can create an extensive and comprehensive information security programme. It can be stated, according to Greene (2014), that of the various risk-assessment frameworks, the focus area is to achieve the objective. It can further be stated that when evaluating the various risk frameworks, it can thus be concluded that frameworks follow similar structures but differ in the description and details of the steps.

However, they all follow the general pattern of identifying assets and stakeholders, understanding security requirements, enumerating threats, identifying, and assessing the effectiveness of controls, and calculating the risk based on the inherent risk of compromise and the likelihood that the threat will be realised.

2.20.2 Risk assessment

A risk assessment can be quantitative or qualitative (Rausand, 2014). Quantitative risk assessment assigns numerical values to the probability that an event will occur and the resulting impact. Furthermore, these numerical values can then be used to calculate an event’s risk factor, which in turn can be mapped to monetary amounts. However, qualitative risk assessments are used more often and do not involve numerical probabilities or predictions of loss. The goal of a qualitative approach is simply to rank which risk poses the most danger (Rausand, 2014). Talabis and Martin (2013) state that risk assessment is all about identifying the threats that are out there, and then determining if those threats pose a real risk to the enterprise. Greene (2014) presents the following methodology, which is the baseline of various information security framework models:

- *Identify assets and stakeholders*
  All risk assessment procedures require a risk assessment team to clearly define the scope, the business owner, and the ICT security professionals of the information asset and in particular the security controls for the asset. The

information asset defines the scope of the assessment, whilst the owners and security professionals define the members of the risk assessment team. This step defines the boundaries and contents of the asset that needs to be assessed.

- *Analyse impact*

  Understand the business impact to the enterprise, assuming the asset was compromised. The impact of the dimensions and magnitude is essential to understand, as the dimensions of compromise are confidentiality, integrity and availability, while the magnitude is typically described as low, medium or high, which corresponds to the financial impact of the compromise.

  The exercise of analysing the value or impact of asset loss can help determine which assets should undergo risk assessment. The output of this step describes the business impact in monetary terms or more often, a graded scale for compromise of the confidentiality, integrity, and availability of the asset.

- *Identify threats*

  Identify the many ways in which an asset could be compromised that would have an impact on the enterprise. Threats involve the exploitation of weaknesses or vulnerabilities intentionally or even unintentionally, that results in compromising information security. This identification process typically starts at a high level, to review general areas of concern and then progress to a more detailed analysis.

  The intent to analyse is to list the most common combinations of perpetrators and ways that might lead to the asset being compromised. These combinations are referred to as threat scenarios, and the assessment team will use this list later in the process to determine whether these cyber threats are effectively guarded against by security and information process controls. The output of this step is the list of threats associated with the potential impact of the compromise.

- *Investigate vulnerabilities*

  To investigate vulnerabilities, it is advisable to use a list of threats that have been identified. The vulnerabilities would have been identified during the design or control process reviews. The assessment team would then determine the likelihood that vulnerabilities can be exploited during a test of threat scenario.

- *Analyse controls*

  The team need to review the technical and process controls to protect an asset and determine the effectiveness of the process controls to guard against the identified cyber threats. Technical controls such as access authentication, intrusion detection, network traffic filtering and routing, and data encryption, are reviewed in this phase of the assessment. The risk assessment team consider the types of controls when reviewing the effectiveness of controls. The assessment team documents the controls associated with the asset, and their effectiveness to defend against the identified threats.

- *Calculate threat likelihood*

  After a particular threat has been identified, the team develop scenarios to define how the threat may be activated to determine the effectiveness of controls to prevent exploitation of a vulnerability. The teams use a "logic formula" to determine the likelihood of exploiting a vulnerability.

- *Calculate risk magnitude*

  The calculation of risk magnitude determines the business impact of the asset, whilst taking into consideration the diminishing effect of the threat scenario under consideration. The result indicates how the threat will impact the business.

This measure of risk assessment serves as a guide to businesses to indicate the importance of addressing the vulnerabilities or control weaknesses that allow cyber-threats to be realised (Greene, 2014). Ultimately, according to Greene (2014), the risk assessment forces a business to decide to treat or accept risk. A risk assessment method when viewed for the first time, will probably create the impression that it describes a clean and orderly stepwise process that can be sequentially executed (Greene, 2014). However, the team need to repeatedly return to earlier steps, as it often takes an enterprise several attempts to get used to the idea that circling back to earlier steps is a necessary and important part of the process.

Violino (2010) states that formal risk assessment methodologies try to take the guesswork out of evaluating ICT risks. Assessing and managing risk should be a high priority for many enterprises, especially given the turbulent state of information security vulnerabilities and the need to be compliant with so many regulations, which is a huge challenge (Violino, 2010). Moreover, a security-framework approach includes benefits such as the right security controls for the right risk level, and the security professionals focus on security controls with the highest benefit to reduce the risk of regulatory compliance concerns.

Moreover, an ICT Security Policy Framework is the method for which an enterprise aligns its policies, standards, procedures, and guidelines that are needed to govern the ICT infrastructure. It is this structure or framework that is typically aligned towards risk management or risk mitigation goals and objectives of the enterprise, such that they can maintain compliance and mitigate risk throughout a typical ICT infrastructure. Guinn (2014) states that it is important to note that an information security framework casts the discussion of cybersecurity in the vocabulary of risk management. With good reason, executive leaders and board members typically are well-versed in risk management, and framing cybersecurity in this context will enable security leaders to articulate the importance and goals of cybersecurity more effectively.

It can thus also help enterprises to prioritise and validate investments based on information risk management. It is important to note that there is no one-size-fits-all solution for cybersecurity, and the government cannot provide comprehensive, prescriptive guidelines for all entities across industries. However, while a Framework offers worthwhile standards for improving cybersecurity, it might not fully address several critical areas (Guinn, 2014).

2.21 CHAPTER SUMMARY

Despite the substantial hurdles and shortcomings of the international approach to fight cybercrime, a common instrument will have a stronger position in the global fight against cybercrime. So long as there remains a weak link in the cybersecurity chain, cybercriminals will seek to exploit it. Unless and until there is broad global agreement on criminalising cybercrime and robust international cooperation to enforce those laws, cybercriminals operating in cybercrime safe havens will continue to target individuals, businesses, and governments with impunity. The use of interconnecting technologies is not without risk, and if left unmanaged, these risks could have a damaging effect on the economy and financial position of countries, enterprises, and society.

Information and Communication Technologies (ICTs) play a vital role in the construction of modern, critical computer systems. The component of such systems is dependent on the reliable operation of interconnecting information infrastructures. Should the ICT environment and its associated security control systems be made inoperable, it could have a devastating effect on information services. There is a need, more than ever, to provide seamless privacy protection for data as it flows through the global Internet. To secure information requires a careful reconsideration of the business community's interest in promoting commerce, the government's interest in fostering economic growth and protecting its citizens, and the interest of individuals in protecting themselves from intrusive cybercriminals.

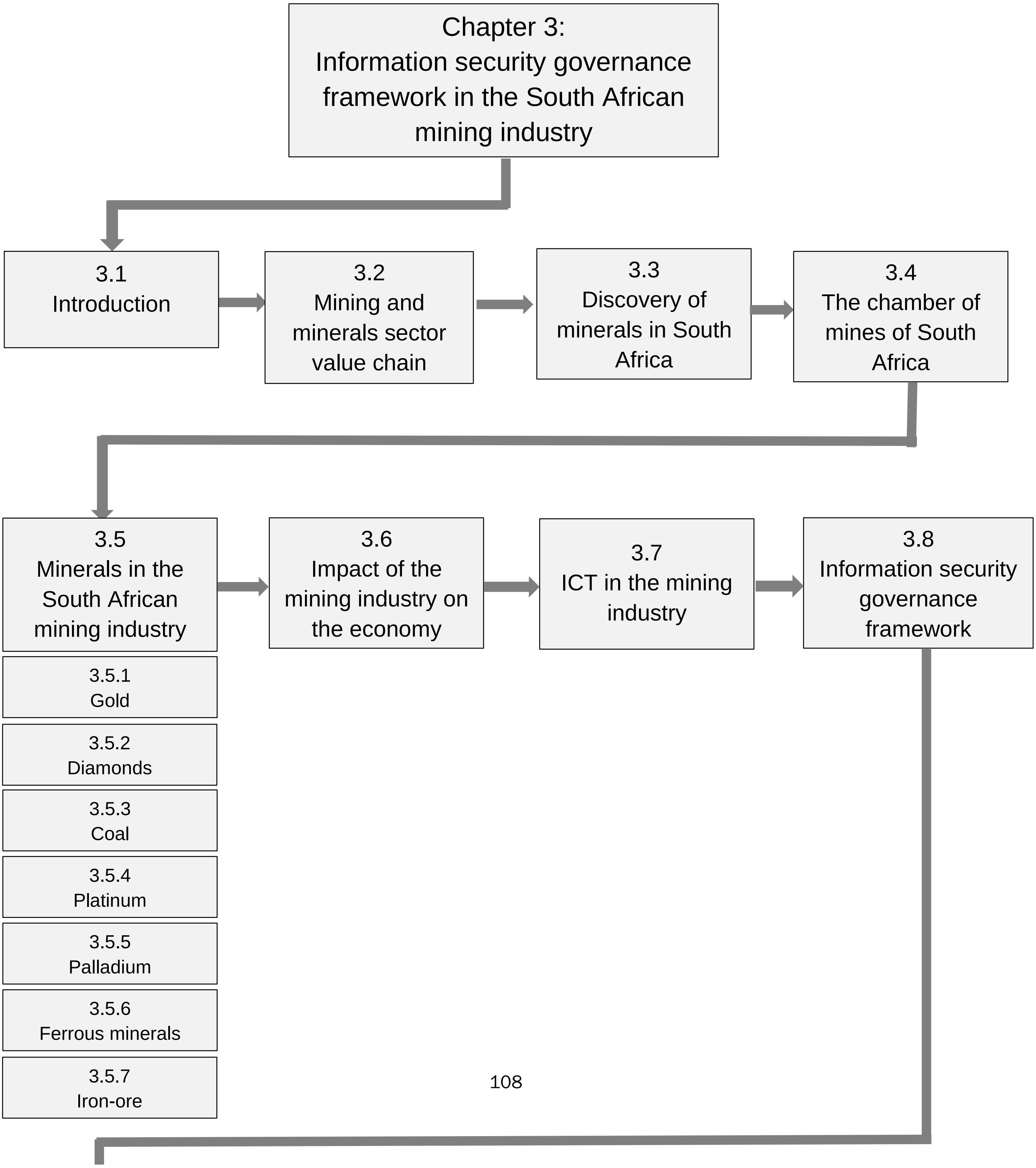
This chapter highlighted the global and South African role of the ICT environment and information security governance in modern society. Various components were discussed, which are used to form a critical base of an ICT environment. Furthermore, the chapter also highlighted the vulnerability of the ICT if not protected sufficiently against cyber-attacks. Cyber-attacks can have a major impact on the functioning of critical ICT environments. This can severely hamper a country's ability to operate effectively. If Africa becomes known as a cybercrime safe harbour, this could have devastating consequences for the continent's potential growth.

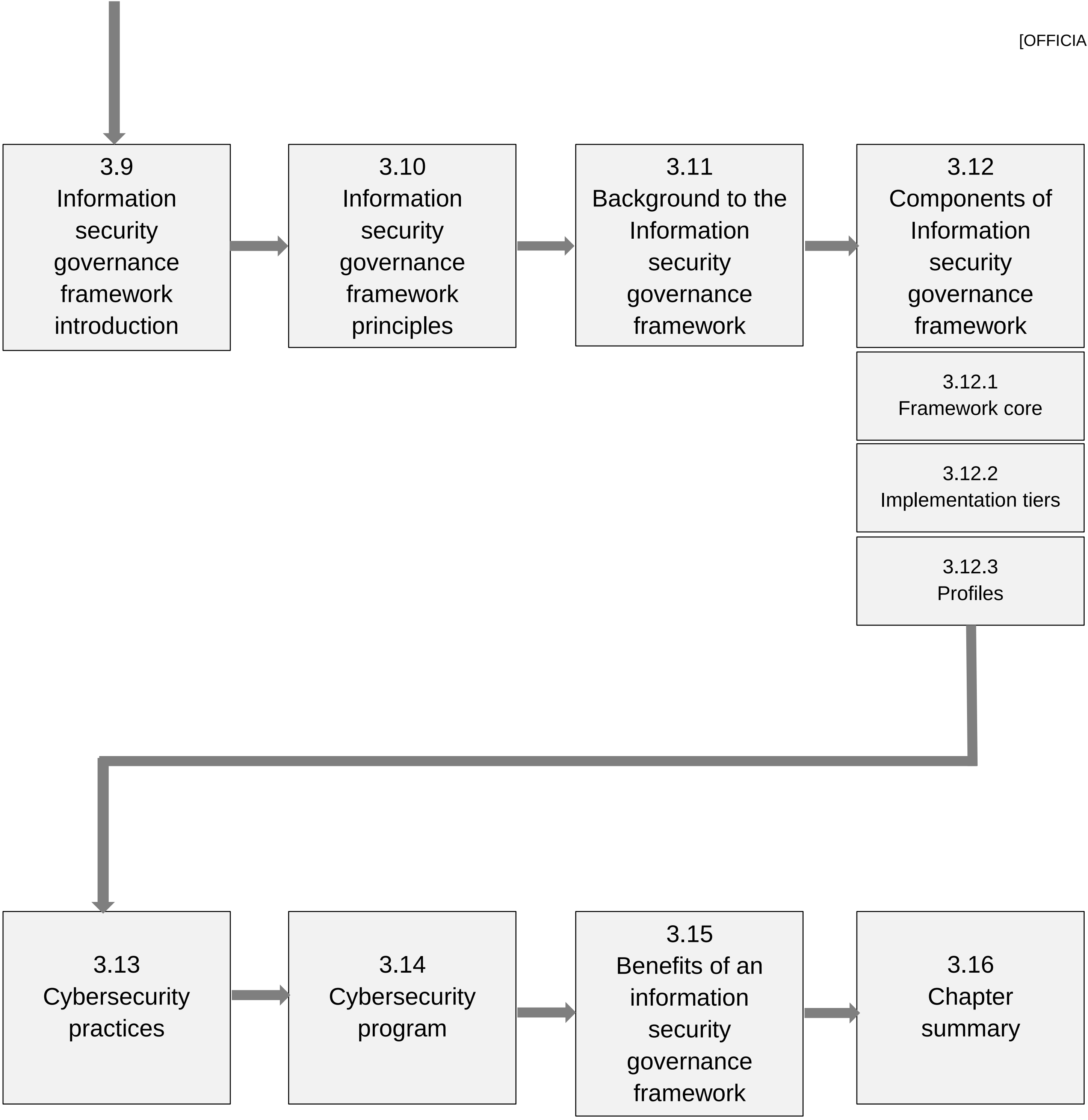
Furthermore, if an African state becomes known as a hospitable environment for cybercriminals, it will not only damage that country but will also have a negative impact on the reputation of the continent. Africa, and especially South Africa should instead focus on improving their cybersecurity and enhancing their capacity and capability to fight cybercrime immediately. Different types of cyber-attacks were also discussed, and the governance of an ICT environment. The Internet as a factor of a cyber-attack was discussed, and the emerging technology of the "Internet of Things", which raises further vulnerabilities in society. The effect of cyber-attacks in developed and developing countries cannot be overlooked, as the impact and consequence of cyber-attacks are different in both scenarios.

The chapter highlighted the importance of policy frameworks in ICT environments. It can thus be concluded that the development of a national cybersecurity structure is of vital importance for all nations, to protect the economies of both developing and developed nations. However, the development of such a structure does not form part of this study. Based on the discussion of cybersecurity and governance in this chapter, the next chapter will discuss the South African mining industry.

CHAPTER 3: INFORMATION SECURITY GOVERNANCE FRAMEWORK IN THE SOUTH AFRICAN MINING INDUSTRY

The South African mining industry has a rich history. This chapter aims to review the history of the mining industry in South Africa. Furthermore, the study reviewed the discovery of minerals in South Africa, the mining industry, and conclude by reviewing information, communication, and technologies in the mining industry of South Africa.


Chapter 3:
Information security governance framework in the South African mining industry
3.1
Introduction
3.2
Mining and minerals sector value chain
3.3
Discovery of minerals in South Africa
3.4
The chamber of mines of South Africa
3.5
Minerals in the South African mining industry
3.5.1
Gold
3.5.2
Diamonds
3.5.3
Coal
3.5.4
Platinum
3.5.5
Palladium
3.5.6
Ferrous minerals
3.5.7
Iron-ore
3.6
Impact of the mining industry on the economy
3.7
ICT in the mining industry
3.8
Information security governance framework


3.9 Information security governance framework introduction
3.10 Information security governance framework principles
3.11 Background to the Information security governance framework
3.12 Components of Information security governance framework
3.12.1 Framework core
3.12.2 Implementation tiers
3.12.3 Profiles
3.13 Cybersecurity practices
3.14 Cybersecurity program
3.15 Benefits of an information security governance framework
3.16 Chapter summary

3.1 INTRODUCTION

The Mineral Revolution in South Africa came to life towards the end of the 19th century when the barren landscape showed little potential of any economic development (Davenport, 2013). However, just beneath the sandy surface of the mineral-rich landscape laid the richest gems of diamonds, coal, gold, platinum, and many other mineral gems that have ever been discovered in a country. This led to the first discovery of diamonds in 1870. Gold was discovered in 1886 and proved to be the great mineral revolution ever experienced in the world (Davenport, 2013). Moreover, the discovery of these rare commodities resulted in South Africa becoming the greatest industrialised nation on the African continent.

Smit (2015) states that South Africa’s economy has been supported by mining for almost 150 years. Furthermore, mining continues to underpin the South African economy and to support the development and growth of the socio and cultural demographics of the country. Moreover, Antin (2013) further states that the mining industry is pivotal in attracting foreign direct investment and remains the most rewarding economic sector in South Africa. The production of a variety of major mineral commodities in South Africa is regarded as the second largest after the United States (De Beer, 2015). Furthermore, there are only two minerals that are not available in South Africa, being crude oil and viable bauxite, which is the primary ore of aluminium. Smit (2015) states that the mineral wealth of South Africa exceeds 65 commodities throughout the country.

3.2 MINING AND MINERALS SECTOR VALUE CHAIN

The Technology Innovation Agency (TIA, 2016), defines the value chain of the mining and minerals industry as the exploration process of minerals, being the first step in mining that encompasses finding a reasonable amount of minerals. The TIA further explains that the mine development phase is initiated to determine if mineral deposits can be extracted economically. This initial phase involves a technical assessment of the mining area, the design of mining plans and mining infrastructure, adherence to all the compulsory regulatory requirements, impact evaluations, the final project evaluation, and finally the building and commissioning of the mine.

The final phase is to construct the mine buildings and processing plants so that the recovery and extraction of the ore can start to extract valuable minerals from the earth (De Beer, 2015). Moreover, after mining begins, the minerals are processed through an extraction and preparation phase before it goes through a separation and purification process (De Beers, 2015). It must be stated as defined by Smit (2015) that mining is an exclusive business operation as it requires at its initiation phase, an approved plan that incorporates the mine closure plans, including the rehabilitation of the environment. The South African mining industry was directly subsidized to the formation of the Johannesburg Stock Exchange in the 19th century and still accounts for a third of its market capitalisation (Jones & Muller, 2013).

3.3 DISCOVERY OF MINERALS IN SOUTH AFRICA

Diamond was first discovered on the banks of the Orange River in 1867 that started the proliferation of the mining industry in South Africa (Beck, 2014). Furthermore, by 1886, the gold and diamond rush started to evolve mining in South Africa into a healthy economy. McCulloch (2012) states that the richest mineral deposits are found beneath the earth in South Africa that has ever been discovered in a confined country. Martin (2018) states that in 1970, the gold sector in South Africa reached its highest level and contributed about 68% of the global production.

Based on current mineral demand, the global targets are indicative of which mineral commodities the world will require in the future, meaning that South African mining will continue to be feasible to grow the economy well into the future (Martin, 2018). South Africa has the minerals and mining industry that the world desires, meaning that as long as there are people and a requirement, the demand for these minerals will continue to grow (Harvey & Press, 2013).

3.4 THE CHAMBER OF MINES OF SOUTH AFRICA

The name of the Chamber of Mines (CM) changed many times in its history, which concur with mining and political changes in South Africa (Baxter, 2016). Furthermore, the history of the CM was formed on 7 December 1887 in a downtown Johannesburg hotel. The Chamber of Mines was officially constituted by its founding members on 5 October 1889 (Baxter, 2016). Harvey and Press (2013) state that the Chamber of Mines (CM), which is a producers’ enterprise, was funded by its members, that represented mine owners, government, and the mining labour. Furthermore, the CM’s key mandate is to protect the assets of the mining industry in South Africa.

Mining in South Africa provides the single most export revenue and employs directly, and indirectly, more people than any other comparable industry (Teffo, 2016). Teffo (2016) further states that the CM represents a sector that contributes more than R18 billion in taxes to South Africa, has a workforce of about 500 000 employees, and contributes about R102 billion in employee earnings. Martin (2013) states that the CM responded well to the ever-changing political and economic environment in which it operates and has redirected many of its key activities to work with the government to redefine major mining policies.

3.5 MINERALS IN THE SOUTH AFRICAN MINING INDUSTRY

3.5.1 Gold

Gold was first discovered in 1870 on a farm called Eersteling, which is about 40km southeast of Polokwane (Weston, 2012). More gold deposits were discovered in 1873 in Pilgrim's Rest and in 1885 in Barberton. This was followed by the discovery of the Kaapschehoop gold field, and in 1883, the Barberton gold field produced more than 340 tons of gold (Weston, 2012). Gold was also discovered on the Highveld in 1875, and in 1881 in Kromdraai, and in 1884 in Wilgespruit which forms part of the Gauteng Province (Coulson, 2011).

Witwatersrand gold mining started on the Central Rand, then the East and West Rand which fall within the boundaries of Gauteng, thus making this province the largest gold producing province in South Africa (Coulson, 2011). According to the Department of Mineral Resources (Baxter, 2016), there are currently 35 gold mines that operate in South Africa, which include the record gold producing mine, TauTona mining at a depth of 3,9 km. South Africa produces about 11% of the total global gold reserves (Baxter, 2016).

3.5.2 Diamonds

Diamonds were discovered in 1866 in the Kimberley area and in 1870 started to transform the South African economy from an agricultural economy to a mining and industrial-based economy (Williams, 2011). The 21¼ carat diamond was discovered in 1866 and named the Eureka diamond. This discovery was followed by the 83½ carat diamond in Cullinan in 1869 and named the “Star of South Africa” which then led to South Africa’s first great rush for mineral wealth (Williams, 2011). The diamond rush resulted in South Africa gaining global dominance in producing diamonds for about 70 years, which meant that it needed technology and specialised mining equipment to establish itself (McKenna, 2011).

However, the global dominance of diamonds also triggered the development and establishment of supporting mining industries locally and globally. Furthermore, Big Hole Museum in Kimberley is testimony to the early days of diamond digging which has become an iconic mine of South Africa and the history of the mine is well appreciated. This “Big Hole” diamond mine in Kimberley was in operation for 43 years, from 1871 to 1924, and produced 14.5 million carats (McKenna, 2011. The “Big Hole” is famous for producing one of the largest diamonds in South Africa, being the 128.53 carat diamond that was later named “Tiffany Yellow” (McKenna, 2011).

McCulloch (2012) states that the successful economy of South Africa is underpinned by the production of gold, platinum, and diamonds, however coal, and iron-ore have a huge influence on the South African economy. South Africa remains the producer of high-quality gem diamonds in the world and is ranked 5th in contributing towards diamonds globally (Williams, 2011).

3.5.3 Coal

Coal was discovered in mid-1850 and the demand to produce large quantities of coal excelled from the 1890s onwards, in order to provide electricity to the power base of South Africa and neighbouring countries (Klotz, 2013). By 1852, there was a demand for bunker coal to supply steamships from what was then known as the Natal Colony (Klotz, 2013). Furthermore, from 1870 onwards, coal was produced from the Molteno coal fields, which is based in the Eastern Cape. Galvin (2016) states that large-scale coal mining started in the Emalahleni area in 1895 which resulted in the area being developed into the most strategically coal-mining region in South Africa. The national energy plan has a demand for coal which essentially means that coal remains a strategic commodity of South Africa’s future energy mix and requirements (Baxter, 2016).

3.5.4 Platinum

Platinum, which is a precious metal has now established itself as the flagship in South Africa’s mining sector. This precious metal was discovered in 1924 and showed significant growth in the early 1970s (Zereini & Wiseman, 2015). Moreover, the surrounding areas in Rustenburg which is situated in the North-West are still actively being mined. Baxter (2016) states that South Africa’s platinum group metals (PGM) reserves account for about 96% of global PGM reserves. Platinum Group Metals (PGM) comprises of platinum, palladium, rhodium, osmium, ruthenium, and iridium, which is mined with nickel and copper (Zereini & Wiseman, 2015). Zereini and Wiseman (2016) state that Rustenburg is regarded as the epicentre of platinum deposits in South Africa.

3.5.5 Palladium

South Africa is regarded as the world’s second-largest palladium producer (Zereini & Wiseman, 2016). All South Africa’s palladium deposits are found in the Bushveld Igneous Complex, which is the largest mining resource for PGM operations in the world (Baxter, 2016). Moreover, palladium, together with platinum, is more abundant than any of the other PGMs.

3.5.6 Ferrous minerals

Baxter (2016) states that South Africa is regarded as the largest producer of chromium and vanadium ores and a leader in supplying alloys. Furthermore, South Africa produces iron and manganese ores in high quantities and lesser quantities of ferrosilicon and silicon metal.

3.5.7 Iron-ore

South Africa’s mining operations of iron-ore are based in the North-West and Northern Cape provinces (Coulson, 2011). Moreover, a state-controlled establishment of iron and steel industry was formed in the 1920s and facilitated the growth of a secondary industry that enabled South Africa to develop into the most industrially self-sufficient country in Africa (Coulson, 2011). Mostert (2012) states that large-scale iron ore mining operations started in Gauteng; the majority of iron ore is currently mined in the Northern Cape and Limpopo Provinces at the iron-ore rich Sishen and Thabazimbi Mines, respectively.

The production of iron and steel in South Africa dates to 1901 when two tons of pig iron were mined and produced from a primitive blast furnace near Pietermaritzburg. Coulson (2011) states that large-scale steel production in South Africa started with the establishment of the Union Steel Corporation (Usko) in 1911. However, in 1928 the Iron and Steel Corporation of South Africa (ISCOR) was established and further developed to become a major global producer of iron and steel products.

3.5.8 Copper

Phalaborwa is one of the largest copper mines, smelter, and refinery complex and managed by Phalaborwa Mining Company in Limpopo, which is South Africa’s only producer of refined copper (Baxter, 2016). Moreover, according to Baxter (2016), the Phalaborwa Mining Company mine and produce about 80 000 tons of copper per annum and supplies most of South Africa’s and global copper needs. The copper deposit at Phalaborwa copper mine operated until 2002 and produced more than 3 million tons of copper metal (Baxter, 2016). Furthermore, the area in and around Phalaborwa also produces large amounts of magnetite (iron ore), uranium, zirconium, gold, and sulphides.

3.6 IMPACT OF THE MINING INDUSTRY ON THE ECONOMY

South Africa's mining industry is the foundation on which the South African economy was built (Jones & Muller, 2013). At the beginning of the 21st century, after more than a century in operation, the mining industry in South Africa remains the country's economic cornerstone (Lucas, 2014). Jones and Muller (2013) state that the evolution of mining in South Africa resulted in high demand from supporting industries that helped shape the economy of South Africa into a mining economy. Antin (2013) states the sole purpose to establish mining houses was to acquire capital with the intent to attract foreign investment.

Antin (2013) further states that the prominent mining houses among others, included Goldfields, Harmony, Anglo American, and De Beers created the Chamber of Mines who then dominated the South African economy up until the 1990s and functioned as investment banks. The mining industry remains the largest exporter of South Africa's economy. (Fedderke & Pirouz, 2013). Fedderke and Pirouz (2013) state that the mining sector remains a top earner of foreign exchange in the South African economy. Manilal (2016) of the Technology Innovation Agency states that South Africa's economic growth is closely linked to the wealth of the mining industry.

Baxter (2015) from the Chamber of Mines states that the total mineral reserves of South Africa were estimated at about $2.5 trillion in 2015, whilst the mining sector contributed 18% of the GDP which is more than 50% in foreign exchange earnings. Mining contributes handsomely to State Treasury, and about R17 billion in corporate taxes and R6 billion in royalties (Baxter, 2016). Moreover, having been founding members of the Johannesburg Stock Exchange, mining houses still contribute about 30% of their market capitalisation. Furthermore, mining and its related industries actively employ over one million people and pay out about R78 billion in salaries, which is the largest contributor by value to Black Economic Empowerment (BEE).

3.7 ICT IN THE MINING INDUSTRY

The development of innovative technologies benefits every major technical component of the mining industry, including exploration for mineral deposits, mining operations, mineral processing, accompanied by health, safety, and environmental issues (Manilal, 2016). Therefore, according to Manilal (2016) technology development needs to be the focus point of the critical areas of the entire value chain. The overall objectives of information, communication, and technology ICT in the mining industry, according to Manilal (2016), is to:

- Provide efficient, healthy, safe, and competitive mining production.
- Develop environmental and health management technology solutions that will reduce the impact of mining hazards on the workforce, the natural environment and the mining area, and surrounding communities.
- Research lateral migration by exploiting the skills and capability in the mining sector to help in creating novel high-value economic sectors.
- Encourage an innovative culture through developing skills that embody modernization with the support of leadership and infrastructure.
- Provide an Information Technology and Communications environment.
- Provide an environment to manage the information of mining enterprises.

Van den Berg (2015) states that in modern business, innovation has become one of the central drivers of success for enterprises across all industries and in every corner of the globe. Moreover, the mining industry is no different and there is even greater pressure on enterprises in the mining industry to deliver solutions that leverage the latest technology in mining, energy, and ICT. Furthermore, South African mining enterprises, in particular, are pressurised to innovate on social, ICT, and operational fronts. Zimmermann and Emspak (2014) state that innovation in the mining process design relies on drawing inspiration from areas outside the mining industry.

Furthermore, there are emerging technologies that might come to influence the future of mining process design, that might not necessarily exist within the confines of mining technology but may only be on the periphery. Emerging ICT such as big data, Internet of Things (IoT) devices, cloud storage, simulation modelling, and 3D visualisation can provide improvements to data analytics and financial forecasting. Furthermore, in order to address some of the challenges associated with labour-intensive and safety drill-and-blast mining on the gold and platinum mines, the Council for Scientific and Industrial Research (CSIR) developed a network communication architecture called AziSA, an isiZulu word meaning “to inform”. Drill-and-blast mining is often not closely managed, due to the lack of meaningful information about how the mining is done underground (Menell, 2015).

As a result, mining operations could be dangerous and unhealthy especially underground mining, as well as expensive depending on the commodity being mined. AziSA was primarily designed for technology systems that operate in underground mining conditions where there is limited power and network communication infrastructure. As a by-product, the AziSA solution enables network communication to cover and track all areas where people work. This mechanisation was designed to reduce the possibility of physical harm to employees and to provide greater access to mining reserves that would otherwise be too dangerous to explore (Menell, 2015).

Griffith (2015), states that the South African mining industry has huge potential to do well, but needs political will, social cohesion, and industrial and commercial pragmatism. Furthermore, modernisation is key in technology and a precondition for the survival of the industry. The mining industry of South Africa must have the boldness and vision to make a step-change in an ever-changing innovative industry by collaborating with each other to close the technology gap (Griffith, 2015). Griffith (2015) states that innovative technology will improve performance and particularly in areas such as productivity, health, and safety, and thus creating a modern working environment for employees and the mining industry.

Van den Berg (2015) states that South Africa and its business community are up against critical ICT unprecedented levels of cyber-attacks in a rapidly evolving world of information security threats. Furthermore, the reliability and resilience of South Africa’s ICT are essential to the efficiency of the country’s economy in critical areas such as power distribution, telecommunications, mining, national security and intelligence, water supply, social security, public health, and emergency services. According to the Cisco Annual Security Report 2017, Stewart (2017) states that two of South Africa’s biggest economic contributors, being mining and agriculture, are under threat.

The threat is not striking workers, a weakening rand, or poor rainfall, but rather cyber-attacks. Furthermore, the mining industry, energy, oil, and gas are being increasingly targeted by cyber-criminals. Stewart (2017) further states that Cisco observed an extraordinary growth in malicious software encounters in the agriculture and mining industry, which was essentially a relatively low-risk sector. Van den Berg (2015) states that malicious software reports are shifting towards the electronics and manufacturing sector, including the agriculture and mining industries which are estimated at six times the average encounter rate across the industry verticals. Mataranyika (2016) states that mining and telecommunications enterprises in South Africa are the fifth-ranked (5th) target for cyber-attacks.

The mining sector, according to Van den Berg (2015), along with energy, oil and gas is being increasingly targeted by cyber-attackers. Moreover, this is worrying, as mining represents 60% of exports, so an attack on this industry would have serious consequences on the wellbeing of the economy in South Africa. Furthermore, the mining industry must be shielded from cyber-attackers who are after nefarious gains.

3.8 INFORMATION SECURITY GOVERNANCE FRAMEWORK

The purpose of this study was to investigate auditable control measures and policies to propose an information security governance framework for the mining industry of South Africa. The characteristics of the proposed framework will first be discussed and subsequently, the proposed information security governance framework will be depicted. Azmi, Tibben and Than-Win (2018) state that the steep rise of digital activity in modern society has created the need for sound cyber resilient processes for enterprises. Moreover, one important aspect of developing such resilience is the creation of an Information Security Governance Framework that will enable enterprises to access a range of precautionary protection measures to safeguard critical ICT infrastructure (Azmi *et al.*, 2018).

Information and Communication Technology (ICT) combines technology which includes the full range of computer hardware, software and telecommunication which is viewed as the foundation of the internet (Fazlidaa & Said, 2015). ICT can be defined as “technologies that support activities which involve information management that include information gathering, processing, storing, retrieving, presenting in digital format collaboratively in a manner using internal and external communication components (Fazlidaa & Said, 2015). ICT Governance is an element of corporate governance, that is aimed at improving the overall management and governance of ICT to deliver value-add from investment in information, communication, and technology (Calder, 2018).

Moreover, ICT governance frameworks enable enterprises to manage their ICT risks effectively to ensure that the activities associated with information, communication and technology are securely aligned with their overall strategic objectives of the enterprise. An information security governance framework necessitates the deployment of various components to facilitate the directing, execution and controlling of information security processes in an enterprise (Fazlidaa & Said, 2015). ICT Governance is the process of establishing and maintaining an ISG framework and supporting management structures and processes that will provide assurance that the applicable strategies are aligned to support business objectives (Nnoli, Lindskog, Zavarsky, Aghili & Ruhl, 2012).

Moreover, an ISG framework must apply to auditable controls, adhere to policies and internal information procedures to manage risk. Nolan (2019) states that enterprises will be well placed to define an ISG framework that will offer adequate protection to safeguard critical information and technologies against cybersecurity vulnerabilities. Scholtz (2020) states that a well-defined information security governance framework can transform the ICT security of an enterprise. Moreover, to aid the implementation of an excellent ISG framework requires a sound cybersecurity base strategy that seamlessly aligns with strategic business objectives. Moreover, an information security governance framework provides enterprises with the ability to protect themselves against constant evolving global cyber threats.

As the importance of information and IT and their protection increases in modern-day enterprises, proper governance should also be ensured (Von Solms & Von Solms, 2008). This is a vital duty of both executive-level management and every other employee of the enterprise, especially if executive-level management is to address its corporate governance obligations (King III Report, Institute of Directors in Southern

Africa, 2009). Information security governance necessitates the employment of various components to facilitate both the directing and the controlling of information and cybersecurity of an enterprise (Von Solms & Von Solms, 2006).

These components include board directives, information security policies, compliance analysis and many more (Von Solms & Von Solms, 2008). Some enterprises often experience a lack of resources and information security expertise when attempting to address information security governance gaps and fail when they attempt to establish a cybersecurity governance solution (Ozkaya, 2019; Yildirim, Akalp, Aytac & N. Bayram, 2011). Consequently, the literature suggests that these enterprises often have little or no information security governance measures in place. Ozkaya (2019) states that a modern-day information security governance framework should be developed to address the cybersecurity inadequacies in enterprises where there is a requirement.

Ozkaya (2019) believes a framework will address the current information security issues being experienced worldwide and especially by mining enterprises in South Africa. However, as pointed out by Nolan (2019), it does not make sense to reinvent the wheel by starting from scratch with a new ISG framework as there are many to choose from, but certain frameworks might not address all cybersecurity issues of an enterprise. Moreover, the framework must take all stakeholders' interests into account and that processes are in place to provide measurable results.

3.9 INFORMATION SECURITY GOVERNANCE FRAMEWORK INTRODUCTION

Many guiding documents assist enterprises in establishing proper information security governance and management principles. The international standard ISO/IEC 2700x series focuses specifically on information security management and is supported by the certification standard ISO/IEC 27001 (Von Solms & van Niekerk, 2013). In support of the ISO/IEC 2700x series, many guidelines have been written to provide details on both corporate and information security governance frameworks. These include CoBiT 4.1 (IT Governance Institute, 2007), CoBiT 5 (ISACA, 2012) and the King III Report (Institute of Directors in Southern Africa, 2009). The National Institute of Standards and Technology (NIST) SP-800 series framework, which was designed in 2014 through a broadly inclusive, 7-year highly rigorous design process.

ISACA CoBiT 5: Control Objectives for Information and related Technology (COBIT) was developed in 1996 by the Information Systems Audit and Control Association & Foundation (ISACA) to provide management and business process owners with an IT governance model to help understand and manage the risks associated with ICT governance (Witt, Wolanske & Merhout, 2019). COBIT is a framework used by enterprises worldwide for the governance and management of their information and technology, which encompass the entire ICT infrastructure (Witt *et al.*, 2019). Moreover, CoBiT is deployed to manage the technology and information processing of the enterprise so that the business can achieve its strategic objectives.

ISO/IEC 2700x (2013) series of standards: The International organization for Standardization (ISO) is the world's largest developer and publisher of international standards in a wide area of subjects including information security management systems and practices (IT Governance, 2019). The ISO 2700X series is an industry benchmark code of practice for information security. The ISO/IEC 2700x series is the international standard for information security that defines the specifications for an Information Security Management System (ISMS). Moreover, the ISMS system's best-practice approach helps enterprises manage their information security by addressing people and processes including technology.

ISMS is a holistic approach to secure the confidentiality, integrity and availability of corporate information assets.

King III Report: IT governance is defined by King III as "the effective and efficient management of IT resources to facilitate the achievement of corporate objectives" (Liell-Cock, Graham & Hill, 2009). Moreover, IT governance is about the management of governance processes relating to the information, technology and communication services used by an enterprise. The principles of the King III report on IT governance states that:

- The board should be responsible for IT Governance and oversee the implementation of an IT governance framework.

- The board should ensure that information assets are managed effectively.
- Formal processes to manage information are in place that include information security management including the protection of information and personal information.
- IT should be aligned and integrated with the business strategy, performance, and sustainability of the enterprise.
- The board should oversee while delegating the responsibility to management to implement an IT governance framework.
- IT should form an integral part of the enterprise’s risk management strategy.
- A risk and audit committee should assist the board in carrying out its IT responsibilities.

Thus, the conditions of controls and governance depend on the enterprises’ structure, written policies, audit committees, evidence of controls and the competence and integrity of the resources involved. Based on the outcome of this study, the most appropriate framework for mining enterprises in South Africa, as a proposed structural foundation of a cybersecurity framework is the National Institute of Standards and Technology (NIST) framework which was designed in 2014. The aim is to define a detailed and practical end-to-end process to provide an explicit methodology to manage risk to information and communication technology (ICT) systems.

Nolan (2019) states that according to the National Institute of Standards and Technology (NIST), the information security strategies of an enterprise must be consistent with the applicable security laws and regulations through adherence to policies and internal controls to manage information security risk. Moreover, the NIST framework is flexible to define and implement functional day-to-day enterprise-wide policy-based strategic management controls within its operations and business units. Hopkin (2017) states that a comprehensive risk management program is a key component in the planning, design and implementation of any enterprise’s operational cybersecurity program.

Moreover, a selection of an appropriate set of corporate security behaviours and culture is needed to protect the users and the information assets of any ICT system of the enterprise. The NIST information security governance framework will be detailed in this chapter as follows: Firstly, the principles that should be exhibited by the proposed framework will be deliberated to offer a detailed understanding of the proposed ISG framework. Secondly, the framework combined with a detailed discussion of its workings will be introduced. Finally, a discussion of the benefits which originate from the framework will follow.

Several frameworks and best practices exist to help enterprises with ISG design and implementation; however, they share the idea that there is no real “silver bullet” (the ideal way) for designing, implementing, and maintaining a good Information security governance framework within an enterprise (Arnold, 2017). Moreover, enterprises differ in culture, operate in different sectors, and vary in market positioning resulting in different business and information security strategies. Despite evidence that enterprises are taking a more holistic and strategic view of information security governance, recent surveys have revealed large variations in governance practices, that no single ISG framework or document provides the ideal framework for information and cybersecurity (Arnold, 2017).

The guidance is either too detailed or not actionable in a comprehensive manner from the top to the bottom of an enterprise.

3.10 INFORMATION SECURITY GOVERNANCE FRAMEWORK PRINCIPLES

Before the information security governance framework is presented, its principles should be clearly articulated. Hence, a series of principles will now be articulated. Johl, von Solms and Flowerday (2014) state that all forms of governance and in particular information security governance should exhibit a distinctive direct-execute-control cycle. The cycle generally consists of three actions, namely: the *direct, execute* and *control* actions. It is thus essential that the framework which addresses information security governance use this action cycle as its foundation and clearly illustrates it in its process flow. Information security governance requires all levels of management including strategic and executive level management to be involved in the process.

This is indicated by Johl *et al.* (2014), who suggests that three broad levels of management can generally be observed within an enterprise, namely executive, tactical, and operational management. The three different levels of management have specific duties to fulfil during the successful implementation and continued operation of information security governance. Executive-level management does not only display commitment towards the information security governance roadmap and deployment but should also play a critical role in overseeing its implementation and continued management of the program (Von Solms & Von Solms, 2006). Thus, the executive level management collaborates with the operational level cybersecurity custodians to create a framework profile for implementation.

According to international standards and the King III Report, best practices for the direction of information security governance is the responsibility and accountability of management at executive level (ISACA, 2012; ISO/IEC, 2005; King III Report, 2009). Directing starts with executive level management who will clearly articulate the importance of information assets and how they contribute to the strategic vision and success of the enterprise (Von Solms & Von Solms, 2008). The involvement of executive management is essential if information security governance is aligned with the ICT and business objectives of the enterprise (ISACA, 2012; King III Report, 2009). Consequently, the executive-level involvement is often one of the first areas that are looked at when initiating the direct action (Johl *et al*., 2014).

Johl *et al*. (2014) state that when focusing specifically on the *direct* action of information security governance, the executive level management should indicate its vision and strategy for information security in an enterprise. This is critical if a successful information security governance program is to be initiated and subsequently implemented. Moreover, the success of the vision and the strategy of the enterprise will have a direct impact on the motivation for the program to be implemented in the entire enterprise. Consequently, the framework must indicate that it is an executive-level management task to establish these directives Johl *et al*. (2014).

The next phase requires the development of the information security policy architecture which have to be drafted (Johl *et al*., 2014). Moreover, the drafting of the corporate information security policy is typically drafted by the tactical-level management and approved by the executive level management. The corporate information security policy will usually contain, among other details the information security duties of all parties within the enterprise (ISO/IEC 2007, 2005; Von Solms & Von Solms, 2008). The corporate information security policy is generally supported by various secondary-level policies and security procedures and will form the information security benchmark in the enterprise (Von Solms & Von Solms, 2006).

However, as stated by Johl *et al.* (2014) a corporate information security policy offers little detail in the way the selected security measures should be used and implemented, hence these policies are typically supported by several aligned security procedures. Moreover, these policies are used and enforced by operational staff, and it is thus essential that the proposed framework include the information security policy architecture, which is the drafting of a corporate information security policy, supporting secondary-level policies and security procedures. Johl *et al.* (2014) state that when focusing specifically on the *control* action of information security governance, the processes implemented for information security and its governance must be complied with and adhered to.

Moreover, it is thus important to have control measures in place to evaluate and capture any deviations from the control standards so that corrective action is taken if compliance is unsatisfactory. The control action focuses specifically on measuring compliance with the policy, procedures and security measures that were introduced during the direct action. The control action is typically initiated by the operational-level management who perform the compliance analysis with the support of various operational and IT resources. The outcome of this initiative is submitted to the tactical-level management who in turn pass the detail onto the executive level management to update the strategy for information security if necessary (Johl *et al*., 2014).

Executive-level management is never above reproach, it too should evaluate its information security governance efforts (Fitzgerald, 2012). Moreover, it should be clear if the approach in addressing information security governance is done with due care and due diligence at this management level. The proposed framework will allow enterprises to customize their own framework so that it will influence the critical cybersecurity factors to influence the adoption and implementation of the framework. The cybersecurity policies and procedures will thus form part of the ISG framework.

3.11 BACKGROUND TO THE INFORMATION SECURITY GOVERNANCE FRAMEWORK

Based on the earlier discussion of a suitable information security governance framework, the most appropriate framework for mining enterprises in South Africa, as a foundation of a cybersecurity program is the National Institute of Standards and Technology (NIST) framework. This section provides a clear statement to address the findings in this study which indicated a lack of auditable control measures and policies. The research objectives that have been formulated to address this problem statement will be articulated and discussed in the next section. The primary objective of this study was to investigate auditable control measures and policies to propose an information security governance framework for the mining industry of South Africa.

This framework uses concepts and principles that are applicable, usable, and adopted by mining enterprises in South Africa. This framework is based on an existing information security management framework that was developed by the National Institute of Standards and Technology (NIST) and can be adopted by enterprises in any industry as a cybersecurity framework. Calder (2018) referred to the NIST cybersecurity framework as the new game in town and referred to it as the Rosetta stone of cybersecurity. Moreover, NIST offers a blueprint for creating and implementing a cybersecurity program that borrows from a collection of existing frameworks, standards, and industry best practices.

The framework was created to offer enterprises guidance on the critical elements of a cybersecurity program and further offer these enterprises a roadmap to achieve program maturity (Calder, 2018). Ernst & Young endorses the NIST framework and states that the important guidance of the framework supports enterprises to embed privacy management in every aspect of their operations, including cybersecurity (DeBos, 2020). The NIST framework was originally developed in the U.S. and designed to help protect enterprises from cyber-attacks and manage privacy risk across the data life cycle (DeBos, 2020). Moreover, NIST reported that the framework is flexible and can be adopted by small or large enterprises across all industry sectors.

The framework is not limited to enterprises in the U.S. and has been adopted by many global enterprises outside of the U.S. Gurney (2020) states that the NIST framework provides a common language that makes it easier to understand, manage and socialise cybersecurity risk to internal and external stakeholders. Moreover, the framework is used to help identify and prioritise activities to reduce cybersecurity risk, which is also a tool to align security policies and manage cybersecurity, technology, and business risk. The NIST framework can be deployed across the entire enterprise, or it can be focussed on the delivery of critical services within the operations or business units of an enterprise.

The framework is a "living" document that will be continually updated and improved as the technological industry evolve. Enterprises will align their security vulnerabilities and be able to identify the type of threats that will help them determine their risk appetite to formulate a strategy to deploy an ISG framework (Gurney, 2020). Moreover, enterprises will review the potential harm from any given cybersecurity incident to consider if the risk is negligible or tolerable as this will assist the enterprise to pursue a specific framework implementation opportunity. The implementation of an ISG framework will establish an entirely new cybersecurity program, improve an existing one or simply provide an opportunity for the enterprise to review its current framework (DuBos, 2020).

Moreover, should enterprises implement the ISG framework following their specific technological circumstances and mitigate their cybersecurity risks. The primary goals of IT Governance as pointed out by Ellis and Mohan (2019) are to assure that the investments in IT generate business value, and to mitigate the risks that are associated with IT. This can be done by implementing an enterprise structure with well-defined roles for the responsibility of information, business processes, applications, and ICT infrastructure. Moreover, enterprises need a structure or an ISG framework to ensure that the IT function can sustain the enterprise's strategies and objectives.

The ISG framework is methodical, simple yet extremely effective in managing cybersecurity risk to internal and external stakeholders (DuBos, 2020). The framework may be used to help identify and prioritise actions to reduce cybersecurity and privacy risk (Kohnke, Sigler & Shoemaker, 2017). Moreover, the framework is a tool to safeguard and align information security policies, critical business information policies and technological approaches to managing cyber security risk. Kohnke *et al.* (2017) state that the ISG framework is not a one-size-fits-all approach to manage cyber security risk for critical ICT infrastructure. Enterprises will continue to have unique information security risks with different cyber threats, different security vulnerabilities and different risk tolerances.

Thus, the framework must be designed according to the cyber risk profile of each enterprise. Ultimately, according to Kohnke *et al.* (2017), the framework is aimed at reducing and better managing cybersecurity risks to the unique information security challenges of enterprises. The framework can be used in a variety of ways, however, the decision about how to apply it is left to the implementing enterprise. Once the framework is put into greater practice, the additional information security lessons learned can be integrated into future versions of the framework by the enterprise (Kohnke *et al.,* 2017).

The ISG framework complements and does not replace an enterprises' existing information security risk management program (Bellero, 2020). The enterprise can thus use its existing processes to leverage the framework and identify opportunities to strengthen its management of cybersecurity risk while aligning with industry best practices. Alternatively, an enterprise without an existing cyber security program can use the framework as a reference to establish one and seamlessly implement the proposed framework (Bellero, 2020).

3.12 COMPONENTS OF INFORMATION SECURITY GOVERNANCE FRAMEWORK

Having defined the purpose of a framework along with the goal of the envisaged ISG framework, the principles were used as guidelines for developing an information security governance framework. A detailed discussion of the components, relationships and workings of this ISG framework follows in the next subsection as per the recommendation by the National Institute of Standards and Technology (NIST, 2014). The framework consists of three parts, being the framework *core*, *tiers* and *profiles*.

3.12.1 Framework Core

The framework core presents industry standards, guidelines and practices in a manner that allows the socialising of cyber security activities and outcomes across the enterprise from the executive level to the tactical and operations level. The elements of the framework core propose detailed guidance for the development and customization of profiles for individual enterprises. Moreover, the NIST cybersecurity framework is internationally recognised with a strong foundation for the development of a good information security governance core structure. The framework core consists of five concurrent and continuous functions that align with the framework. These functions are divided into five functions, namely: *Identify; Protect; Detect; Respond and Recover* which is defined below:

These functions do not necessarily need to be deployed sequentially to achieve the desired state but can be deployed concurrently and continuously so that an operational culture with a dynamic cyber security risk culture is adopted by the enterprise.

Identify – The enterprise should aim to understand the business context in which it operates as this will enable them to manage cybersecurity risk within the ICT environment, its people, assets, data, and the enterprises' capabilities. Thus, the enterprise develops an understanding of how it can effectively manage the specific cybersecurity risks that it faces.

Protect – Develop and implement appropriate information security measures to protect critical and sensitive information. The aim of the protect measure is to contain the impact of threats that can materialise and harm the most critical ICT functions of an enterprise.

Detect – Develop and implement appropriate security scanning activities to identify the potential occurrence of a cyber security event. An enterprise should aim to detect adverse cybersecurity incidents in a predictive manner by having detective and monitoring controls in place.

Respond – Develop and implement appropriate responsive action when cyber security incidents or breaches are detected.

Recover – Define resilient plans to restore an ICT environment to a known state that might have been compromised due to a cybersecurity incident or breach. Below in figure 3.1 is a simplified version of the Core elements of the NIST framework:

NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Management	Info Protection, Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Figure 3.1: Core elements of the NIST ISG Framework (Source: NIST 2017)

3.12.2 Implementation tiers

Implementation *Tiers* help the enterprise decide and socialise the adequacy of its processes and resources for managing cybersecurity and privacy risk so that it can achieve its desired target state – known as its Profile. Moreover, the tiers provide an enterprise with an instrument to view and understand the defined technical design specifications that will assist them to manage cybersecurity risk. The design and flexibility mean that the framework is not limited to a defined group of enterprises but can seamlessly be adopted by enterprises in the mining industry of South Africa. The framework thus offers a flexible way to address cybersecurity.

The *Implementation tiers* will provide context on how an enterprise assess their cybersecurity risk and the processes that are in place to manage that risk. The tiers will characterise an enterprises' cybersecurity practices over a range that ranges from Tier 1 (Partial), Tier 2 (Risk Informed), Tier 2 (Repeatable) to Tier 4 (Adaptive). During the Tier selection process an enterprise should consider its current risk management practices, threat management, legal and regulatory requirements, strategic business objectives and possible constraints of the enterprise.

Tier 1 (Partial)

Risk management process – The risk management practices of an enterprise are not formalised, and risk is managed in an ad-hoc manner and at times in a reactive manner.

Integrated Risk Management Program – There is limited awareness of cybersecurity risk at the enterprise. The enterprise will implement cybersecurity risk management processes on an irregular, case-by-case basis, based on experienced gained from external sources. The enterprise may not have cybersecurity information that is shared internally.

External Participation – The enterprise does not collaborate with or receive information (for example, threat intelligence, best practices, technologies) from other entities (for example, suppliers, dependencies, researchers, government), nor does it share information. Furthermore, the enterprise is generally not aware of the cyber risk of the products and services it provides or use.

Tier 2 (Risk Informed)

Risk management Process – Management approves risk management practices, although it might not have been established enterprise-wide as a policy. The prioritisation of cybersecurity activities and protection of information are directly informed by enterprise risk objectives, the threat environment or business requirements.

Integrated Risk Management Program – There is an awareness of cybersecurity risk, however, a process to manage cybersecurity risk has not been established. Cybersecurity information is shared informally within the enterprise. Cybersecurity objectives and programs are not shared at all levels within the enterprise.

External Participation – The enterprise collaborates and receive information from other entities but does not share the information with others. This risk essentially indicates that the enterprise is aware of the risks associated with the products and services it provides but does not act consistently or formally to mitigate these risks.

Tier 3 (Repeatable)

Risk management Process – The management of risk has been identified and approved by the enterprise, and then expressed as a policy. The cybersecurity practices, policies and procedures are regularly updated based on the changing risk threat that's identified by the enterprise.

Integrated Risk Management Program – The enterprise deploys an enterprise-wide cybersecurity management process. The enterprise defines and deploy risk-informed policies, processes, and procedures to effectively manage changes in risk. The enterprise also deploys a strategy and methods to respond effectively to changes in cyber risk. Furthermore, the cybersecurity personnel have the knowledge and skills to perform their appointed roles and responsibilities to manage cyber risk. The enterprise has processes in place to monitor the cybersecurity risk of its assets consistently and accurately. Senior and non-cyber security executives engage on a regular basis to manage cybersecurity risk within the enterprise. Senior executives ensure the cybersecurity strategy filters through the entire enterprise.

External Participation – The enterprise collaborate with other external entities regularly to share cybersecurity information. The enterprise formally acts on the risks, including written agreements to communicate baseline requirements, governance structures and policy implementation and monitoring.

Tier 4 (Adaptive)

Risk management Process – The enterprise adapts its cybersecurity practices based on preceding and existing cybersecurity activities, including lessons learned and predictive indicators. Through a process of continuous improvement that includes advanced cybersecurity technologies and practices, the enterprise actively adapts to changing cybersecurity threats and responds promptly to evolving more sophisticated threats.

Integrated Risk Management Program – The program align the relationship between cybersecurity risk and enterprise objectives which is clearly understood when making strategic decisions. Senior executives monitor cybersecurity risk in the same context as financial risk and other critical business risks in the enterprise. The budget of the enterprise includes the existing and predicted risk environment and risk tolerance. The business units implement the vision of the executive leaders as cybersecurity risk management becomes part of the enterprise’s culture.

External Participation – The enterprise understands its role, dependencies, and dependents in the larger cyber risk environment. The enterprise receives, generates and review information about its risks as cyber threats and that of technology evolve. The enterprise shares that information internally and externally with other collaborators. The enterprise uses real-time or near real-time information to understand and act upon cyber supply chain risks associated with the products and services it provides. Finally, the enterprise communicates proactively using formal and informal tools to develop and maintain strong supply chain relationships.

3.12.3 Profiles

Profiles are a set of specific functions, categories, and subcategories from the Core that the enterprise can prioritise to manage cybersecurity and privacy risk. Moreover, the core aligns its cybersecurity activities with its strategic business objectives, risk tolerances and resources. They may represent an enterprise's current privacy activities or desired outcomes. The ISG framework profile enables an enterprise to establish a roadmap so that cybersecurity risk can potentially be reduced (NIST, 2014). Moreover, the profile must be aligned with the objectives of the enterprise, consider legal and regulatory requirements, align with industry best practices, and reflect the cybersecurity risk management priorities.

Given the uniqueness of many enterprises, they may choose to have multiple profiles that are aligned with cybersecurity components that recognise their individual needs. ISG Framework profiles can describe the existing or desired state of specific cybersecurity activities. The existing profile indicates the cybersecurity outcomes that are currently being achieved, whilst the target profile indicates the outcomes that are needed to achieve the desired cybersecurity risk. The ISG framework does not prescribe templates that enterprises should follow to allow for flexibility during implementation.

According to the NIST framework, enterprises compare their existing and target profile that may reveal gaps to address their cybersecurity risk management objectives. The enterprise will define an action plan to address any gaps which can contribute to their roadmap to prioritise and mitigate the enterprise's business needs and risk management processes. This risk-based approach enables the enterprise to determine the resources needed (example, staffing, funding, software, hardware) to achieve its cybersecurity objectives in a cost-effective, prioritised manner.

The life cycle phases of the framework consist of *plan*, *design*, *build* and *deploy*.

- The *plan* phase lays the groundwork and should be defined as clearly as possible. However, the plan should recognise that all considerations and requirements are likely to evolve during the remainder of the life cycle.

- The *design* phase defines the cybersecurity requirements to match the cybersecurity needs and risk disposition of the enterprise.
- The *build* phase involves the resource requirements to start the development of the system to achieve the desired outcomes.
- The *deployment* phase assesses and validate the design specifications to ensure the planned features and functionality of the system is implemented.

The cybersecurity outcomes determined by the framework should serve as a basis for the ongoing operation of the framework system.

3.13 CYBERSECURITY PRACTICES

The newly defined ISG framework can be used to compare its existing cybersecurity activities with those outlined in the newly proposed framework. However, an enterprise may find that it is already achieving the desired outcomes, thus managing cybersecurity commensurate with the known information risk of the enterprise. Ellis and Mohan (2019) state that an enterprise may determine that there are opportunities to improve on its current cybersecurity position when designing a new ISG framework. Thus, the enterprise can use its existing information security framework to develop an action plan to strengthen its current cybersecurity practices and reprioritise resources to reduce cybersecurity risk. The existing state of the cybersecurity risk profile of an enterprise will provide senior executives with a concise way to refine the fundamental concepts of cybersecurity risk (Ellis & Mohan, 2019). Moreover, the executive level management can then assess how the identified risks are managed and how their enterprise stack up at a high level against existing cybersecurity standards, guidelines, and practices. The assessment can help the enterprise to move in a more informed way to strengthen its cybersecurity practices.

3.14 CYBERSECURITY PROGRAM

The following steps illustrate how an enterprise could use the ISG framework to create a new cybersecurity program or improve an existing program (Ellis & Mohan, 2019). The steps should be repeated as necessary to continuously improve cybersecurity.

Step 1: Prioritise and Scope: The enterprise identifies its business mission and objectives and high-level priorities to help them make strategic decisions regarding cybersecurity.

Step 2: Orient: Once the scope of the cybersecurity program has been determined, the enterprise determine the related information systems, assets, regulatory requirements, and the overall risk approach. The enterprise then consults sources to identify threats and vulnerabilities that align with those systems and assets.

Step 3: Create a Current Profile: The enterprise develops a current profile based on the outcomes from the framework core.

Step 4: Conduct a Risk Assessment: The assessment is guided by the enterprise's overall risk management process or previous risk assessment activities. The enterprise analyses the ICT environment to determine the likelihood of a cybersecurity event and the impact it could have on the enterprise. It is also important that the enterprise identify emerging risks as well as using cyber threat information from internal and external sources to understand the potential impact of cybersecurity events on the enterprise.

Step 5: Create a Target Profile: The enterprise creates a target profile that will focus on a cybersecurity assessment of the enterprise to help determine the desired cybersecurity outcome. The target profile will most probably be unique to the enterprise as it reflects on its criteria within the profile.

Step 6: Determine, Analyse and Prioritise Gaps: The enterprise compares the current profile and the target profile to determine gaps. The enterprise creates and prioritise action plans to address gaps. The enterprise then determines the resources and funding necessary to address any gaps. This process allows the enterprise to make informed decisions about cybersecurity activities, support risk management and enable the enterprise to perform cost-effective targeted improvements.

Step 7: *Implement Action Plan*: The enterprise determine what actions to take that will address the identified gaps to achieve the target profile.

An enterprise will repeat the steps as needed by continuously assessing and improving its cybersecurity management strategy (Ellis & Mohan, 2019). Moreover, enterprises may monitor progress through iterative updates to the current cybersecurity profile.

Communication: The ISG framework provides a common language to easily communicate its requirements among interdependent stakeholders who is responsible for the delivery of essential critical ICT infrastructure products and services (Ellis & Mohan, 2019). Moreover, to ensure the effectiveness of the cybersecurity strategy, and ensure the communication requirements are communicated to all the internal and external stakeholders of the enterprise.

3.15 BENEFITS OF AN INFORMATION SECURITY GOVERNANCE FRAMEWORK

The primary goals of IT Governance as pointed out by Uddin, Hassan and Hakim (2020) is to ensure that the investments in IT generate business value and to manage any risks associated with IT. This can be done by implementing an enterprise structure with well-defined roles for the responsibility of information management, business processes, applications, and ICT infrastructure (Uddin *et al*., 2020). Moreover, enterprises need a structure or an ISG framework to ensure that the IT function can sustain the enterprise's strategies and business objectives. The establishment of the information security governance framework (ISG) has many benefits for both enterprises and the information security community.

This subsection highlights the benefits that this framework adds as a result of its principles, as well as identifying the way it enhances the existing information security management framework which was established by the National Institute of Standards and Technology, published in 2014, and revised during 2017 and 2018 (NIST, 2014).

This information security governance framework provides many benefits and beyond those offered by the previously established information security management frameworks (Arnold, 2017). The evolving technology changes witnessed globally and the dependency on information and ICT in enterprises (Arnold, 2017) has resulted in an increased requirement for a sound information security governance framework to be addressed and adequately implemented (Von Solms & Von Solms, 2008).

The NIST information security governance framework offers a significant benefit because it specifically addresses information security governance while still retaining many of the critical concepts depicted in the previously established management frameworks in the IT industry (Hall, 2020). Furthermore, the NIST information security governance framework specifically addresses the critical success factors and implementation steps of information security governance. Thus it offers the mining industry in South Africa a sound foundation for their information security governance implementation, which adheres to international best practices and principles.

The NIST framework offers a significant benefit to the mining enterprises in that it details the entire direct-execute-control action cycle and subsequently each individual action (Belding, 2020). Furthermore, it offers specific details in the way each of these actions is deployed, thus offering greater insight into the components and processes that should be implemented. Executive-level management did not feature prominently in the previous frameworks. Thus, executive management might have believed that they should only show commitment to information security. This was, however, clarified in the new NIST framework and the King III Report, as it indicates that this level of management should be actively involved in the information security governance process by establishing an information security strategic vision and, subsequently, information security board directives (King III Report, 2009; NIST, 2017).

Moreover, this is indicated by means of an executive-level management layer in the core of the NIST framework as well as an indication that board directives should be established, and that executive-level management should also evaluate its information security efforts for due care and due diligence. Landoll (2016) state that it can be argued that the existing control action of the cybersecurity frameworks in the industry only focus on the maintenance of information security policies and procedures, therefore information security governance should also involve other cybersecurity activities. These activities include a compliance analysis of security controls, policies and procedures including the aggregation of the evaluation results to the corporate information security policy and procedures and security requirements (Von Solms & Von Solms, 2008).

Consequently, the information security governance framework offers a significant benefit to the South African mining industry in that it depicts the activities and components that should be implemented and/or used during the control action of information security governance. It can therefore be concluded that the establishment of the information security governance framework has many benefits, not least because it enhances the existing information security management frameworks of an enterprise. However, it should be noted that many more benefits could emanate from the implementation or use of this ISG framework by enterprises in the South African mining industry.

3.16 CHAPTER SUMMARY

The mining industry is important in supporting the wellbeing and growth of South Africa's economy. However, although some mines have reached maturity, South Africa is still heavily dependent on the mineral output, whilst the producers in the mining industry have become global participants. South Africa's mineral reserves – while diminishing – continue to be some of the world's most valuable mineral commodities, which have an estimated net worth of $2.5 trillion (Baxter, 2015). The potential is clear, a consistent mining policy increased investment in existing and new mines, and crucially in the infrastructure serving them, including ICT, which will create conditions for improved growth over the coming years.

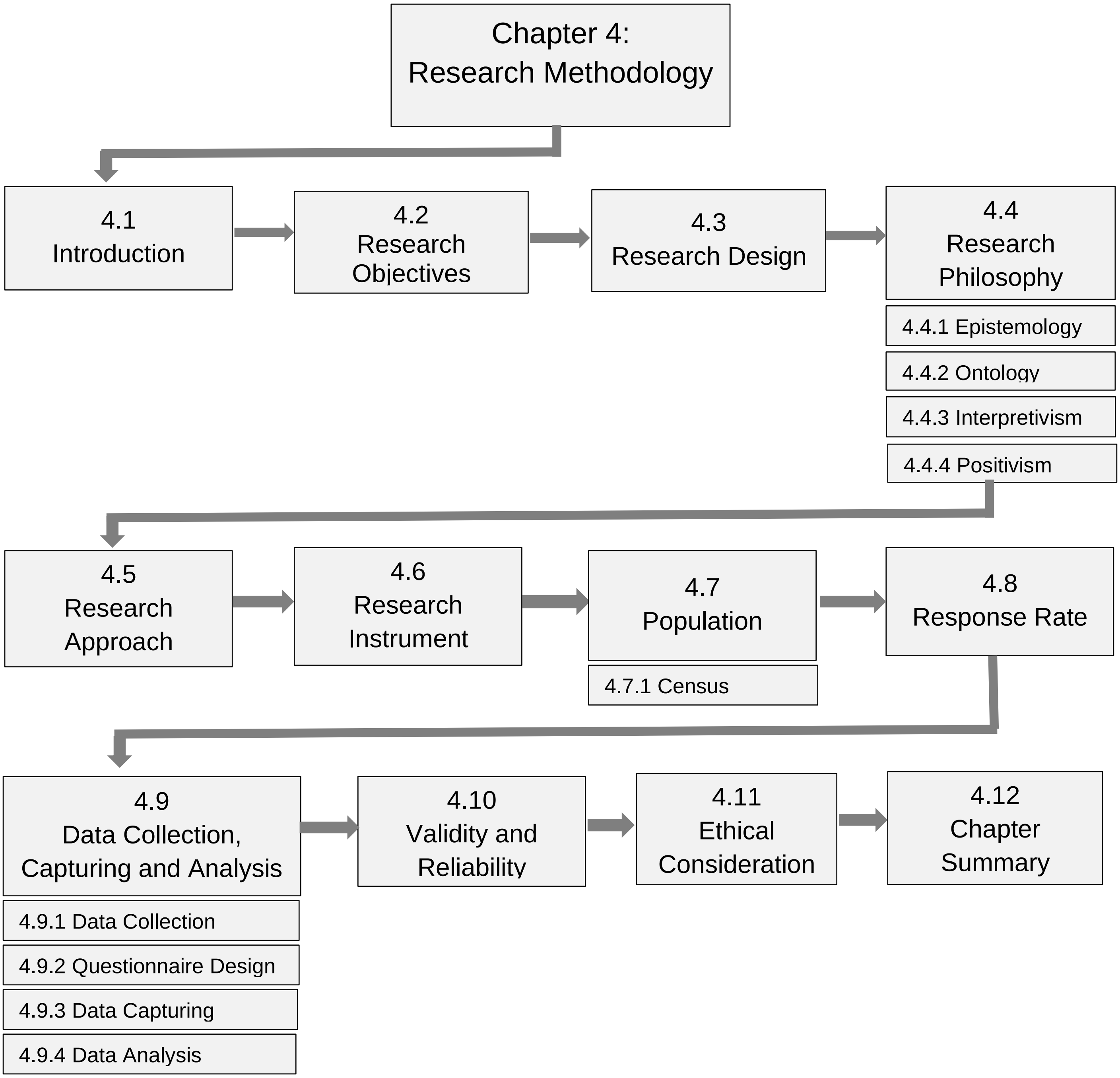
South Africa is popular in the global market for its gold deposits, diamond, and platinum reserves, which remain massive, although gold reserves in the country are believed to be declining. However, the mineral wealth in other metals also provides support to the mining industry as new economic sectors have developed. The production of platinum group metals (PGM), chrome, manganese, nickel, and iron ore, as well as its coal output, promise to ensure South Africa benefits from extractive revenues for years to come.

Enterprises especially those in the South African mining industry can use the ISG framework as a key component in its systematic process to identify, assess and manage cybersecurity risk (Belding, 2020). Moreover, enterprises can use their current process in conjunction with the framework to develop a suitable roadmap that will improve and mitigate cybersecurity risks. The ISG framework should be designed to complement the existing business and cybersecurity operations and can thus serve as the foundation for a new cybersecurity program to align or improve an existing program (Belding, 2020). Mallory (2019) states that the ISG framework is designed to potentially reduce risk and improve the management of cybersecurity risk so that an enterprise can achieve its strategic business objectives.

Moreover, an enterprise that have a framework in place will be able to measure and assign values to their risk and have the benefit of steps to be taken to reduce cybersecurity risk to an acceptable level. The better an enterprise can measure and manage the risks and benefits of cybersecurity strategies, the more value its investments in information technology will materialise in business value add (Mallory, 2019). Enterprises are encouraged to be innovative so that they can customise how they incorporate measurements into their application of the ISG framework with a full appreciation of its usefulness and limitations (Mallory, 2019). With the introduction of this dissertation, the primary objective was to propose an information security governance framework that could facilitate the implementation of sound information security governance principles in enterprises. With the establishment of the information security governance framework in this section, the primary objective has been achieved. Based on the discussion of the South African mining sector and the proposed information security governance framework in this chapter, the following chapter will discuss the methodology that was used in this study.

CHAPTER 4: RESEARCH METHODOLOGY

This chapter discusses the research methodology followed in this study. It outlines, describes, and discusses the objective of the research, design, philosophy, approach, and research instrument. The chapter also outlines the study population, census, response rate, data collection, capturing, and analysis. The chapter also discusses the validity and reliability of the research instrument and conclude by discussing the ethical consideration.



4.1 INTRODUCTION

A quantitative research approach was used to develop meaningful segmentation to provide an account of usage and attitudes (Samuel, 2012) which is in line with the objectives of the study. Research is an academic activity and as such the term should be used in a technical sense (Kothari, 2014). Moreover, the research comprises defining and redefining problems, formulating hypotheses or suggested solutions; collecting, organising, and evaluating data; making deductions and reaching conclusions, and finally carefully testing the conclusions to determine whether they fit the formulating hypothesis (Kothari, 2014).

Research is thus an original contribution according to Kothari (2014), to existing knowledge in the pursuit of truth with the help of study, observation, comparison, and experiment. Thus, according to (Kothari, 2014), research is the pursuit of truth with the assistance of study, observation, comparison, and experiment. Kothari (2014) concludes by stating that research refers to the systematic method which consists of enunciating the problem, formulating a hypothesis, collecting, and analysing the facts or data, and researching certain conclusions either in the form of a solution (s) towards the area of study or in certain generalisation for some theoretical formulation.

Neville (2007) and Melnikovas (2018) support this view by stating that research is a process of enquiry and investigation; it is systematic, methodical, and ethical; research can help solve practical problems and increase knowledge. Moreover, research may be defined as a scientific and systematic search for pertinent information on a specific topic or area of interest. Research methodology is the systematic, analysis of the methods applied to a field of study, as it comprises the theoretical analysis of the body of methods and principles associated with an area of knowledge (Richey & Klein, 2014).

Moreover, research methodology typically encompasses concepts such as paradigm, theoretical model, phases, and quantitative or qualitative techniques. Richey and Klein (2014) state that a methodology does not set out to provide solutions. Research methodology offers the theoretical foundation for understanding which method, set of methods, or best practices can be applied to specific research. Research methodology is described by Goundar (2019) as a systematic way of resolving a problem. The methodology can be defined as science according to Goundar (2019) which is the studying of how research is to be carried out.

Essentially, it entails the procedures by which researchers go about their work of describing, explaining, and predicting phenomena which are defined as research methodology (Goundar, 2019). Moreover, it is also defined as the study of methods by which knowledge is gained to provide a work plan for the research. The term research philosophy refers to a system of beliefs and assumptions about the development of knowledge (Saunders, Lewis & Thornhill, 2019). Although this sounds rather profound according to Saunders *et al.* (2019), it is precisely what the researcher is doing when embarking on a research study, developing knowledge in a particular field.

Research philosophy is what the researcher perceives to be truth, reality, and knowledge (Gemma, 2018). Moreover, the philosophy outlines the beliefs and values that guide the design, collection, and analysis of the data in a research study, by which these choices complement philosophical principles. To have a complete understanding of this phenomenon, this study examined the ontological, epistemological, and methodological procedures as they are implemented in the philosophy of this study. There are three commonly known philosophical research paradigms used to guide research methods and analysis (Gemma, 2018). These paradigms are positivism, interpretivism, and critical theory.

All three paradigms have different ontological and epistemological principles guiding them. Gemma (2018) states that being able to justify the decision to adopt or reject a philosophy should form part of the basis of research. Thus, it is therefore important to understand these paradigms as pointed out by Gemma (2018), as the origins and principles of these paradigms will assist the researcher in the appropriate decision for the study that informs its design, methodology, and analysis. This chapter presents the research methodology followed in the study. The discussion begins by outlining the research paradigm epistemological principle than the paradigm using the ontological principle.

The discussion further outlines the paradigm in the positivist and interpretivist research philosophy. Subsequently, there is a discussion of the research approach as well as the research strategy which outlines the data collection and analysis techniques used.

Finally, the population and sampling procedures are described that were used in this study.

4.2 RESEARCH OBJECTIVES

The primary objective of this study is to investigate auditable control measures and policies in order to propose an information security governance framework for the mining industry of South Africa.

In order to fulfil the primary objective, the following secondary objectives were examined:

4.2.1 To determine IT governance practices used by enterprises in the mining industry.

4.2.2 To identify the types of access control processes put in place by enterprises in the mining industry.

4.2.3 To establish if Information Security policies are implemented within South African mining enterprises.

4.2.4 To analyse auditable control measures used by enterprises in the South African mining industry.

4.3 RESEARCH DESIGN

A research design is a procedure to collect, analyse, interpret, and report on the data in research studies (Creswell & Plano Clark, 2007). Saunders *et al.* (2012) state that research design is the overall plan to connect the conceptual research problems with the relevant and achievable empirical research. Moreover, the researcher will go about to answering the research questions, and that during the research design phase, the researcher needs to decide on the various quantitative and qualitative data-collection techniques and the succeeding data-analysis procedures. Grey (2014) supports this view by stating that research design sets the procedure on the required data, the methods to be applied to collect and analyse this data, and how the research question will be answered.

Creswell (2014) supports the view of Grey (2014) by stating that a research design is a strategy for answering the research questions, whilst defining the overall approach and determining how data will be collected and analysed. Moreover, the research design is intended to provide an appropriate framework for a research study. A very significant decision in the research design process is the choice to be made regarding the research approach since it determines how the relevant information for a study will be obtained (Creswell, 2014). The research design according to Fraenkel, Wallen and Hyun (2012) establishes and assists the researchers' decision-making processes, the conceptual structure of the research and, presents the analysis methods that were used to address the central research problem of the study.

Moreover, a thorough research design helps the researcher set the boundaries of the study, maximise the reliability of the findings and avoid misleading or providing incomplete conclusions. Thus, if any aspect of the research design is flawed or under-developed, the quality and reliability of the researchers' final results and the overall value of the study will be weakened. Researcher-initiated studies allow investigators more discretion in terms of the specification of the research goals and objectives (Melnikovas, 2018). Moreover, the classification relies on the purpose of the research area as each design serves a different end goal and purpose. Before defining the goals and objectives of a particular research project according to Melnikovas (2018), it is advisable to identify the purpose of the research.

There are three possible forms of research design according to Bevans (2019), which is exploratory, descriptive, and explanatory. The classification relies on the purpose of the research area as each design serves a different end goal and purpose. Exploratory research aims to formulate problems, clarify concepts, and form hypotheses Bevans (2019). Moreover, exploration can begin with a literature search, a focus group discussion, or case studies. Exploratory research typically seeks to create hypotheses rather than test them. Data from exploratory studies tends to be qualitative. Saunders *et al.* (2012) state that exploratory research is conducted when not enough is known about a phenomenon as well as when a problem has not been clearly defined.

Moreover, exploratory research does not aim to provide the final and conclusive answers to the research study questions but merely explores the research topic with varying levels of depth. Therefore, according to Saunders, Lewis and Thornhill (2019), its theme is not to find a solution to new problems of which little or no previous research has been done. Thus, exploratory research is typically conducted when a researcher started an investigation and wishes to understand the topic. Moreover, exploratory research is typically conducted during the early stages of a project, usually when a researcher wants to test the feasibility of conducting a more extensive study. Descriptive research provides additional research guidelines by describing people and situations (Saunders *et al.,* 2019).

This view is supported by Blumberg, Cooper and Schindler (2005) who state that the purpose of descriptive studies is to provide a picture of a situation, person, or event or show how things are related to each other as it naturally occurs. Moreover, descriptive studies generally are not driven by structured research hypothesis as it frequently aims to describe characteristics. Punch (2005) states that data collected from descriptive research may be qualitative or quantitative whilst quantitative data presentations is normally limited to frequency distribution and summary statistics. Descriptive studies cannot explain why an event has occurred according to Punch (2005) and is such is more suitable for a relatively new or unexplored research area.

Thus, descriptive research aims to describe or define the topic at hand or describe or define a particular phenomenon. Explanatory research builds on exploratory and descriptive research which further identifies actual reasons a phenomenon occurs Bryman & Bell (2015). This view is supported by Creswell (2014) who states that the primary purpose of explanatory research is to explain why phenomena occur and to predict future occurrences. Explanatory studies are characterised by research hypotheses that specifies the nature and direction of the relationships between or among the variables being studied (Bryman & Bell, 2015).

The data are quantified and almost always require the use of statistical testing to establish the validity of the relationships (Babbie, 2010). Moreover, explanatory research tries to identify causes and reasons and provides evidence to support or refute an explanation or prediction. Babbie (2010) states that explanatory research is conducted to discover and report on certain relationships among different aspects of the phenomenon of the study. Thus, explanatory research aims to explain why particular phenomena work it does. This study was quantitative and was descriptive using a secured web-based questionnaire to collect and analyse data obtained from participants and generate statistical numerical data (Hair, Celsi, Money, Page & Samouel, 2011).

The analysis of the questionnaire data was analysed using quantitative techniques, such as correlation, cross-tabulation, and additional descriptive and statistical techniques. Bell (2010) states that particular attention must be given to the comments of respondents whilst this study will discuss the practices of information security of enterprises in the South African mining industry. This approach meant that the researcher was not able to influence or manipulate any of the variables or outcomes of the survey but only observed, measured and report on the results. Moreover, the descriptive research of this study aims to describe a population situation or phenomenon accurately and systematically.

The goal of descriptive research is to describe a phenomenon and its characteristic (Gall, Gall & Borg, 2007), which is what this study aims to achieve. Moreover, the descriptive research design methodology focuses more on *what*, *where*, *when,* and *how* of the research subject rather than the '*why'*. One of the aims of this study was to collect relevant information to address the research problem because not much was known about the information security status in the South African mining industry. Moreover, descriptive research was deemed an appropriate choice for this study as it aims to identify characteristics, frequencies, trends, and categories of the research problem.

The research design of this study was carefully designed to ensure that the results are valid and reliable. The data analysis of this study was descriptive, which is referred to as the basic conversion of research data which describes the crucial characteristics, such as tendency, distribution, and variability (Zikmund *et al.,* 2013). This study used descriptive statistics to summarise the data attained for a collection of individual units of analysis (Welman, Kruger & Mitchell, 2009; Weiers, 2008). Descriptive statistics involve statistical procedures that are used to organise, simplify, summarise, and display data, that describe imperative qualities of a set of measurements (Mendenhall, Beaver & Beaver, 2013).

Furthermore, Schniederjans, Schniederjans and Starkey (2015) state that descriptive statistics are used to identify possible trends in large data sets or databases which are to provide a general idea of what the data looks like. Furthermore, this study made use of descriptive statistics of reliable factors and Pearson's correlations of valid and reliable factors. This study was quantitative and descriptive. Moreover, according to Hair *et al.* (2011) research design provides a basic direction for doing a research project. The research design needs to provide the relevant information in the research questions and hypothesis as this will guide the researcher to formulate a study design. The study concludes by providing a detailed analysis of one-way ANOVA analysis.

Descriptive statistics include measures of tendency mean and measures of dispersion (standard deviation). This study analysed the data to ensure appropriate validity and reliability measures were employed in the quantitative research. Somekh and Lewin (2011) state that reliability refers to the extent that the measurement instrument yields the same results over multiple trials. It can thus be stated that the research design is a structure, strategy, and plan that provides direction when doing a research project (Bell, 2010; Saunders et al., 2012; Hair *et al.,* 2011). Quantitative research is defined as a systematic investigation of phenomena by gathering quantifiable data and performing statistical, mathematical, logical, or computational techniques that is unbiased (Bhandari, 2020).

The major characteristics of quantitative research are the focus on deductive methods of reasoning and explanation, prediction using standardised data collection, and statistical analysis methods (Chakraborty *et al.,* 2013). Moreover, quantitative research is usually associated with the positivist philosophy that is linked with natural sciences. As such the researcher's preconceptions do not influence the research; it is the objective facts and empirical evidence that matter. The strength of the quantitative approach is that it is suitable for testing and validating the already constructed theories through numerical data, thus allowing generalised conclusions to be made.

The quantitative research method is often used to standardise the data collection process and generalise findings (Bhandari, 2020). Thus, this study used the quantitative research approach based on data collection measures, positivism philosophy, the research being unable to influence the research results and presented objective facts. Furthermore, the quantitative approach used for this study was suitable to test and validate the data collected which allowed the conclusions to be generalised. Thus, based on the quantitative and descriptive research methods, this study used the approach in quantifying, analysing, and presenting the data. Qualitative research is a process of inquiry that seeks an in-depth understanding of a phenomenon within its natural settings (Streefkerk, 2020).

Moreover, qualitative research focuses on 'why' rather than 'what'. Qualitative research as stated by Streefkerk (2020) gathers data that is non-numerical and research methods that are more communication based rather than logical or statistical procedures. Qualitative research investigates attitudes, behaviours, and experiences, through research techniques, such as meetings, in-depth interviews, personal observation, etc. (Flick, 2018; Cohen, Manion & Morrison, 2007). Qualitative research as pointed out by Flick (2018) is a methodology that can include relational, social, and cultural settings with a view of gathering detailed opinions from participants. It can thus be stated according to Cohen *et al.* (2007) that qualitative research is defined as a market research method that focuses on obtaining data through open-ended and conversational communication.

This method is not only about 'what' people think but also 'why' they think so. In this study, a quantitative research approach was used with close-ended questions to gather quantifiable data and performed statistical analysis to derive meaningful outcomes.

4.4 RESEARCH PHILOSOPHY

Research is a process of enquiry and investigation; it is systematic, methodical, and ethical; research can help solve practical problems and increase knowledge (Neville, 2007). Melnikovas (2018) states that research in common vernacular refers to a search for knowledge. Moreover, it may be defined as a scientific and systematic search for pertinent information on a specific topic or area of interest. Research methodology is the systematic, analysis of the methods applied to a field of study, as it comprises the theoretical analysis of the body of methods and principles associated with an area of knowledge (Richey & Klein, 2014).

Richey and Klein (2014) state that a methodology does not set out to provide solutions, which is not the same thing as a method. Instead, it offers the theoretical underpinning for understanding which method, set of methods, or best practices can be applied to a specific case. Research methodology is described by Goundar (2019) as a systematic way of resolving a problem. The methodology can be defined as science according to Goundar (2019) which is the studying of how research is to be carried out.

Essentially, it entails the procedures by which researchers go about their work of describing, explaining, and predicting phenomena which are called research methodology (Goundar, 2019). Saunders, Lewis and Thornhill (2018) proposed the research onion framework (Figure 4.1), which defines pictorially the various aspects of the research to be examined and planned in order to come up with a sound research design. The research onion guides the researcher through all the steps that can be used when developing a research methodology. Figure 4.1 Research onion

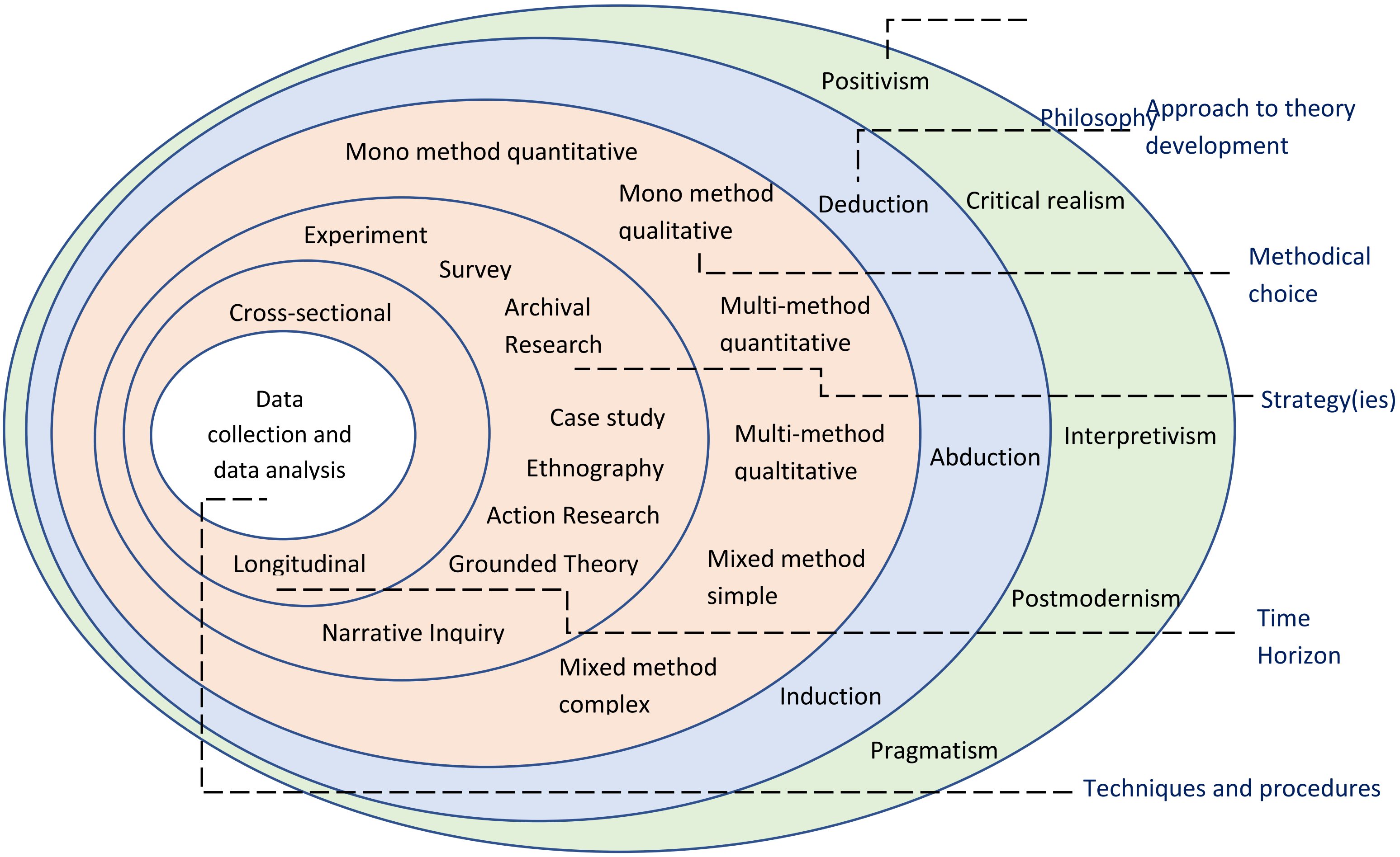


Figure 4.1 The “Research onion” Source adapter from Mark Saunders, Philip Lewis, and Adrian Thornhill ©2018

The proposed research philosophy of and approach to information security in the South African mining industry, as adapted from the research onion of Saunders *et al.* (2012) is outlined in figure 4.1. It depicts six layers that are embedded in a quantitative approach. The six layers are as follows:

Philosophy: To measure information security in the South African mining industry. A positivism philosophy may be used according to Saunders *et al.* (2012) where a structured methodology is recommended for researching information security using quantitative methods including statistical analysis. According to De Villiers (2012), the objective of positivist research is to obtain research results that are reliable, consistent, unbiased, and replicable through other research studies in order to represent reality. In the context of information security in the South African mining industry, one might argue that although a survey gives precise and accurate measures of the perceived information security.

However, according to Saunders *et al.* (2012) the survey questions might not be interpreted in the same manner by all employees, nor would employees have the same background of information security when answering the questions. Moreover, focus groups and interviews can assist in obtaining more in-depth information on certain variables that are measured when using an information security questionnaire. However, a positivist philosophy, using a quantitative method, is primarily proposed for this study in order to propose a methodology to derive a valid and reliable measuring instrument (Saunders *et al.,* 2012).

Method: A deductive method is often linked with a survey. The research starts with a theory and then a hypothesis is deducted from the theory and tested. In the case of information security in the South African Mining industry, participants completed a questionnaire. Thus, for this study, the approach is limited to a questionnaire of a quantitative method to propose which steps to follow in order to derive a valid and reliable measuring instrument. If focus groups or interviews are considered, then the methods could be extended to an inductive method.

Strategy: Quantitative research methods have been used with great success in the information security discipline (Da Veiga, 2016). Questionnaires and surveys have been widely used as research tools in the social sciences. Moreover, this method is beneficial in descriptive or exploratory research. Da Veiga (2016) further state that surveys are specifically beneficial as they are cost-effective and potentially a large number of responders can participate with minimal resource requirements. To assess cybersecurity, the overall status of information security can be determined. Through such an analysis, the status of information security in the South African mining industry can be assessed and shortcomings identified that require a solution in order to improve information security to an acceptable level in the South African mining industry, thereby protecting information, information assets and people.

Choices: A mixed-method approach can be used to assess information security, however in this study a questionnaire would be used to perform the quantitative assessment. This approach can be used successfully when survey responses are not sufficient to generalise the findings across the mining industry group to align with the sampling requirements. Thus, for this study, the approach is limited to a questionnaire of a quantitative method to propose which steps to follow in order to derive a valid and reliable measuring instrument.

Time horizon: This study used a secured online web-based questionnaire allowing the researcher to monitor reactions to changes over time by comparing data collected at different intervals.

Techniques and procedures: The data were analysed using statistical calculations. Statistics are used in quantitative research methods to analyse survey data as well as in the questionnaire development to ensure its validity and reliability (Da Veiga, 2016).

4.4.1 Epistemology

Epistemology relates to the elements of satisfactory knowledge in research (Saunders *et al.,* 2019). Researchers will subconsciously develop new knowledge at every stage of their research will make several assumptions (Burrell and Morgan, 2016). These include (but are not limited to) assumptions about the realities the researcher encounter in their research (ontological assumptions), about human knowledge (epistemological assumptions), and about the extent and ways their values influence the research process (axiological assumptions) (Saunders *et al.,* 2019). Epistemology refers to assumptions of knowledge that constitute acceptable, valid, and legitimate knowledge, and how society can communicate knowledge to others (Burrell & Morgan, 2016).

Consequently, different business and management researchers adopt different epistemologies in their research, which include project-based or archival research and autobiographical accounts (Martí & Fernández, 2013), narratives (Gabriel, Gray & Goregaokar, 2013), and fictional literature (De Cock & Land, 2006). The variety of epistemologies provides a large choice of research methods (Saunders *et al.,* 2019). Moreover, it is important to understand the implications of different epistemological assumptions related to the researchers' choice of method(s), strengths, and limitations of subsequent research findings. Within the epistemology framework according to Saunders *et al.* (2019), the subsequent research findings are likely to be considered objective and generalisable.

4.4.2 Ontology

Ontology is the nature of reality (Saunders *et al.,* 2019) and epistemology is the relationship between the researcher and the reality of how this reality is captured or known (Carson *et al.,* 2001). Moreover, ontological assumptions shape how researcher sees and study their research objects. The researchers' ontology, therefore, determines how he or she see the world of business and management which in turn support them in making their choices with their research project. Ontology relates to the values of a researcher's view of what is known as real and what someone believes to be factual (Bryman & Bell, 2015). Ontology is concerned with identifying the overall nature of the existence of a particular phenomenon (Edirisingha, 2012).

Thus, when researchers seek answers (reality) to their research questions, they are referring to a particular type of knowledge that exists external to the researcher. On the contrary, as pointed out by (Edirisingha, 2012), epistemology is about how we go about uncovering this knowledge (that is external to the researcher) and learn about reality. This essentially means according to (Edirisingha, 2012) that ontology is concerned with questions such as how we know what is true and how do we distinguish between true from falls, whilst epistemology is internal to the researcher which is how they see the world around them (Edirisingha, 2012). It is generally accepted that research is based on several interconnected philosophical assumptions (Saunders *et al.,* 2019).

This study will follow Davies (1991) in concentrating on the relationship of ontology (theory of being/reality/essence), epistemology (theory of knowledge), and methodology (theory of method/action). This study's key assumptions are predicated upon the relationship between human beings and their environment since ontological and epistemological conscripts cannot be conceptually separated. Since the ontology of this study is mainly concerned with the reality of cybersecurity and interpretations, whilst the assumptions of epistemology stance are mainly constructionist (Crotty, 2003), legitimate knowledge, learning about the social reality of cybersecurity in the South African mining industry, it is thus logically sequenced that interpretivism is the theoretical perspective underpinning this study (Saunders *et al.,* 2019).

This study's key assumptions are based on the relationship between human beings and their environment since ontological and epistemological conscripts cannot be conceptually separated. This key assumption underpins all areas of social science, more especially since the impact of cybersecurity on human beings is fundamentally the subject and object of enquiry (Burrell & Morgan, 2016).

4.4.3 Interpretivism

The position of interpretivism in relation to ontology and epistemology is that interpretivist believes the reality is multiple and relative (Hudson & Ozanne, 1988). Furthermore, Lincoln and Guba (1985) state that these multiple realities also depend on other systems for meanings, which makes it even more difficult to interpret in terms of fixed realities. Interpretivism deals with an understanding phenomenon in a cultural and contextual situation (Orlikowski & Baroudi, 1991). Interpretivists avoid rigid structural frameworks such as in positivist research and adopt a more personal and flexible research structure (Carson, Gilmore, Perry & Gronhaug, 2001), which are receptive to capturing meanings in human interaction (Black, 2006) and make sense of what is perceived as reality (Carson *et al.,* 2001).

The interpretivist researcher enters the study with some sort of prior insight into the research context, but as pointed out by (Hudson & Ozanne, 1988) the researcher assumes that this insight is insufficient in developing a fixed research design due to complex, multiple, and unpredictable nature of what is perceived as reality. Information Systems research is often viewed as interpretive, on the assumption that knowledge within a research discipline is deduced from social constructions such as tools, documents, language, and other Information Technology artefacts (Klein & Myers, 1999). Interpretivism in Information Systems (IS) emerged in the 1980s (Neuman, 2000). While at the time according to Neuman (2000) it presented an important alternative to positivism, however, the world has changed significantly since then, raising questions about its efficacy for Information Systems relevant to the emerging world of ubiquitous Information Technology.

4.4.4 Positivism

The positivist ontology believes that the world is external (Carson *et al.,* 1988) and that there is a single objective reality to any research phenomenon or situation regardless of the researchers' perspective or belief (Hudson & Ozanne, 1988). Positivism as a philosophy adheres to the view that only factual knowledge is gained through observation (the senses), including measurement, and is trustworthy (Saunders, Lewis & Thornhill, 2016). Positivists also claim it is important to clearly distinguish between fact and value judgement. Moreover, in positivism studies, the role of the researcher is limited to data collection and interpretation objectively. In these types of studies, research findings are usually observable and quantifiable.

Saunders *et al.* (2016), state that the only limitation is the researchers' ability to know the absolute truth is the tools that are used to collect and analyse data. Positivist researchers remain detached and neutral from the participants and data to avoid influencing the research findings (Carson *et al.,* 2001; Saunders *et al.,* 2016). Moreover, for positivists, this is a credible position, because of the measurable, quantifiable data that the researcher collects. Remenyi *et al.* (1998) define positivism as "a researcher that follows methodological rules that are independent of the content and context of the enquiry".

This study supports epistemology and was based on the philosophical position of positivism, whilst the research findings in positivism studies are only descriptive and subsequently selected to be the preferred philosophical method adopted for this study (Denscombe, 2010). Collins (2010) informs that the researcher is independent of the study and there are no provisions for human interests within the study. Moreover, whilst the research findings in positivism studies are descriptive, the positivism philosophy was subsequently selected to be the preferred philosophical method adopted for this study.

4.4.5 Positivism as the preferred research philosophy

This study used the positivism research philosophy as this philosophy can be attributed to the characteristics of abstraction of positivism. Validity is an extensive area in positivism as it retains data by way of the vigilant use of methods (Cohen, Manion & Morrison, 2007). Positivist research asserts that this philosophy is conceivable to embrace a distant, detached, impartial, and non-interactive position when adopting an isolated, detached, unbiased, and non-reciprocal position (Cohen *et al.,* 2007). Positivism depends on quantifiable observations that lead to statistical analysis (Wilson, 2010).

Crowther and Lancaster (2008) state that researchers need to be mindful that a positivist approach requires that they are independent of the research and remain objective. In other words, studies with positivist philosophy are based purely on facts and objectives. The researcher of this study conformed to the positivist approach by remaining independent and objective during the entire research. The data collected and analysed for this study was independently consolidated and presented by an independent statistician so that the researcher remain neutral and detached from the outcome to avoid influencing the research findings of this study. This study therefore adopted the positivist research philosophy. This study will test the validity of the analysed data and present the evidence which supports or rejects the claims and the assumptions made in the study.

Table 4.1 below summarises the various research philosophies including the positivist philosophy used in this study.

Ontology	Positivist	Interpretivist
Nature of 'being' / nature of the world	Have direct access to real world	No direct access to real world
Reality	Single external reality	No single external reality
Epistemology		
'Grounds' of knowledge / relationship between reality and research	Possible to obtain hard, secure objective knowledge	Understood through 'perceived' knowledge
	Research focus on generalisation and abstraction	Research focus on the specific and concrete
	Thought governed by hypotheses and stated theories	Seeking to understand specific context
Methodologies		
Focus of research	Concentrates on description and explanation	Concentrates on understanding and interpretation
Role of the researcher	Detached, external observer	Researchers want to experience what they are studying
	Clear distinction between reason and feeling	Allow feeling and reason to govern actions
	Aim to discover external reality rather than creating the object of study	Partially create what is studied, the meaning of phenomena
	Strive to use rational, consistent, verbal, logical approach	Use of pre-understanding is important
	Seek to maintain clear distinction between facts and value judgements	Distinction between facts and value judgements less clear
	Distinction between science and personal experience	Accept influence from both science and personal experience
Techniques used by researcher	Formalised statistical and mathematical methods predominant	Primary non-quantitative

Source: Adopted from Carson, Gilmore, Perry and Gronhaug, 2001, *Qualitative Marketing Research*

4.5 RESEARCH APPROACH

Research approaches are plans and the procedures for research that span the steps from broad assumptions to detailed methods of data collection, analysis, and interpretation (Bryman & Bell, 2015). Moreover, there are three approaches to research namely: deductive, inductive, and abductive research approaches. The Deductive research approach tests the validity of assumptions (or theories/hypotheses) being considered, whereas the inductive research approach contributes to the emergence of new theories and generalisations. However, according to Bryman and Bell (2015), abductive research starts with surprising facts, and the research process is devoted to defining clarification.

Creswell *et al.* (2007), state that the inductive researcher works from the “bottom-up”, using the views of the participants to build broader themes that aid in generating a theory to interconnect the themes. Moreover, in research, the two main types of analysis typically used are quantitative (deductive) and qualitative (inductive). Gray (2009) argues and states that there seems to be some disagreement among researchers in deciding which is the best method to use when conducting research and gathering data, as these two methods are not mutually exclusive and often address the same question using different methods.

This study adopted the deductive research approach which Saunders *et al.* (2012) describe as an approach that has a clearly defined strategy with the research question(s) and objectives; whereby the researcher does not start with any predetermined philosophies or conceptual frameworks. Moreover, this study further aligned with the deductive theory testing which is usually associated with a positivist philosophy of scientific research and with quantitative research methods in social sciences (Guba & Lincoln, 1994; Yin, 1994). Thus, the deduction research approach begins with a universal view of a situation and works back to the particulars; in contrast, the induction research approach moves from fragmentary details to a connected view of a situation.

This study adopted a deductive research approach which Myers (2010) describes as an approach that explores a known theory or phenomenon and then tests if that theory is effective in given circumstances. Neuman (2003) states that the deductive approach is to collect quantitative data, however, this does not necessarily mean that the deductive approach may not use qualitative data. The final characteristic of the deduction is generalisation which is adopted by this study. The characteristics of the deductive research approach, being an approach that emphasises a scientific approach, emphasises structure, quantification, generalisability, is most likely underpinned by the positivist research philosophy which is used as a research methodology for this study.

The inductive research approach begins with specific observations and the conclusions are generalised (Zalaghi, 2016). In the inductive approach, once the researcher selects several observations correctly, the outcome can then be generalised to all or groups of similar conditions and situations. Moreover, these generalisations need to be tested, of which some might be verified, and some rejected. Saunders *et al.* (2012), states that in the induction process, the researcher being the observer, should honestly and without any prejudgements and biases, and with an impartial mind, register what has been observed.

Moreover, in induction research, no theory is applied at the beginning of the research and the researcher thus enjoys complete freedom to determine the course of the research. The main concern with the inductive approach as pointed out by Zalaghi (2016), is that the inductive method can be influenced by the researcher who has limited knowledge of the relations and the data of the research. It must be noted that this study does not use the inductive research approach. As the deductive research approach is the prevalent view for this study, other types of research philosophies are less accepted. In an abductive approach, the research process starts with ‘surprising facts’ or ‘puzzles’, and the research process is devoted to their explanation (Bryman & Bell, 2015).

Moreover, these ‘surprising facts’ or ‘puzzles’ may emerge when a researcher encounters an empirical phenomenon that cannot be explained by the existing range of theories. While explaining ‘surprising facts’ or ‘puzzles’, Bryman and Bell (2015) state that the researcher can combine both, numerical and cognitive reasoning. Despite its increasing popularity in business studies, the application of abductive reasoning in practice is challenging and researchers are advised to use traditional deductive or inductive approaches.

The following table illustrates the major differences between deductive, inductive, and abductive research approaches in terms of logic, generalisability, use of data and theory. Table 4.2 summarises various research approaches.

	Deduction	Induction	Abduction
Logic	In a deductive inference, when the premises are true, the conclusion must also be true	In an inductive inference, known premises are used to generate untested conclusions	In an abductive inference, known premises are used to generate testable conclusions
Generalisability	Generalising from the general to the specific	Generalising from the specific to the general	Generalising from the interactions between the specific and the general
Use of data	Data collection is used to evaluate propositions or hypotheses related to an existing theory	Data collection is used to explore a phenomenon, identify themes and patterns, and create a conceptual framework	Data collection is used to explore a phenomenon, identify themes and patterns, locate these in a conceptual framework and test this through subsequent data collection and so forth
Theory	Theory falsification or verification	Theory generation and building	Theory generation or modification; incorporating existing theory where appropriate, to build new theory or modify existing theory

Source: Adopted from Bryman and Bell, 2015, *Business research methods*

4.6 RESEARCH INSTRUMENT

A structured self-administered, web-based questionnaire was designed to collect data from information security administrators. Based on the quantitative and descriptive approach of this study, the questionnaire consisted of closed-ended questions. The following six types of closed-ended questions criteria are identified by Saunders *et al.* (2012) which were used in the survey of this study:

- Define questions that offer the respondent a range of responses to select from.
- Define questions to allow a single response from a given set of categories.

- Rank questions as this will require the respondent to arrange items in rank order.

- Rating questions will be presented to respondents to gather and record data. The Likert rating scale will be used in the rating questions.

Questionnaires are generally used for descriptive or explanatory research. Gill and Johnson (2010) describe descriptive research as an approach that is used in attitude and opinion questionnaires, that enables the researcher to identify and describe the variability in dissimilar phenomena. With the introduction and usage of the Internet, web-based questionnaires have become an important tool to conduct surveys, as it has numerous advantages as outlined below (Braekman, Berete, Charafeddine, Demarest, Drieskens, Gisle, Molenberghs, Tafforeau, Van der Heyden & Van Hal, 2018). Moreover, web-based questionnaires normally produce higher data quality since survey logic and warning messages are built into the product in anticipation of missing and implausible answers. This study used a secured online web-based survey based on the advantages below outlined by Braekman *et al.* (2018):

- Costs for conducting web-based surveys are far lower than paper-based surveys

- The researcher saves time because there is not a requirement to physically follow up with survey participants. The researcher simply sends out electronic reminders.

- The researcher can reach a wider audience and is not limited by geographic constraints.

- Researchers can obtain quicker turnaround times since participants complete these surveys online at their leisure.

- These surveys allow the researcher to similarly collect para data.

Data for this study were collected using a secure web-based survey. Gang and Ravichandran, (2015) support the usage of a web-based survey and states that it has psychometric qualities similar to those of collecting physical data. Web-based surveys also have several associated disadvantages; for example, participants may alternatively lack the knowledge to answer the relevant questions (Gravetter & Forzano, 2012). Standardised questionnaires rarely capture what is important to some participants, especially when considering experiences, attitudes, orientations, and circumstances.

Braekman *et al.* (2018) also identify the deficiencies of surveys:

- They do not deal with social life given that the researcher fails to develop an understanding of the present situation in which participants encounter themselves.
- Modifying the survey during the research investigation is difficult, even though the research becomes aware of new associations or constructs.

Descriptive research is a quantitative research method that attempts to collect quantifiable information for statistical analysis of the census. It is a popular market research tool that allows us to collect and describe the demographic segment's nature (Bhandari, 2020). The survey used for this study was presented to all respondents in English. The researcher designed a structured web-based questionnaire hosted securely by SurveyMonkey, which is an online survey-developed, cloud-based software-survey tool; see appendix A. The survey was administered using *electronic mail* and *Linked-in* to collect the primary data for this study.

The survey questionnaire was self-administered and presented to participants through the Internet employing personalised e-mail and Linked-in addresses. Prior to participation, the potential respondents were offered an opportunity via electronic mail to ask questions and also confirm their willingness to participate in the survey. The participants were offered an opportunity to reject the opportunity to participate in the survey. A dedicated e-mail address was used for this study so that participants could respond, to reinforce the legitimacy of the research, whilst providing a central point of contact for the participants. This e-mail address was monitored by the researcher to be aware and act on issues that the participants might experience.

The questionnaire was defined with the input collected from the literature review and consisted of 42 close-ended questions. The questionnaire was narrated using Microsoft Word processing and uploaded to a web-based online survey tool, being

SurveyMonkey. The Likert scale formed part of the questionnaire, being the most widely used method to scale responses in survey research, although there are other types of rating scales (Debasis, 2012). The introduction content of the survey included the name of the researcher, the aim of the survey, assurance that the respondents' enterprises will be mentioned in any way, and that the survey was completely confidential.

The survey header was presented with the heading *(Cybersecurity and Governance Framework of Information Systems in the South African Mining Industry)* and included an introduction survey message from the researcher (See *Annexure A*). The questionnaire was designed with the input gathered from the primary and secondary objectives. Furthermore, the questionnaire was designed, and divided into five sections as follows:

Consent letter: All respondents were sent a consent letter to request permission to conduct the survey. The letter invited participants to the research survey and outlined the aim of the survey. Moreover, it indicated that all information collected would be treated confidentially. The respondents were also assured that the research would not reveal any sensitive information attributed to their enterprises (See *Annexure B*).

Introduction Page: This category introduced the survey and welcomed the respondents to the online survey. The welcome page to the survey also indicates that the survey will take no more than 15 minutes to complete.

Page 1: Demographical and geographical information gathering of respondents: The section includes questions 1 to 7. The category focused on determining the geographical and demographical information of the mining enterprises, web-browsing software, and the antivirus solution that these enterprises have in place.

Page 2: To determine IT governance practices used by enterprises in the mining industry: This section includes questions 8 to 18. These questions aimed establish what IT governance practices do for enterprises to protect their information systems from being compromised.

Page 3: To identify the types of access control processes put in place by enterprises in the mining industry. This section includes questions 19 to 30. These questions aimed to determine what access-control processes are being used by enterprises to protect information systems from unauthorised access.

Page 4: To establish if information security policies are implemented within South African mining enterprises. This section includes questions 31 to 34. These questions aimed to establish if enterprises have information security policies in place, to improve their security and risk management programmes.

Page 5: To analyse auditable control measures used by enterprises in the mining industry. This section includes questions 35 to 42. These questions aimed to establish what access control processes enterprises have in place to protect information systems from unauthorised access.

Finalise: The step of ending the gathering of data involved thanking respondents for their participation. This was accomplished via a posting on the last page of the survey after the "Done" button was clicked. The survey was then submitted, and all data was captured. The Likert scale was used as part of the questionnaire, whilst some questions presented respondents to select from default close-ended questions.

4.7 POPULATION

Information security administrators in the South African mining industry were defined as the population for this study. Saunders *et al.* (2012) define a population "as the complete set of cases or group members upon which a research study will be based". The market capitalisation of listed mining enterprises and its Information, Communication and Technology infrastructure footprint in South Africa was the determining parameter in the research population and census. The mining enterprises included in this study are those enterprises that align to the following criteria: a) listed on the Johannesburg Stock Exchange (JSE); b) are members of the Chamber of Mines of South Africa (COMSA); and c) have legal mining licences with the Department of Mineral Resources (DMR). The aggregate number of enterprises in the South African mining industry consists of 62 listed mining enterprises, with a combined market capitalisation value of approximately R791 billion.

4.7.1 Census

This study used the census method with the collection of data from the research participants. Census and sampling are two methods of collecting survey data about the population that will be used when doing research (Surbhi, 2017). According to Hair *et al.* (2011), census refers to the quantitative research method, in which all members of the population are enumerated. In a census, data about all participating units (e.g. people or households) are collected from the population (Lanjouw, 2016).

Moreover, the census method gather information from every entity in a population (Lanjouw, 2016). Census and surveys both involve data collection, however they differ in their objectives and practice. This study used census as a suitable method to collect survey data from participants. The census data collection method was based on the small research population group at the mining enterprises. Census implies complete enumeration of the study participants, whilst sampling surveys connotes enumeration of the subgroup of elements chosen for participation.

These two survey methods are often contrasted with each other. The table below summarises the differences between census and sampling survey. Census is a well-organised procedure of gathering, recording, and analysing information about the population (Cohen *et al.,* 2011; Hair *et al.,* 2011). The enumeration of a census considers the entire population. Thus, based on the census research method, the entire population group was used to collect research data which relates to this study.

Table 4.3 below summarises the differences between census and sampling surveys.

Basis for comparison	Census
Meaning	A systematic method that collects and records the data about the members of the population is called Census.
Enumeration	Complete
Time required	It is a time-consuming process.
Cost	Expensive method
Appropriate for:	Population of heterogeneous nature.
Applicability	Census method is effective for a heterogeneous population
Enquiry nature	The nature of enquiry is extensive in its ambit
Organising and monitoring	Due to the vastness of the census population, organising and monitoring is difficult
Verification	The results borne out of verification cannot be verified
Accuracy and reliability	Given the extensive method, the results are closer to accuracy and have greater reliability

Source: Adopted from Surbhi, 2017, *Difference between census and sampling surveys*

Sampling is a widely used method that involves a statistical analysis of an already determined number of members that is derived from a larger set of the population (Turner, 2019). Moreover, this method is used for statistical testing where it is not possible to consider all members as the population size is very large.

Census was thus the preferred method to collect research data from the entire population group for this study (Surbhi, 2017). The usage of the census method was based on the constraints and limitations of the sampling method that was presented to the researcher when data was collected to achieve the primary research objective. For this study, the emphasis remained on the total number of enterprises in the South African mining industry as units of interest. This study reached out to individuals with knowledge as well as practical experience of Information Security in the South African mining industry. For this reason, an information security administrator representing each of the 62 mining enterprises participated in this study.

The questionnaire was designed to gather auditable information security information. The contact details of these mining enterprises were drawn from their respective enterprise Internet websites and annual company reports. The initial access provided the researcher with a way of obtaining the contact details of the information security administrators of the participating mining enterprises. Further contact details were gathered from information security interest groups, information security peer-review forums, and technical and professional community user groups.

In a census, data about all participating units (e.g. people or households) are collected of the population (Lanjouw, 2016. Thus, a census gather information from every entity in a population.

4.8 RESPONSE RATE

Response rate is the number of completed surveys by suitable participants (Agustini, 2018). Moreover, according to Agustini (2018), response rates essentially consist of two aspects based on the interaction with the participants: contacting the participants and gaining their cooperation which involves different strategies. However, if the wrong participants are contacted without their cooperation it can result in a low response rate (Agustini, 2018). According to Blair, Czaja and Blair (2013), the response rate is extremely important to the credibility of the research results of a survey. Blair *et al.* (2013) state that a low response rate may decrease the statistical accuracy of the collected data and weaken the reliability of the results.

Floyd and Fowler (2013) argue against this view by stating that surveys with a low response rate, sometimes as low as 20%, could yield more accurate results than surveys with response rates of 60% to 70%. The data captured from all 37 respondents from a population group of 62 were analysed with the aid of a secured online web-based survey tool. This survey was thus completed by 59.67% of the census group.

4.9 DATA COLLECTION, CAPTURING AND ANALYSIS

4.9.1 Data collection

This study quantified data and generalised the results from the population from an information security administrator, who represented each of the 62 mining enterprises in the South African mining industry (Van der Stroep & Johnson, 2010). This study used a questionnaire to collect and generate statistical numerical data (Hair *et al.,* 2011). Gang and Ravichandran, (2015) contend that employing a web-based survey has psychometric qualities similar to those of collecting physical data. A dedicated e-mail address was used for this study to reinforce the legitimacy of the research, while also providing a central e-mail address for respondents to have a single point of contact. This e-mail address was monitored by the researcher to be aware of issues that the respondents might experience.

The questionnaire was defined with the inputs collected from the literature review and consisted of 42 questions. Multiple attempts were made to improve the response rate of this study, by sending follow-up emails, contacting respondents through Linked-in, follow-up attempts with telephonic encouragement. All respondents were thanked for their participation as part of the survey briefing. Enterprises were contacted telephonically and via electronic mail to introduce the research and to invite and encourage their participation in this study. The questionnaire was sent to an information security administrator representing each of the 62 mining enterprises were identified in the census.

The criteria for enterprises to participate in this survey was drawn from listed enterprises on the “Johannesburg Stock Exchange” (JSE), and members of the “Chamber of Mines of South Africa” (COMSA) that have legal mining licences with the “Department of Mineral Resources” (DMR). Secondary data which Myers (2013) describes as any data that has been previously published, was collected from books, peer-reviewed journals, information-security conference proceedings, newspaper articles, credible Internet websites, Special Interest Groups (SIG) on information security, institutes that research information security, and relevant documents from mining enterprises in South Africa.

4.9.2 Questionnaire design

This quantitative study employed and adapted a self-administered structured questionnaire to collect data from the selected participants. The questionnaire was narrated using Microsoft Word and uploaded to a secured web-based online survey portal. The questionnaire survey tool used the Likert scale with close-ended questions which were mainly used in the information security section of the questionnaire. Moreover, the Likert scale formed part of the questionnaire, being the most widely used method to scale responses in survey research, although there are other types of rating scales (Debasis, 2012). However, the questionnaire also had multiple-choice questions to determine the demographics of the mining operations as well as determining various types of information security technology strategies.

4.9.3 Data capturing

This study made use of a survey as its data collection method and research strategy. This strategy helps in establishing relationships amongst constructs. This is supported by Saunders *et al.* (2019) who, contend that deductive research works well with the survey research approach. The questionnaire used for the survey in this study was secure, online web-based, designed to be concise, unbiased, unambiguous with clear instructions on how to navigate through the survey. The researcher subscribed to Survey Monkey on a six-month agreement that enabled the questionnaire to be securely uploaded, maintained, and administered by Survey Monkey. For this study, informed consent, voluntary participation was deemed important.

The participants were not forced nor coerced into their participation. The researcher ensured the confidentiality and anonymity of the participants as well as that of their mining enterprises. Critical care was taken with the information provided by the participants not to be disclosed to other parties except to the independent statistician. To ensure anonymity and confidentiality, responses from participants were treated confidentially and all responses were only used for this study. Any information used in this study finding does not signify any person involved in the study voluntarily after an agreement to participate was maintained. In the study, the researcher secured permission from Unisa to conduct this study – see Appendix D.

The participants who were invited to participate were advised of the expected duration of the survey. The participants were offered an opportunity to either accept or reject to participate in the survey. According to Bell (2010) and Hair *et al.* (2011), primary data is gathered directly from sources of evidence. The questionnaire was web-based and securely hosted by Survey Monkey (www.surveymonkey.com), which is a web-based survey enterprise that facilitates online surveys. The webpage allowed the respondents to capture their responses online which was stored in a database and the results can be viewed online or in real-time. Once the closing survey submission date was reached, the data was securely extracted using interactive software-reporting tools that Survey Monkey provides as a service.

4.9.4 Data analysis

The data analysis in this study was quantitative and descriptive as it references the basic transformation of research data, which defines the essential characteristics such as tendency, distribution, and variability (Zikmund *et al.,* 2013). Descriptive statistics summarise the data attained for a collection of individual units of analysis (Welman, Kruger & Mitchell, 2009; Weiers, 2008). The mean was a measure used to describe the location of a distribution (central tendency). The mean is the average number attained. The median is the mid-point of distribution and is known as the 50th percentile (Weiers, 2008).

The mode is the value of the variable, which occurs most often (Resnik, 2011). Correlation between variables was also be established. Quantitative research makes use of numerical statistical analysis which allows researchers to either reject the hypotheses or to determine the effect size (Creswell, 2014). However, whilst analysing the data in this study, it involved addressing each one of the research questions or hypotheses individually. Creswell (2014) identifies two types of statistical analysis, being: descriptive and inferential. However, Creswell (2014) states that with descriptive analysis, the researcher needs descriptive statistics that indicate central tendencies in the data mean, the spread of scores (variance, standard deviation, and range), or a comparison of how one score relates to others (z-scores, percentile rank).

Moreover, analysing the data might identify the variables: independent, dependent, control, or mediating.

4.10 VALIDITY AND RELIABILITY

This study used Cronbach’s alpha to measure internal consistency reliability. The reliability of a measurement instrument is the degree to which it produces consistent results when the measurable characteristic does not change (Quinlan, 2011). Rubin and Babbie (2011) define reliability as a “matter of whether a particular technique, applied repeatedly to the same object, would yield the same result each time”. Moreover, the Cronbach alpha test was used to test the reliability and consistency of the Likert scale questions of the survey. Cronbach’s alpha is the most common way of assessing reliability (Van der Stoep & Johnson, 2009).

Devellis (2006) define Cronbach’s alpha as “an average of all the possible split-half reliability estimates of an instrument”. The coefficient generally varies from 0 to 1 and a value of 0.6 or less generally indicates unsatisfactory internal consistency reliability (Malhotra, 2004). This measure is supported by Rubin and Babbie, (2011) who state that Cronbach’s alpha is used to assess if the various items that confirm the measure, are internally consistent. The validity and reliability of the research instrument were tested by using exploratory factor analysis (EFA). The response rate was also discussed and the ethical considerations that were aligned with this study are explained.

Exploratory Factor Analysis (EFA) is a statistical technique that is used to reduce data to a smaller set of summary variables to explore the underlining theoretical structure of the phenomena (Sing, 2014). Moreover, it is used to identify the structure of the relationship between the variables and the respondent. EFA is a statistical technique in this study, which is used to reduce data to a smaller set of summary variables and to explore the underlining theoretical structure of the phenomena to address the primary and secondary objectives, which is to investigate auditable information security control measures and policies in the South African mining industry (Tavakol & Dennick, 2011).

Furthermore, EFA is used to identify the structure of the relationship between the variable and the respondent. Since this study is descriptive, during the analysis phase of the survey data, the EFA technique was used for validity testing. This was done to determine whether the items loaded on their respective factors. Moreover, one of the advantages of EFA is that it identified hidden factors that may or may not be apparent from the questionnaire (Tsironis, Gotzamani & Mastos, 2017). Shekharan and Bougie (2010) state that a very important aspect of factor analysis is the Kaiser-Meyer-Olkin Measure of Sampling Adequacy (KMO) and Bartlett's Test of Sphericity. The KMO was used as a statistic in this study to see if the proportion of variance in the variables is being caused by underlying factors (Shekharan & Bougie, 2010).

Moreover, the KMO in this study was used to check if the factor analysis is useful for the research data. The scree plot is used in multivariate statistics which is a line plot of the eigenvalues of factors or principal components in an analysis (Ledesma, Valero-Mora & Macbeth, 2015). The scree plot was used in this study to determine the number of factors to retain in the EFA or principal components to keep in the principal component analysis (PCA). The rotation component matrix-assisted the analysis of this study to determine what the components represent in a correlated matrix (Sheth, 2018). Moreover, the rotated component matrix is at times referred to as the loadings which is the key output of principal components analysis (PCA) which was used in this study as it contained estimates of the correlations between each of the variables and the estimated components.

The rotation component matrix also provided clarity to this study by indicating which variables measured which factors. The total variance is the analysis of variance and regression analysis, the variability that is because of treatment (true variance) plus the Variability that is due to error (error variance) (Sheth, 2018). Moreover, the total variance can be subdivided into systematic variance and error variance. Thus as part of the validity and reliability phase, this study aligned with total variance. Systematic variance refers to the part of the total variance that can predictably be related to the variables that the researcher examines. However, an error is the result when the behaviour of participants is influenced by variables that the researcher does not examine.

4.11 ETHICAL CONSIDERATION

This study adhered to the Policy on Research Ethics of the University of South Africa (UNISA), which is the Policy on research ethics contents of September 2016. Ethical clearance was obtained from Unisa which is attached as *Appendix F*. Creswell and Plano Clark (2011) support the research policy by UNISA by stating that, the conduct of research is likely to be guided by the university's code of ethics or ethical guidelines. Respondents were formally informed that their participation in this survey is voluntary, and they can decide whether to participate or decline. They were advised of the possible risks as well as the benefits of the research and that their participation is free. The purpose of the study and an explanation of the selection process of the participants and the process and procedures that were followed was shared with participants.

Participants in this study were not compensated. There was no foreseeable harm, discomfort, and invasion of privacy to participants of this study. The participants were informed that the methods used were to protect anonymity and confidentiality. An informed consent form was issued to the participants to gain their consent to participate in the research. Participants were advised that participation in this survey is voluntary and that there are no penalties for refusal to participate (Fouka & Mantzorou, 2011). Participants were further advised that about their freedom to withdraw from participating in the research at any given time before submitting the completed questionnaire (Fouka & Mantzorou, 2011).

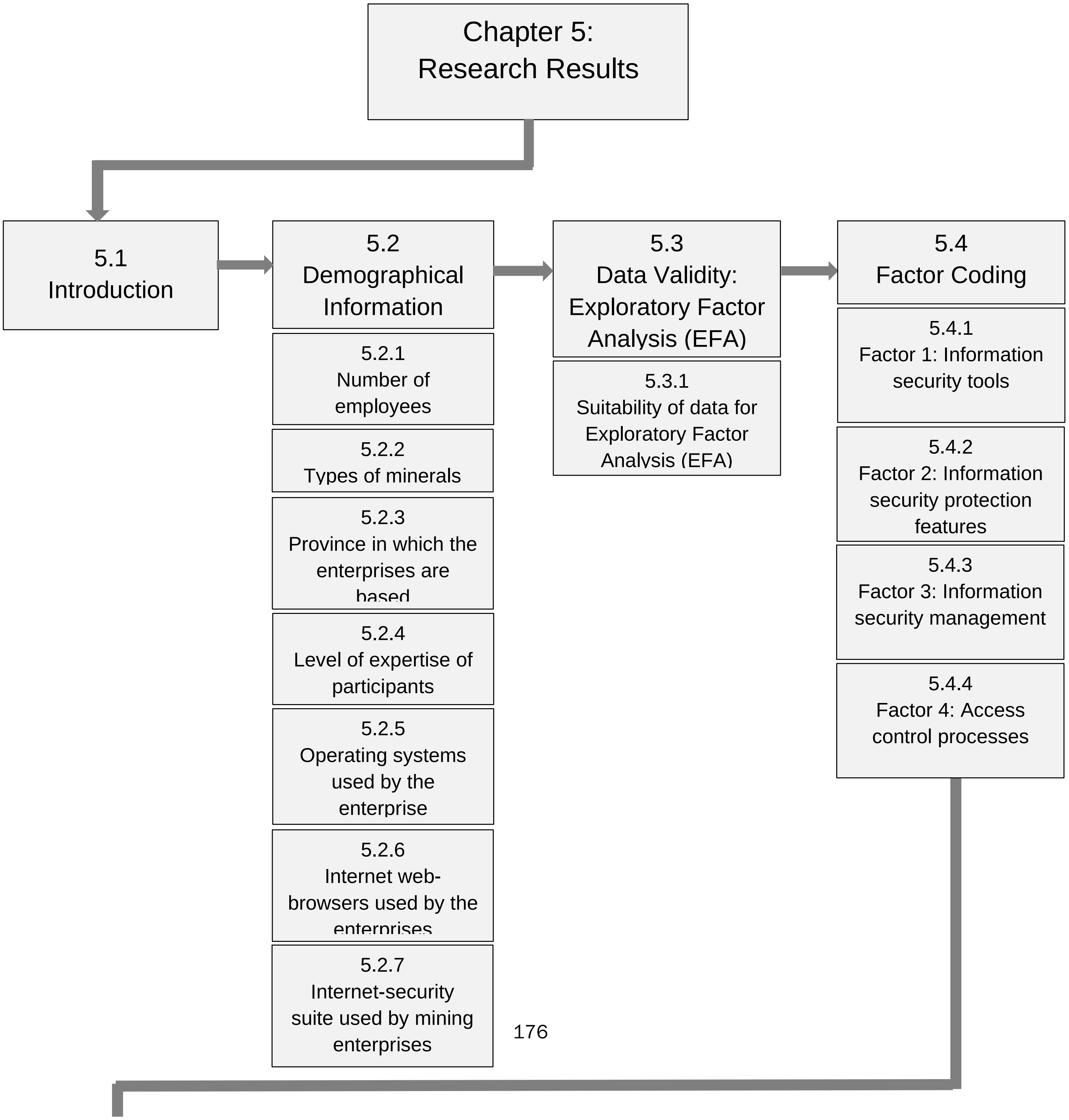
4.12 CHAPTER SUMMARY

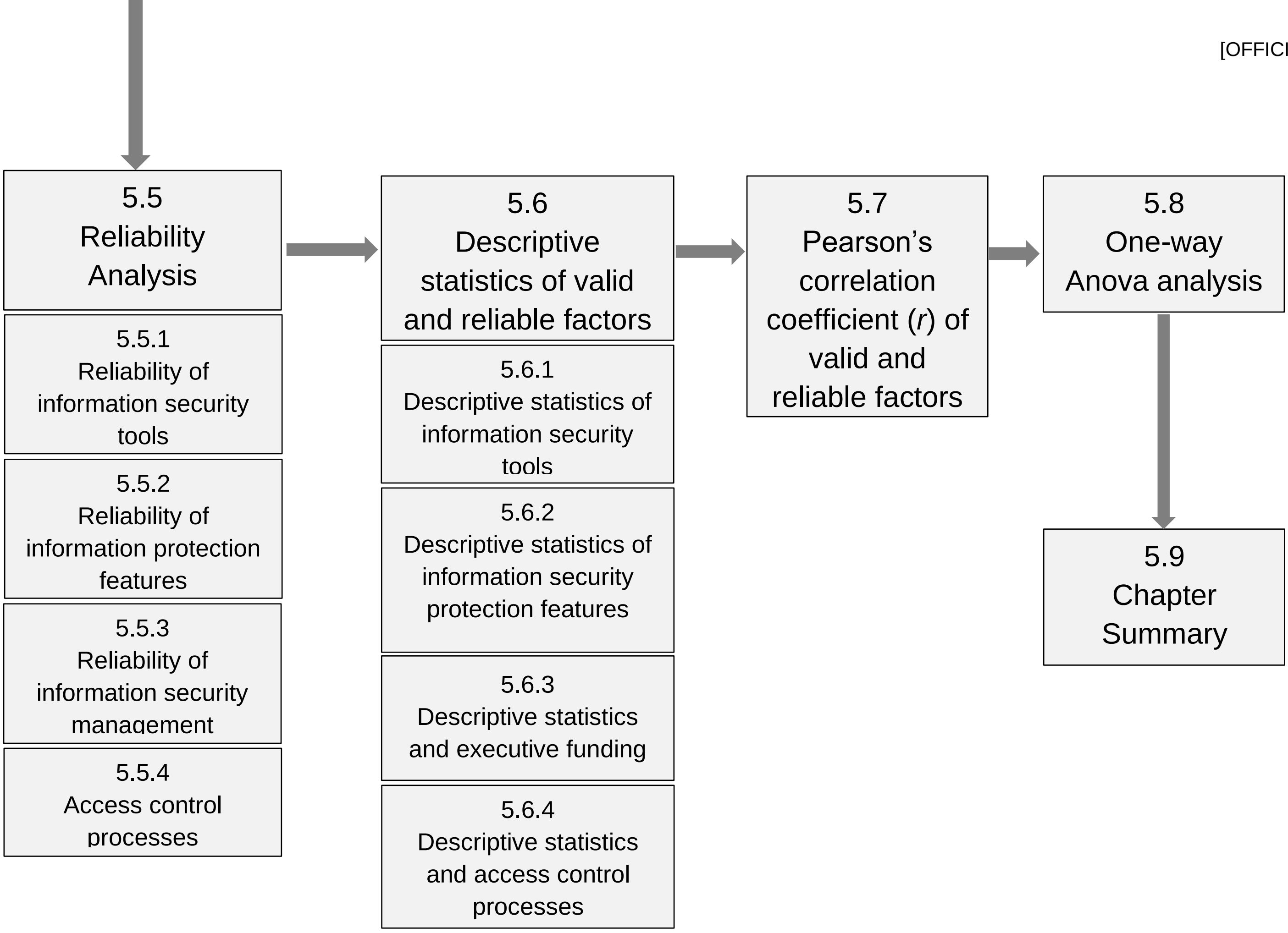
This chapter explained how the research was conducted and the methodology used. The research design, approach, and philosophy were defined and discussed in this chapter. The discussion started with the research philosophy section and outlined the interpretivism and positivism research philosophies that were used to underpin the discussion. A structured, self-administered online secured web-based questionnaire was defined and designed to collect data from information security administrators.

For this study, the focus remained on the total number of South African enterprises in the mining industry as units of interest. The chapter also discussed how the data was collected, captured, and analysed. The validity and reliability of the study instrument were tested by using exploratory factor analysis (EFA). The response rate was also discussed and the ethical considerations that were aligned with this study were explained. The next chapter being (Chapter 5) reports and analyses and the results of this study.

CHAPTER 5: RESEARCH RESULTS

This chapter discusses the research results and methodology used to conclude the study findings. The chapter reviews the demographical information of the South African mining industry. Furthermore, it analyses and validates the data by using exploratory factor analysis, factor coding and reliability analysis. The chapter also discusses the descriptive statistics of reliable factors and Pearson’s correlations of valid and reliable factors. It concludes by providing a detailed analysis of one-way Anova analysis.


Chapter 5:
Research Results
5.1
Introduction
5.2
Demographical Information
5.2.1
Number of employees
5.2.2
Types of minerals
5.2.3
Province in which the enterprises are based
5.2.4
Level of expertise of participants
5.2.5
Operating systems used by the enterprise
5.2.6
Internet web-browsers used by the enterprises
5.2.7
Internet-security suite used by mining enterprises
5.3
Data Validity: Exploratory Factor Analysis (EFA)
5.3.1
Suitability of data for Exploratory Factor Analysis (EFA)
5.4
Factor Coding
5.4.1
Factor 1: Information security tools
5.4.2
Factor 2: Information security protection features
5.4.3
Factor 3: Information security management
5.4.4
Factor 4: Access control processes


5.5
Reliability Analysis
5.5.1
Reliability of information security tools
5.5.2
Reliability of information protection features
5.5.3
Reliability of information security management
5.5.4
Access control processes
5.6
Descriptive statistics of valid and reliable factors
5.6.1
Descriptive statistics of information security tools
5.6.2
Descriptive statistics of information security protection features
5.6.3
Descriptive statistics and executive funding
5.6.4
Descriptive statistics and access control processes
5.7
Pearson's correlation coefficient (r) of valid and reliable factors
5.8
One-way Anova analysis
5.9
Chapter Summary

5.1 INTRODUCTION

Research results are discussed with references to the objectives and questions of the study. Moreover, there is continued reference to the questions as they appear in the online survey as per the SurveyMonkey platform.

The following results are discussed in this chapter:

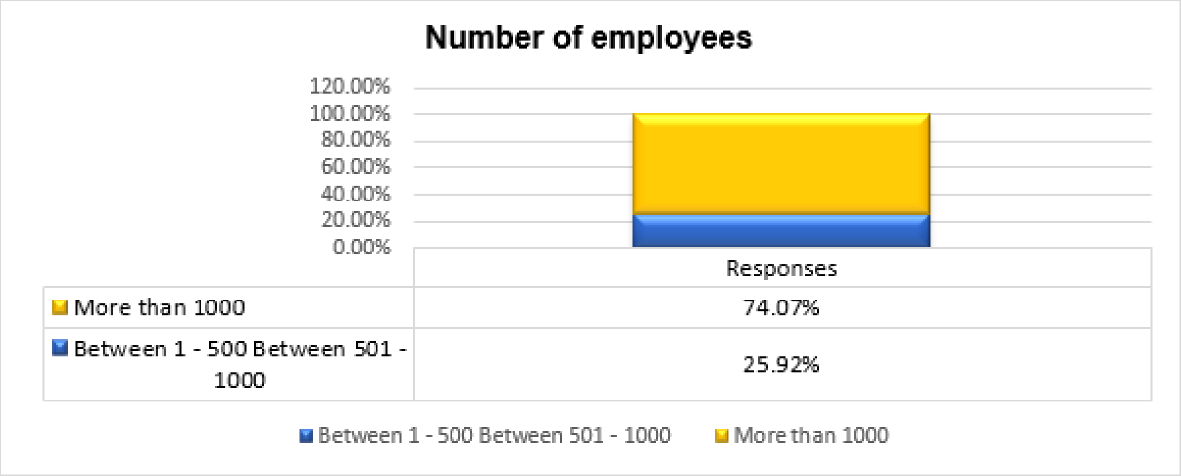
- Exploratory Factor Analysis (EFA) results to determine the factorial structure as the validation of the research instrument.
- Cronbach Alpha test results to establish the internal reliability of the factors.
- The results are then presented after the descriptive statistics of the valid and reliable variables are analysed.
- ANOVA test results to establish the significant differences among the information security requirements; and
- The chapter ends using correlation analysis and analysis of the structured equation models.

5.2 DEMOGRAPHICAL INFORMATION

The aim of questions 1 to 7 of the questionnaire was to determine the geographical, demographical, expertise of participants; web-browsing, operating system software and antivirus solutions that are used by the enterprises who participated in this study. These questions were designed to establish how mining enterprises in South Africa with different characteristics responded to questions that answered the main objectives of the study. The findings narrate the research questions that guided the study. This study used frequency distribution and percentages to describe the demographics.

5.2.1 Number of employees

The aim of question 1 was to establish the number of employees employed in the enterprises that the participants represent. The scales used were as follows: 1-500, 501-1000 and more than 1000. The results indicate that 74.07% of the enterprises employ more than 1000 employees, whilst 22.22% employ less than 500 employees; and, 3.70%; of these enterprises employ between 501 and 1000 employees. This implies that mining enterprises in South Africa employ a large number of employees. Figure 5.1 indicates the number of employees employed by the mining enterprises.



	Responses
More than 1000	74.07%
Between 1 - 500 Between 501 - 1000	25.92%

Figure 5.1: Number of employees

5.2.2 Types of minerals

The aim of question 2 was to establish the minerals being mined by South African mining enterprises. The results indicate that the minerals being mined by the enterprises were as follows: Platinum (32.43%), iron ore (16.22%), gold (13.51%), coal and copper (10.81%), diamonds (5.41%), and nickel, zinc, lead (2.70%). Thus, the most popular mineral being mined in South Africa is platinum. Figure 5.2 indicates the minerals being mined by the mining enterprises.

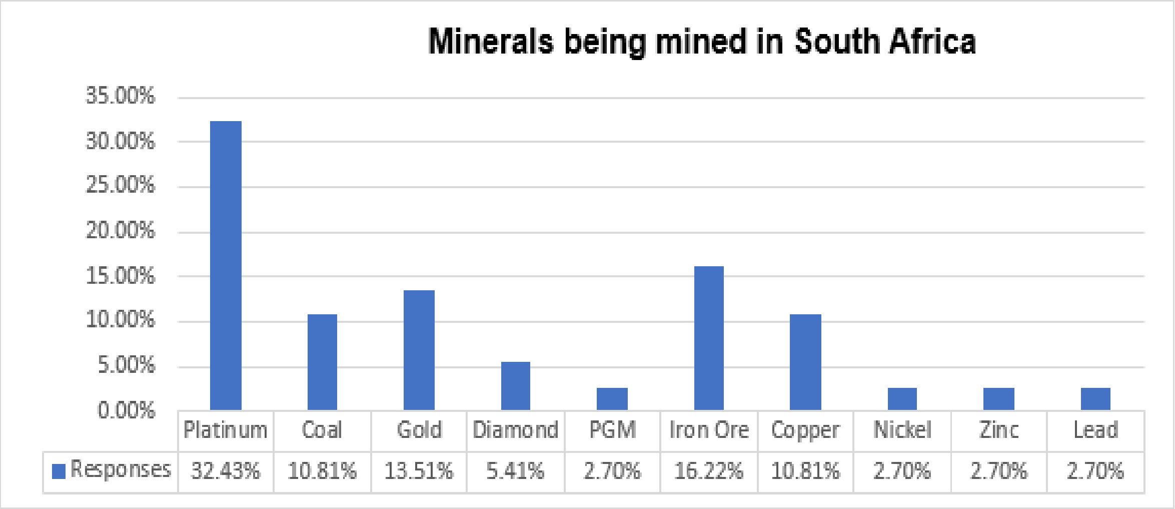


Figure 5.2: Minerals being mined in South Africa

5.2.3 Province in which the enterprises are based

The aim of question 3 was to determine in which provinces were mining enterprises based. All nine (9) South African provinces were presented to the participants as options. The results indicate that mining operations or their headquarters are based in Gauteng (41%), Limpopo (38%), North-West (16%), and Northern Cape (5%). Thus, most mining operations are based in Gauteng and Limpopo. Figure 5.3 indicates the South African provinces that have mining operations.

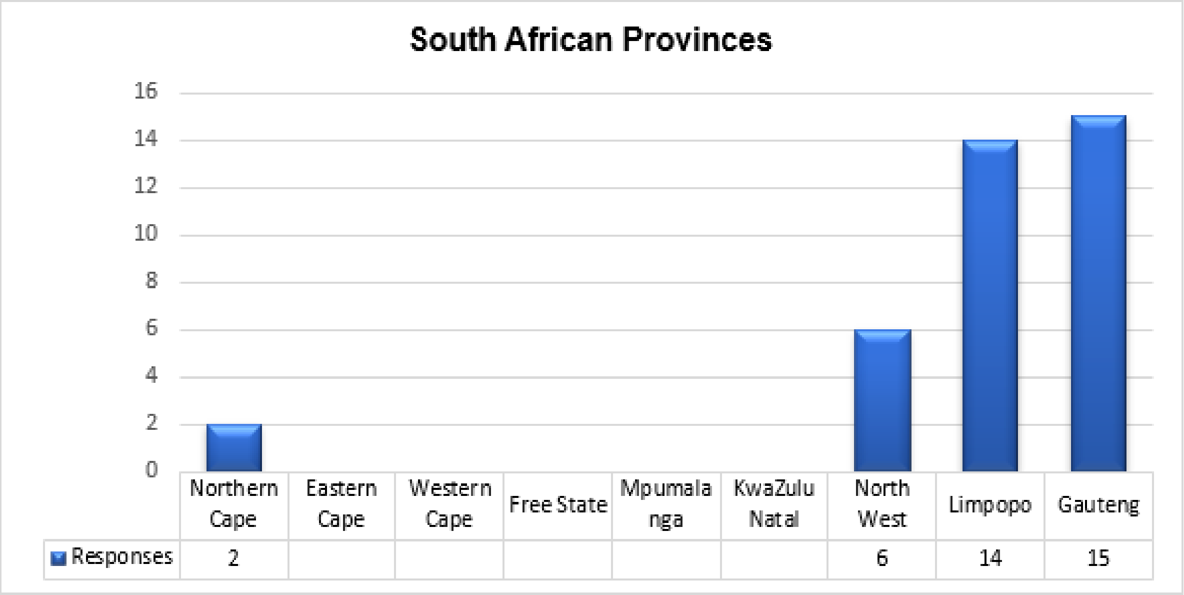


Figure 5.3: Mining operations in different South African Provinces

5.2.4 Level of expertise of participants

The aim of question 4 was to determine the level of expertise of the participants. The results indicate that 59% of the participants were ICT professionals, 22% of the participants were Information Security experts, 11% of the participants were ICT administrators and 8% do not specialise in ICT security but have ICT expertise. Thus, most of the participants were ICT security professionals. Figure 5.4 indicates the level of expertise of the participants.

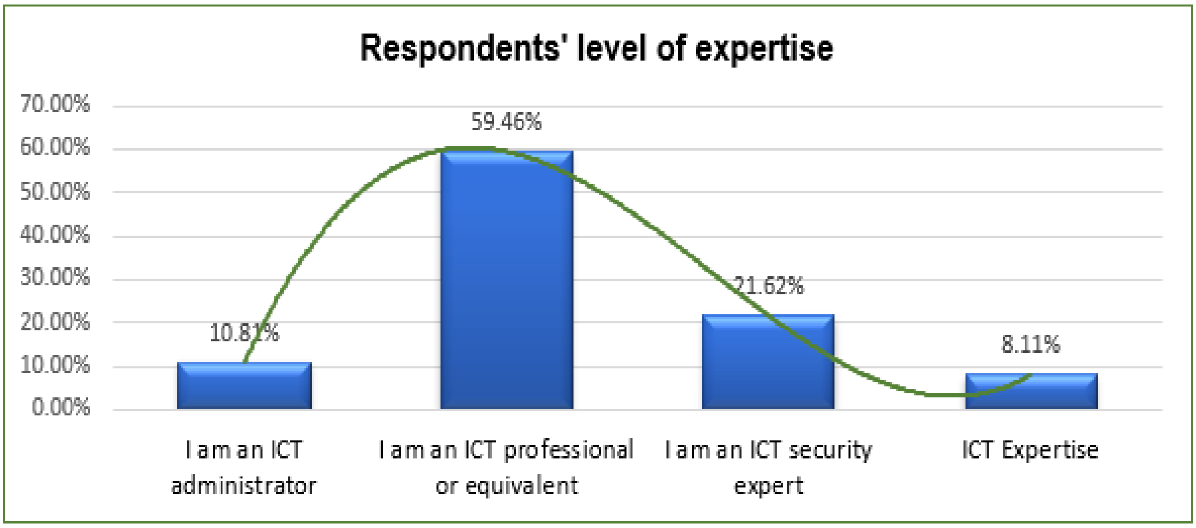


Figure 5.4: Respondents' level of expertise

5.2.5 Operating systems used by the enterprise

The aim of question 5 was to establish the Operating System (OS) that enterprises use on their computer workstations. The result indicates that the Microsoft OS, Office 365 was used by 27% of the enterprises, 22% of the enterprises used Windows 7, which is the previous version of the Microsoft OS suite, 19% of the enterprises used the Windows 8 suite, whilst 13% of the enterprises used Windows 10. It was further ascertained that 11% of the enterprises used Apple Mac operating system and does not use the popular Microsoft operating system, whilst 8% of the enterprises either used Linux, FreeBSD, SunOS, OS2 or UNIX. Figure 5.5 indicate the operating systems used by mining enterprises.

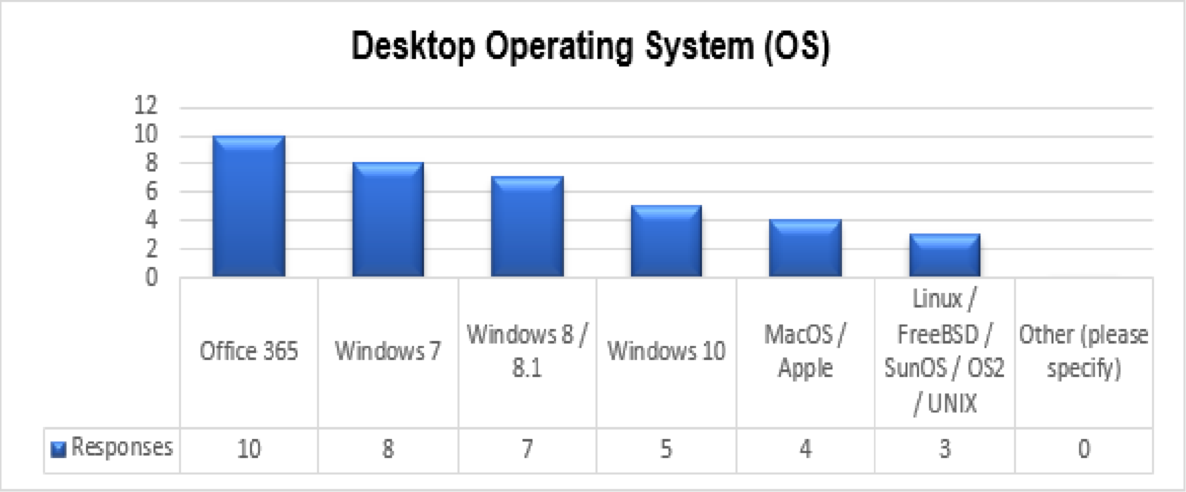


Figure 5.5: Workstation Operating System used by enterprises

5.2.6 Internet web-browsers used by the enterprises

The aim of question 6 was to ascertain which Internet web-browsers are used by enterprises on their workstations. This was a multiple-choice question, which allowed the participants to select more than one internet web browser. The results indicate that Microsoft Internet Explorer is used by twenty-nine (29) of the enterprises, Google Chrome is used by twenty-six (26), Microsoft Edge is used by six (6), and Mozilla Firefox and Apple Safari is used by one (1) and two (2) of the enterprises respectively.

Responses to this question indicate that both Google Chrome and Internet Explorer are used by eighteen (18) enterprises, whilst four (4) enterprises use three Internet web-explorers, Google Chrome, Internet Explorer, and Microsoft Edge. The results also indicate that none of the participants uses Opera web browser or any other web-browsing software. Figure 5.6 indicates the Internet web-browsers used by the mining enterprises.

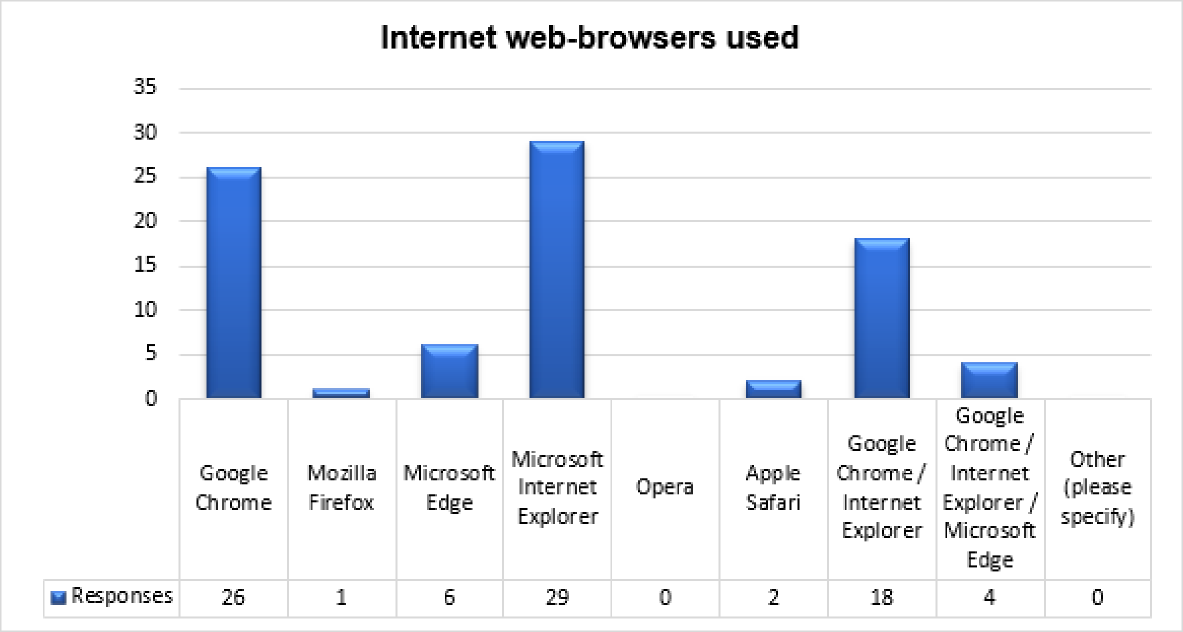


Figure 5.6: Internet web-browsers used

5.2.7 Internet-security suite used by mining enterprises

The aim of question seven (7) was to determine if an Internet security suite offers more security than the same vendors' antivirus-only products. The Likert scale was used in this question, being: Strongly agree, somewhat agree, neither agree or disagree, disagree, and strongly disagree. The graph below (Figure 5.7) shows the frequencies for each statement according to the Likert scale values for the data collected.

The question revealed that 23% of participants somewhat agree, 16% of participants strongly agree, 10% neither agree nor disagree, 8% disagree, whilst 2% strongly disagree with the statement. It can thus be stated that most of the participants agree that an Internet security suite offers more information security than the same vendors' antivirus-only products. Figure 5.7 shows the frequencies for the statements with the highest mean values.

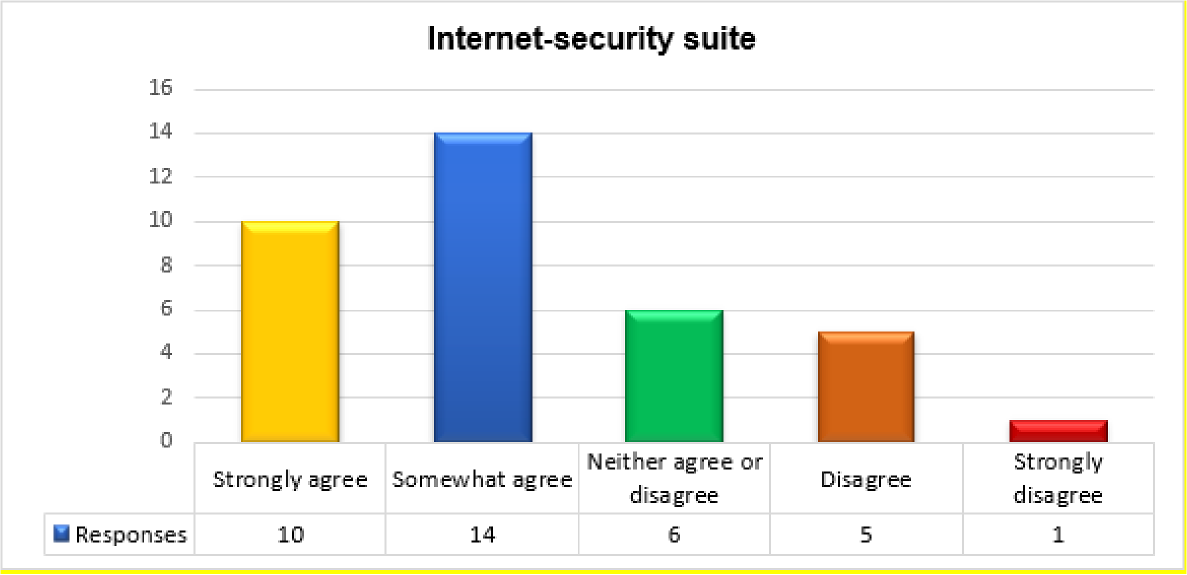


Figure 5.7: Internet-security suite

5.3 DATA VALIDITY: EXPLORATORY FACTOR ANALYSIS

This section analyses the validity of the collected data. Singh (2014) states that Exploratory Factor Analysis (EFA) is long associated with construct validity, which makes it a useful tool to evaluate score validity. The factor analysis analysed the validity of the collected data. Factor analysis functions on the concept that measurable and observable variables can be reduced to fewer latent variables which share a common variance and are unobservable, which is known as reducing dimensionality (Bartholomew, Knott & Moustaki, 2011). EFA is a statistical technique in this study, which was used to reduce data to a smaller set of summary variables and to explore the underlining theoretical structure of the phenomena to address the primary and secondary objectives, which is to investigate auditable information security control measures and policies in the South African mining industry (Tavakol & Dennick, 2011).

Furthermore, EFA is used to identify the structure of the relationship between the variable and the respondent. Reliability and validity are two extremely important and fundamental features when evaluating any measurement instrument to conclude and present excellent research (Singh, 2014). The validity and reliability were statistically tested by computing the KMO and Bartlett tests, using exploratory factor analysis, descriptive statistics, Cronbach's alpha, and confirmatory factor analysis. Reliability is referred to as the stability of findings, whereas validity represents the truthfulness of findings (Altheide & Johnson, 1994). The evidence of validity and reliability is fundamentally important to guarantee the integrity and quality of a measurement instrument (Haynes *et al.,* 2017).

5.3.1 Suitability of data for Exploratory Factor Analysis

In the following sections, the EFA will be discussed as well as determining the underlying factors of the questionnaire. The data was collected and analysed statistically with the support of an independent qualified statistician. The Statistical Package for the Social Sciences (SPSS) software package was used to analyse the data statistically. To test the validity, the EFA statistical technique was employed to detect hidden structures and to enhance the interpretability of the data (Napitupulu, Kadar & Jati, 2017) and thus, determine to construct validity. Shekharan and Bougie (2010) state that a very important aspect of factor analysis is the Kaiser-Meyer-Olkin Measure of Sampling Adequacy (KMO) and Bartlett's Test of Sphericity.

The applicability of factor analysis was tested by using the Kaiser-Meyer-Olkin Measure of Sampling Adequacy (KMO measure) and Bartlett's Test of Sphericity. Both tests inveterate the applicability of factor analysis for both groups of variables (see Table 5.1). Moreover, it is a measure to check the sampling adequacy, which as stated by Shekharan and Bougie (2010) is to check the case to the variable ratio for the different analyses to be conducted. Moreover, Shekharan and Bougie (2010) further state that the range of the KMO falls between 0 to 1. To recommend the suitability of the factor analysis, Bartlett's Test of Sphericity must be less than 0.05 (Anastasiadou, 2011).

The Bartlett sphericity test, where the probability should be 0.05 or less, was statistically significant ($p < 0.004$) which meant that the variables were correlated highly enough to conduct the EFA for this study (Napitupulu *et al.,* 2017). High values, close to 1.0 generally indicate that factor analysis may be useful with the data collected (Anastasiadou, 2011). Moreover, if the value is less than 0.50, the results of the factor analysis might not be suitable. Bartlett's Test of Sphericity tests the hypothesis of the correlation matrix, which then indicates if variables are unrelated and therefore unsuitable for structure detection (Anastasiadou, 2011). Small values (less than 0.05) of the significance level indicate that factor analysis may be useful for the data (Anastasiadou, 2011).

The KMO measures the sampling adequacy, which should be greater than 0.5 for satisfactory factor analysis to proceed. The value of the KMO index in the current study is 0.568, which is more than the threshold of 0.5. Bartlett's Test of Sphericity is an indicator of the strength of the relationship among variables which is used to test if the null hypothesis of the variables in the population correlation matrix is uncorrelated. The observed significance level is 0.004, which is less than 0.05 (*p*<0.05). It was thus concluded that the strength of the relationship among variables is strong. The data for both acceptances was suitable to be used to extract component factors in this study. This is the most common rotation option (Napitupulu, Kadar & Jati, 2017).

The results of the Bartlett sphericity test are portrayed in Table 5-1. With this confirmation, the researcher was able to continue with the factor analysis and to identify the underlying factors. Table 5.1 indicates the Kaiser-Meyer-Olkin Measure of Sampling Adequacy and Bartlett’s Test.

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.568
Bartlett's Test of Sphericity	Approx. Chi-Square	147.461
	df	105
	Sig.	0.004

Table 5.1 KMO and Bartlett’s sphericity tests

Principal Component Analysis (PCA) is a variable reduction technique and is used when variables are highly correlated (Brems, 2017). Moreover, PCA reduces the number of observed variables to a smaller number of principal components. Brems, (2017) states that the total amount of variance in PCA is equal to the number of observed variables being analysed. In PCA, observed variables are standardised. Lever, Krzywinski and Altman (2017) state that PCA is a dimension-reduction tool that is used to reduce a large set of variables to a small set. However, the PCA must still contain most of the information that is in the large set. When PCA is used to describe the common variance, as factor analysis, the typical problem of determining how many components to retain arises (Brems, 2017).

However, the most used rule for PCA is to retain only factors corresponding to eigenvalues greater than the unit, Eigenvalue>1 rule. Moreover, Kaiser (1961) rationalised this rule in several ways. Alternative methods include using the Scree test (Cattell, 1966), by computing the percentage of variance extracted, or evaluating the patterns produced by varying the number of factors and rotated factors extracted. Three criteria were used in this study, namely Kaiser's criteria (Eigenvalue>1 rule); Scree test, and rotated factors. In determining the underlying factors for the variables, the initial Eigenvalues (see Table 5.3 below) and the scree plot (see Figure 5.8 below) were utilised as well as the cumulative percentage (Gerber & Hall, 2017).

The factors should have an Eigenvalue greater than one (Brems, 2017) to ensure internal consistency. For this study, the Eigenvalues for six factors were larger than 1 which suggested that six factors might be extracted (Treiblmaier & Filzmoser, 2010) with a cumulative Eigenvalue of 74.8%. Thus, this criterion is used in this study to extract valid factors. Six (6) strong factors with an eigenvalue greater than 1 were extracted from PCA. Though an eigenvalue of 1 represents the norm in the literature, a cut-off point of an eigenvalue of 1.4 was used to extract the factors in this study. Winsteps and PCA analysis use 1.4 as a cut-off value (Linacre, 2005). However, an eigenvalue is less than 1.4, is most likely to have noise or random error.

Table 5.3 indicates four (4) strong factors that have an eigenvalue greater than 1.4 which were extracted from the PCA. The scree plot in Figure 5.8 below shows all factors in this study. The scree plots the eigenvalue by the component number and confirms the factors above the eigenvalue of 1 (Ledesma, Valero-Mora & Macbeth, 2015). Furthermore, the first component will always have the highest total variance and the last component will always have the least. A Scree plot is a graph plotting the Eigenvalues on the y-axis and is used to determine the number of meaningful factors, whilst the number of factors is shown on the x-axis. The scree plot has a sharp descent, and it is at the turning point where the graph levels out which indicates the cut-off for the meaningful factors (Ledesma *et al.,* 2015).

The cut-off for the number of factors on the scree plot (see Figure 5.8) is four factors. Raiche *et al.* (2013) state that like Kaiser's rule, the Scree test is one of the most frequently used approaches for determining the number of components to retain. However, the graphical nature of the Scree test does not conclusively establish the number of components to retain. To avoid this issue, certain numerical solutions are being proposed; one solution is in the spirit of Cattell's work which deals with the scree part of the eigenvalues plot, and another solution that focuses on the elbow part of the Scree plot (Raiche *et al.,* 2013).

In Figure 5.8 the point where the slope of the curve is flattening is described as the "elbow" which specifies the number of factors that should be generated by the analysis. In this study, a cut-off of an eigenvalue of 1.4 provided four (4) factors that were retained for further analysis. For this study, the researcher chooses to keep the factors corresponding to eigenvalues above 1.4, which is the largest eigenvalues. These four eigenvalues account for 74.8% of the variance and were retained for further analysis. Figure 5.8 Indicates the scree plot for factor retention.

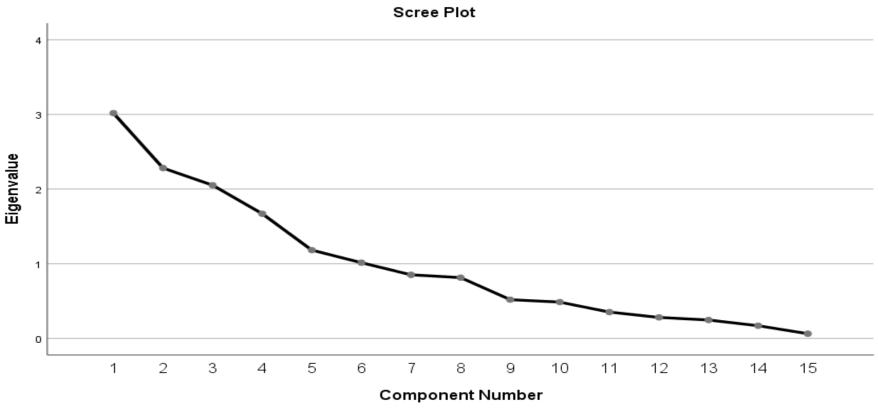


Figure 5.8 Scree plot for factor retention

Rotation is any of a variety of methods used to further analyse initial PCA/EFA results to form the pattern to load clearer, or more pronounced factor loadings (Brown, 2009). Moreover, this process is defined to reveal a simple structure. Brown (2009) further states that research makes rotation choices of either orthogonal or oblique varieties of the rotation methods. Most of the literature supports the use of oblique rotations, however, orthogonal rotations are still widely used and reported in studies using factor analysis (Costello & Osborne, 2005). Tabachnick and Fidell (2007) argue that perhaps a better way in deciding between orthogonal and oblique rotation is to define oblique rotation with the desired number of factors and identify the correlations among factors.

If the factor correlations are not driven by the data, then the solution remains orthogonal. The orthogonal varimax rotation was used in this study as it is commonly used in PCA for data reduction purposes (Fabrigar, Wegener, MacCullum & Strahan, 1999). Moreover, orthogonal varimax rotation is widely used and considered the best orthogonal rotation. It is further pointed out by Fabrigar *et al.* (1999) that the orthogonal varimax rotation method tries to maximise the variance of squared loadings on a factor to produce some high and low loadings for each factor and the variables which in this study is uncorrelated. Furthermore, Tabachnick and Fidell (2007) recommend using orthogonal rotations if the correlations between factors are low, however, if the factors are theoretically independent, then orthogonal rotation is acceptable.

This study aims to retain factors with more variable loading and eliminate factors with fewer variables loading. Schonrock-Adema, Heijne-Penninga, Van Hell and Cohen-Schotanus (2009) state that if an item is not significantly correlated to any of the factors, which is generally considered to be less than .30 as well as not providing a conceptually vital dimension to the measure, then the item should be removed. Moreover, a complex or a variable that loads on more than one factor should be removed if the cross-loading is greater than .40. After the weak items are removed, the data should be factored again without the presence of that item for a more refined solution (Pett, Lackey & Sullivan, 2003).

The interpretation of the factor further requires that each factor is sufficiently identified. This essentially means that a factor that contains at least three to five items with significant loadings to be considered a stable and solid factor (Costello & Osborne, 2005). A construct with fewer than three (3) items is generally weak and unstable, whilst five or more items are desirable and indicate a solid factor (Costello & Osborne 2005). Thus, this study considered factors with an eigenvalue≥1.4 and have a minimum of three (3) items loading at 0.4. Thus, only four (4) factors were extracted and retained for further analysis in this study.

Table 5.2 indicates the factors loading with their items.

Rotated Component Matrix[a]						
	Component					
	1	2	3	4	5	6
Q7				0.693		
Q13		0.746				
Q14		0.874				
Q15	0.859					
Q16	0.871					
Q17	0.607					
Q18		0.622				
Q24				0.543		
Q25			0.821			
Q26				0.712		
Q29			0.734			
Q32					0.491	
Q40					-0.837	
Q41						0.905
Q42			0.743		0.419	
Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.						
a. Rotation converged in 14 iterations.						

Table 5.2: Factors loading with items

The Eigenvalue of the four (4) extracted and retained factors ranges between 3.017 and 1.670. The percentage of variance for these factors ranges between 20.113 and 11.134. The rotated factor matrix provides clarity and simplicity of factor loadings (Osborne, 2015). Referring to Table 5.2 above, three (3) items were found to load on the first factor and labelled as Factor 1. Three (3) items were found to load on the second factor and labelled as Factor 2. Three (3) items were found to load on the third factor and labelled as Factor 3. Three (3) items were found to load on the fourth factor and labelled as Factor 4. Given the discussion of the constructs, the four factors also make theoretical sense.

Table 5.3 indicates the total variance explained with the initial eigenvalues, the extraction, and rotated factors.

Total variance explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3.017	20.113	20.113	3.017	20.113	20.113	2.509	16.729	16.729
2	2.282	15.212	35.325	2.282	15.212	35.325	2.156	14.372	31.101
3	2.051	13.676	49.002	2.051	13.676	49.002	2.038	13.586	44.688
4	1.670	11.134	60.136	1.670	11.134	60.136	1.728	11.520	56.207
5	1.182	7.882	68.018	1.182	7.882	68.018	1.401	9.341	65.548
6	1.014	6.763	74.781	1.014	6.763	74.781	1.385	9.233	74.781
7	0.851	5.674	80.455						
8	0.814	5.429	85.884						
9	0.519	3.458	89.342						
10	0.486	3.241	92.583						
11	0.352	2.348	94.931						
12	0.281	1.874	96.805						
13	0.246	1.641	98.447						
14	0.170	1.133	99.580						
15	0.063	0.420	100.000						

Extraction method: Principal Component Analysis (PCA)

Table 5.3 Total variance explained, initial eigenvalues, extraction factors and rotated factors

5.4 FACTOR CODING

Factor analysis is used to identify underlying variables, or factors and assists to explain the pattern of correlations within a set of observed variables. Factor analysis is mainly used in the reduction of data to identify a small number of factors to explicate most of the variance that is observed in a much larger number of variables. This section discusses the extracted factors and the items grouped in each factor and references the items that are coded according to the question numbers in the questionnaire (see *Appendix K*).

5.4.1 Factor 1: Information security tools

This factor consists of three (3) items discussed under information security tools in the ICT environment in section 4.13 of Chapter 4 of this study. This section of the study wishes to establish what ICT governance practices do enterprises practice to protect their information systems from being compromised. The three items that were grouped in Table 5.4 relate to information security protection and system security software controls, which is the common theme in this factor.

Furthermore, it is also noted that another common theme in this factor relates to information security software control measures and the performance of IT systems in the ICT environment to guard against unauthorised access. The items further highlight the frequency to execute the security system policies in the ICT environment to update security software updates. It was noted that no other factors moved to this factor. Thus, the name information security tools in the ICT environment refer to this factor and its items. Table 5.4 Indicates the items and item codes of information security tools.

Item code	Item description
Q.15	System performance in a security product
Q.16	Information protection tools installed to guard against unauthorised user access
Q.17	Updating system security software updates (Microsoft, SQL, etc.)

Table 5.4 Items and item codes of information security tools in the ICT environment

5.4.2 Factor 2: Information security protection features

This factor consists of three (3) items discussed under Information Security protection features in the ICT environment in Section 4.13 of Chapter 4 of this dissertation. This section of the study wishes to determine the Information Security protection features that these enterprises have in place to protect information systems from unauthorised access. The three items grouped in this factor relate to a common outcome of security protection features, the frequency of scanning the ICT environment for vulnerabilities and thus ensuring there are no data breaches. It is noted that no other factors moved to this factor. Thus, the name Information Security protection features refer to this factor and its items. Table 5.5 indicates the items and item codes of information security features.

Item code	Item description
Q.13	On-demand scan for viruses (example, a full system scan, a scan of removable drives or a scan of single files)?
Q.14	Rating protection against threats in a security product?
Q.18	Full end-to-end scan of the ICT environment to detect any vulnerabilities?

Table 5.5 Items and item codes of information security protection features

5.4.3 Factor 3: Information security management

This factor consists of three (3) items discussed under information security management in the ICT environment in Section 4.13 of Chapter 4 of this study. This section of the study wishes to determine if ICT environments have information security protection services in place. Only one item moved from 'auditable control measures' used by enterprises to join two factors in 'access control measures' in the ICT environment.

The three items are thus a combination of enterprises' network security, the funding of security solutions and the importance of information security at an executive level. For this reason, it can be stated that members at board level are concerned about information security, and thus encourage management to invest in network hardware infrastructure to ensure the ICT environment is sufficiently protected against any vulnerabilities.

Thus, the reason for the grouping of information security management and executive funding. Table 5.6 indicates the items and item codes of information security management.

Item code	Item description
Q.25	Network security of the enterprise
Q.29	Convincing management to invest in security solutions
Q.42	Board of directors' interest in information security

Table 5.6: Items and item codes of information security management

5.4.4 Factor 4: Access control processes

This factor consists of three (3) items discussed under Access Control Processes in the ICT environment in Section 4.13 of Chapter 4 of this study. This section of the study wishes to determine if ICT environments have access control processes in place when providing access to requests for users. The three items are thus a combination of enterprises' access control processes, sharing of information and internet security. For this reason, it can be stated that enterprises have procedures in place to manage their access control processes to ensure the ICT environment is sufficiently protected against any vulnerabilities. Thus, the reason for the implementation and management of access control processes. Table 5.7 indicates the items and item codes of access control processes.

Item code	Item description
Q7	Internet security suite offering more security
Q24	Process in place to authenticate a user when he/she request a password change or a user account to be unlocked.
Q26	Sharing information of security attacks with third parties

Table 5.7: Items and item codes of access control processes

5.5 RELIABILITY ANALYSIS

This section analyses the results of the internal consistency reliability of the extracted variables. Cronbach's alpha coefficient is the preferred measure of internal consistency because all items are compared with each other and with the total questionnaire (Nunnally & Bernstein, 1994). Cronbach's alpha was developed by Lee Cronbach in 1951 to provide a measure of the internal consistency of a test or scale, which is expressed as a number between 0 and 1 (Tavakol & Dennick, 2011).

The closer the alpha is to one (1), the greater the internal consistency of the items in the questionnaire. Internal consistency should be determined before a test can be deployed for research to ensure validity (Nunnally & Bernstein, 1994). In addition, reliability estimates show the amount of measurement error in a test. In this study, Cronbach’s alpha (or coefficient alpha) was used as a reliability analysis method to determine if the questions exhibit a homogeneous structure (Kalayci, 2006).

The following four criteria used for judging Cronbach’s alpha coefficient results, as proposed by Kalayci (2006), were used in this study:

- If the alpha is between 0.00≤ α <0.40, the scale is not reliable.
- If between 0.40≤ α <0.60, then reliability is low.
- If between 0.60≤ α <0.80, then the scale is reliable.
- If between 0.80≤ α <1.00, then the scale is highly reliable.

Appendix L summarises the reliability results of the extracted factors. It indicates the Cronbach’s alpha for each factor and the number of items in each factor.

5.5.1 Reliability of information security tools

The factor in Table 5.8 consists of three items. The Cronbach’s alpha for these items ranges between 0.555 and 0.563. It is noted that items, “system performance in a security product”, “information protection tools” and “update your system security software” have a Cronbach’s alpha which is less than 0.6. However, Van Griethuijsen, Van Eijck, Haste, Den Brok, Skinner & Mansour, Gencer & BouJaoude (2014), completed studies with a Cronbach’s alpha value of ≥0.6 and advised to continue with the analysis, arguing that slightly increasing the number of items would lead to acceptable values for Cronbach’s alpha. This, the three items have a Cronbach’s value of 0.563, 0.555 and 0.562 respectively and will be retained for further analysis. Thus, no item will be deleted to increase the overall Cronbach’s alpha. The item-total statistics in Table 5.8 (See *Appendix L* for the original table) contain the scale mean if item deleted, scale variance if item deleted, corrected item-total correlation and Cronbach’s Alpha if item deleted”. Table 5.8 Indicates the item-total statistics.

Item-total Statistics				
	Scale mean if item deleted	Scale variance if item deleted	Corrected item-total correlation	Cronbach's alpha if item deleted
Q15	25.71	28.880	0.534	0.563
Q16	25.29	26.880	0.382	0.555
Q17	25.65	28.237	0.406	0.562

Table 5.8: Item-total statistics

5.5.2 Reliability of information security protection features

The factor in table 5.9 consists of three items. The Cronbach's alpha for these items ranges between 0.561 and .592. It is noted that items, "on-demand system security scanning", "protection against security threats" and "end-to-end system scans" have a Cronbach's alpha, which is less than 0.6. As earlier stated, Van Griethuijsen *et al.* (2014), completed studies with a Cronbach's alpha value of ≥0.6 and advised to continue with the analysis, arguing that slightly increasing the number of items would lead to acceptable values for Cronbach's alpha. The three items have a Cronbach's value of 0.567, 0.592 and 0.561 respectively; it will be retained for further analysis (See *Appendix L* for the original table). Table 5.9 indicates items and item codes of information security protection features.

Item-total statistics				
	Scale mean if item deleted	Scale variance if item deleted	Corrected item-total correlation	Cronbach's alpha if item deleted
Q13	25.13	27.316	0.314	0.567
Q14	24.77	27.714	0.199	0.592
Q18	24.94	26.329	0.333	0.561

Table 5.9: Items and item codes of information security protection features

5.5.3 Reliability of information security management

The factor in Table 5.10 consists of three items. The Cronbach's alpha for these items ranges between 0.526 and 0.607. The items "to convince management to invest in information security" and "how concerned are the board of directors about information security" have a Cronbach's alpha which is less than 0.6. However, the item "is the enterprises network sufficiently secured" has a Cronbach's alpha of 0.607 (see *Appendix L* for the original table).

As earlier stated, Van Griethuijsen *et al.* (2014), completed studies with a Cronbach's value of ≥0.6 and advised to continue with the analysis, arguing that slightly increasing the number of items would lead to acceptable values for Cronbach's alpha. The three items have a Cronbach's value of 0.607, 0.526 and 0.563 respectively; it will be retained for further analysis. The Item-total statistics in *Appendix L* contain the "scale mean if item deleted, scale variance if item deleted, corrected item-total correlation, and Cronbach's alpha if item deleted". Table 5.10 indicates the items and item codes of information security management.

Item-total statistics				
	Scale mean if item deleted	Scale variance if item deleted	Corrected item-total correlation	Cronbach's alpha if item deleted
Q25	25.32	30.692	0.061	0.607
Q29	24.77	24.981	0.497	0.526
Q42	25.26	28.598	0.432	0.563

Table 5.10 Items and item codes of information security management

5.5.4 Access control processes

The factor in Table 5.11 consists of three items. The Cronbach's alpha for these items ranges between 0.589 and 0.621. The item "does your organisation have a process in place to authenticate a user when he/she request a password change or a user account to be unlocked" have a Cronbach's alpha which is less than 0.6. However, the items "internet security suite offers more security" and "enterprises share information" has a Cronbach's alpha of 0.606 and 0.621 respectively (see *Appendix L* for the original table).

As earlier stated, Van Griethuijsen *et al.* (2014), completed studies with a Cronbach's value of ≥0.6 and advised to continue with the analysis, arguing that slightly increasing the number of items would lead to acceptable values for Cronbach's alpha. The three items have a Cronbach's value of 0.606, 0.589 and 0.621 respectively; it will be retained for further analysis. The Item-total statistics in *Appendix L* contain the "scale mean if item deleted, scale variance if item deleted, corrected item-total correlation, and Cronbach's alpha if item deleted".

Table 5.11 indicates the items and item codes of access control processes.

Total item-statistics				
	Scale mean if item deleted	Scale variance if item deleted	Corrected item-total correlation	Cronbach's alpha if item deleted
Q7	24.71	28.946	0.122	0.606
Q24	25.84	30.006	0.195	0.589
Q26	24.29	29.346	0.065	0.621

Table 5.11 Access Control Processes

5.6 DESCRIPTIVE STATISTICS OF VALID AND RELIABLE FACTORS

The data in this study were analysed using descriptive statistics to determine the usage of information security tools in the ICT environment, then ascertained the usage of information security protection features and finally the holistic management and executive funding of information security infrastructure. Somekh and Lewin (2011) state that descriptive statistics are used to describe and summarise data and include measures of central tendency (average) and dispersion (the spread of data). Descriptive statistics involve statistical procedures that are used to organise, simplify, summarise, and display data that describe imperative qualities of a set of measurements (Mendenhall, Beaver & Beaver, 2013).

Furthermore, Schniederjans, Schniederjans and Starkey (2015) state that descriptive statistics are used to identify possible trends in large data sets or databases which are to provide a general idea of what the data looks like. Somekh and Lewin (2011) state that reliability refers to the extent that the measurement instrument yields the same results over multiple trials. Whilst validity refers to the purpose because the instrument measures were designed to measure. Moreover, a measure can be reliable if it always generates the same result, but not valid if it does not measure the intended concept. However, if it is not reliable, then it cannot be valid. Kohler and Kreuter (2005) define standard deviation as “the most common summary statistic for determining the dispersion of a distribution”.

Kohler and Kreuter (2005) further state that to calculate the standard deviation, the arithmetic mean needs to be calculated first. Descriptive statistics include measures of tendency mean and measures of dispersion (standard deviation). Usually, when describing the position of the distribution with the arithmetic mean, the standard deviation will be used to describe the dispersion of the distribution. Standard deviation is a way of measuring the difference between each value of a variable as well as the mean value of the variable (Somekh & Lewin, 2011). Standard deviation represents the spread of the data or the variability.

Thus, this analysis uses descriptive statistics to further ensure that appropriate validity and reliability measures were employed in the quantitative research, which is discussed in the subsequent sections. The three factors, "'information security tools in the ICT environment", "information security protection features" and "'information security management and executive funding" will be discussed in the next section.

5.6.1 Descriptive statistics of information security tools

The section aimed to describe the information security tools used in the ICT environment. The factor "information security tools used in an ICT environment to guard against information vulnerabilities" is key to sustaining a secure and efficient environment and consists of three measurement items. The first item aims to determine how enterprises rate an information security product from a systems performance perspective.

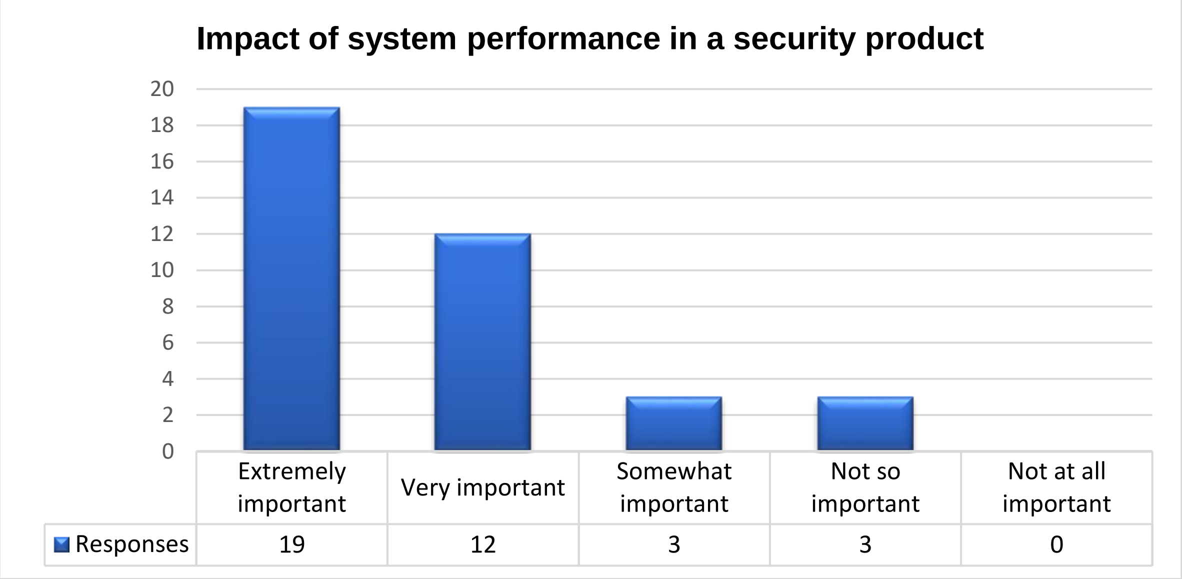
The aim of the second item was essentially defined to determine how enterprises rate information protection tools to guard against unauthorised user access. The aim of the final item wishes to determine how often enterprises update their system security software to guard against vulnerabilities. Table 5.12 indicates the descriptive statistics for information security tools.

Item statistics			
	Mean	Std. deviation	N
Q15	1.32	0.48	37
Q16	1.74	1.00	37
Q17	1.39	0.72	37

Table 5.12: Information security tools

The first item aimed to determine how participants rate the low impact on system performance when reviewing a security product. The Likert scale was used in this question: extremely important, very important, somewhat important, not so important, and not at all important. The standard deviation (SD=0.48) and mean (M=1.32) for the first item indicate the lowest mean and standard deviation relative to the other items of this section. The mean of the three data sets was compared and revealed that the majority of the participants indicated that the impact of system performance in a security product is important.

The results indicated that 52% of the participants regard the impact of system performance in a security product as extremely important; 32% regard it as very important; 8% as somewhat important; and 8% as not so important. Thus, most of the participants regarded the impact of system performance in a security product as extremely important. Figure 5.9 indicates the frequency of the impact of system performance on a security product.



	Extremely important	Very important	Somewhat important	Not so important	Not at all important
Responses	19	12	3	3	0

Figure 5.9: Impact of system performance in a security product

The second item aimed to determine how participants rate information protection tools installed in the ICT environment to guard against unauthorised user access. The Likert scale was used in this question: extremely important, very important, somewhat important, not so important, and not at all important. The standard deviation (SD=1.00) indicates that there was less spread of participants that indicated that information protection tools must be installed in the ICT environment of the enterprise to guard against unauthorised user access.

The mean of (M=1.74) indicated that the majority of participants believe that information protection tools must be installed in the ICT environment of the enterprise to guard against unauthorised user access. The results revealed that 74% of the participant's rate information protection tools installed in the ICT environment to guard against unauthorised user access as extremely important; 24% rate it as very important; 3% as somewhat important; and 3% as not so important. Thus, most of the respondent's rate information protection tools installed in the ICT environment to guard against unauthorised user access as extremely important. Figure 5.10 indicates the frequency of information security tools.

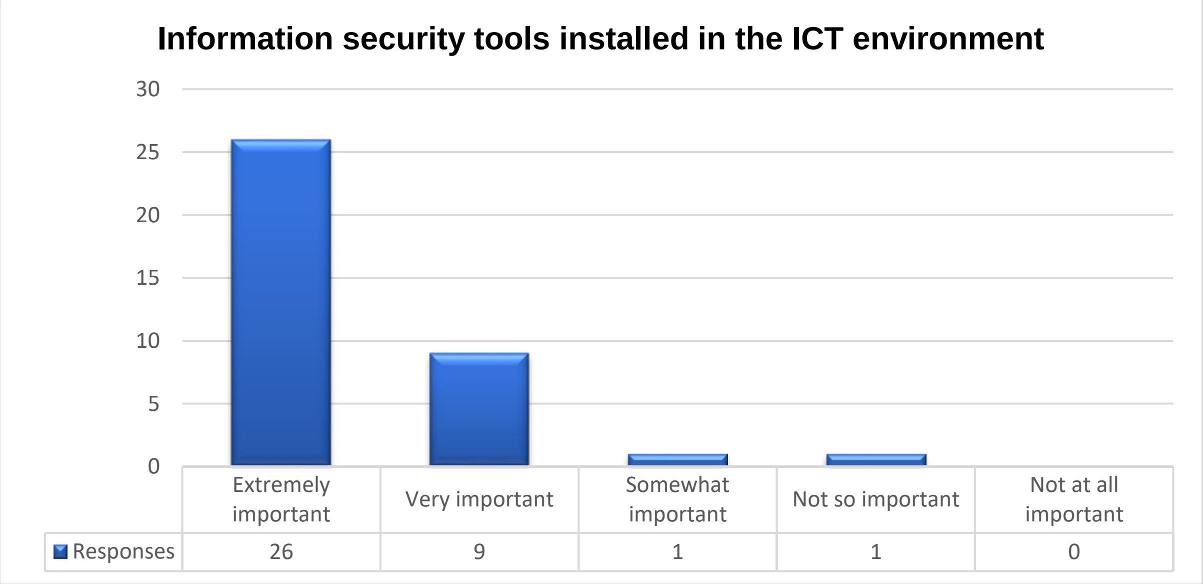


Figure 5.10: Information protection tools installed

The aim of the final item determined how often do enterprises update their security software of the computer systems in the ICT environment. Five (5) options were made available for the participants to choose from. The options were presented as follows: daily, weekly, monthly, annually, and other. The standard deviation (SD=0.72) and mean (M=1.39) for the final item indicate that the higher standard deviation of the data is more spread out. The standard deviation (SD=0.72) indicates that there was less spread of participants that indicated that the security software in the ICT environment of the enterprise must be updated more often. Thus, the mean of (M=1.39) indicates that the majority of participants indicated that security software in the ICT environment of the enterprise must be updated more often.

It can thus be stated that the majority of participants indicated that security software in the ICT environment of the enterprise must be updated at least once a month. The question determined that 46% of enterprises update their system software with security patches monthly, 24% update weekly, 11% update daily, 3% annually, whilst 16% of enterprises selected “other”. It can thus be stated that most enterprises update their system software with security patches monthly. Figure 5.11 indicates the frequency of system security software updates.

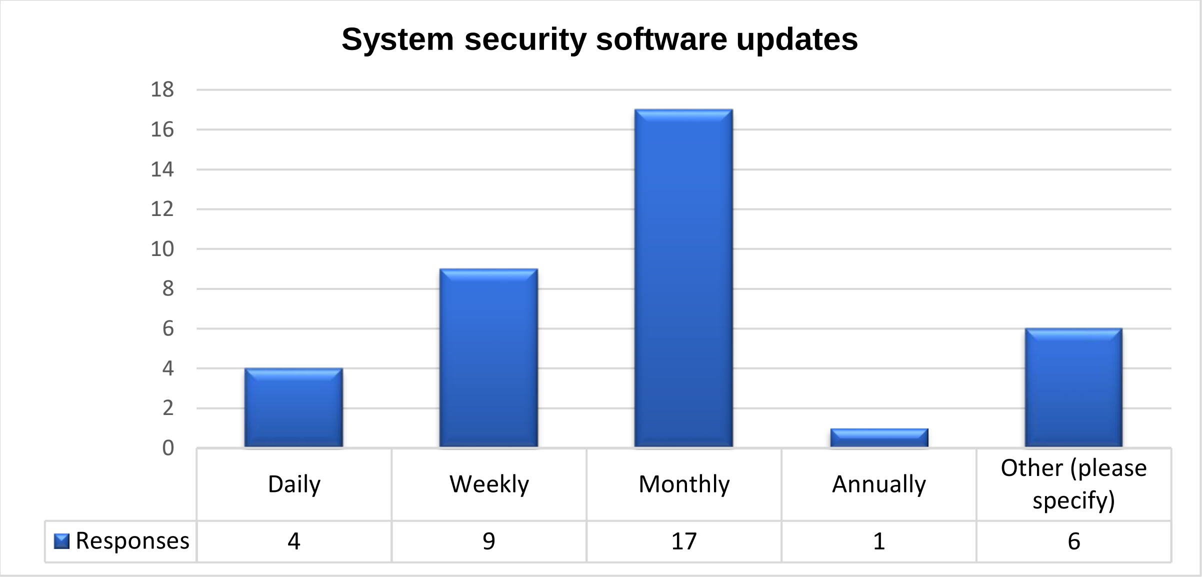


Figure 5.11: System security software updates

The mean of the three data sets was compared and indicated that participants rate information protection tools to guard against unauthorised user access in the ICT environment as extremely important.

5.6.2 Descriptive statistics of information security protection features

The section aims to describe the information security protection features that enterprises use in their ICT environments and if enterprises performed holistic on-demand system scans. The factor “‘information security protection features are used in an ICT environment” to optimize and support the information security systems and consists of three measurement items.

The first item aimed to determine if enterprises perform holistic on-demand system scans of the ICT environment. The next item aimed to determine how highly do enterprises rate information protection against threats in an information security product. The final item aimed to determine how often enterprises perform end-to-end security scans in the ICT environment to detect any information security vulnerabilities. Table 5.13 indicates the descriptive statistics for information security protection features.

Item statistics			
	Mean	Std. deviation	N
Q13	1.90	1.04	37
Q14	2.26	1.24	37
Q18	2.10	1.19	37

Table 5.13 Information security protection features

This question aimed to determine if participants perform scheduled or on-demand system scans for viruses. The Likert scale was used in this question: very likely, likely, neither likely nor unlikely, unlikely, and very unlikely. The standard deviation (SD=1.04) indicates that there was less spread of participants that indicated that on-demand security scans of any ICT device are important. Thus, the mean of (M=1.90) indicates that a concentrated number of participants indicated that on-demand system security scans of any ICT device are critical.

The results show that 32% of the participants indicated that it is very likely that their enterprises perform on-demand scans for viruses; 43% indicate it is likely 5% indicated it is neither likely nor unlikely’; 14% indicated that it is unlikely, and 5%; indicated that it is very unlikely. Thus, most participants indicated that it is likely, and very likely that their enterprises perform on-demand system scans for viruses. Figure 5.12 indicates the frequency of the on-demand system scans.

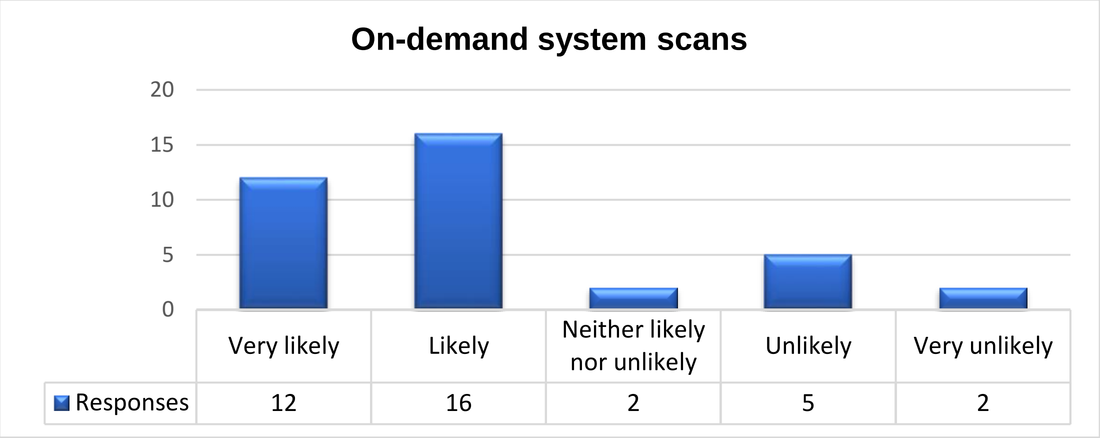


Figure 5.12: On-demand system scans

This question aimed to determine how high participants rate protection in an antivirus security product. The Likert scale was used in this question: extremely important, very important, somewhat important, not so important, and not at all important. The standard deviation (SD=1.24) and mean (M=2.26) for the second item indicated the data is spread out and dispersed from the mean. This result essentially indicates that a large number of participants highly rate the protection against threats in a security product to protect the information of an enterprise. The standard deviation (SD=1.24) indicates that there was a wider spread of participants who believe in a high protection rate in an antivirus security product.

Thus, the mean of (M=2.26) indicates an absolute number of participants who highly rated protection against threats in a security product to protect the information of an enterprise. The results indicated that 67% of the participants regard high protection in an antivirus security product as extremely important, 30% regard it as very important, and 3% as somewhat important. Thus, most of the participants regard high protection in an antivirus product as extremely important. Figure 5.13 indicates the frequency of high protection rate in an antivirus security product.

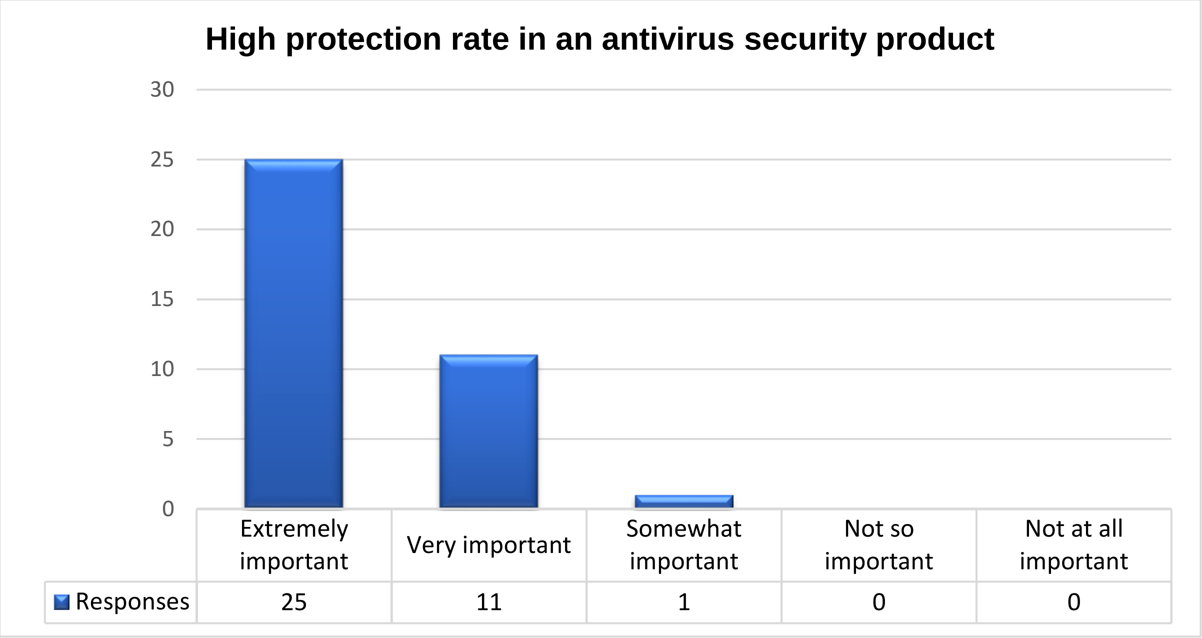


Figure 5.13: High protection rate in an antivirus security protection

This question aimed to determine how often enterprises do a full end-to-end scan of their ICT environment to detect any vulnerabilities. Five (5) options were made available for the participants to choose from. The options were presented as follows: daily, weekly, monthly, annually, and other. The standard deviation (SD=1.19) and mean (M=2.10) for the third item indicate the data is spread out and dispersed from the mean. It can be stated that a large number of participants highly regarded full end-to-end scans to detect any vulnerabilities of the ICT environment as important.

The standard deviation (SD=1.19) indicates that there was a wider spread of participants who believe in a full end-to-end ICT environmental scan. Thus, the mean (M=2.10) indicates a dispersed number of participants believe in a full end-to-end ICT environmental scan. The results indicate that 16% of the participants do a daily full end-to-end scan of their ICT environment to detect any vulnerabilities; 30% perform weekly scans; 38% perform monthly scans, and 16% perform annual scans. Figure 5.14 indicates the frequency of full end-to-end scans.

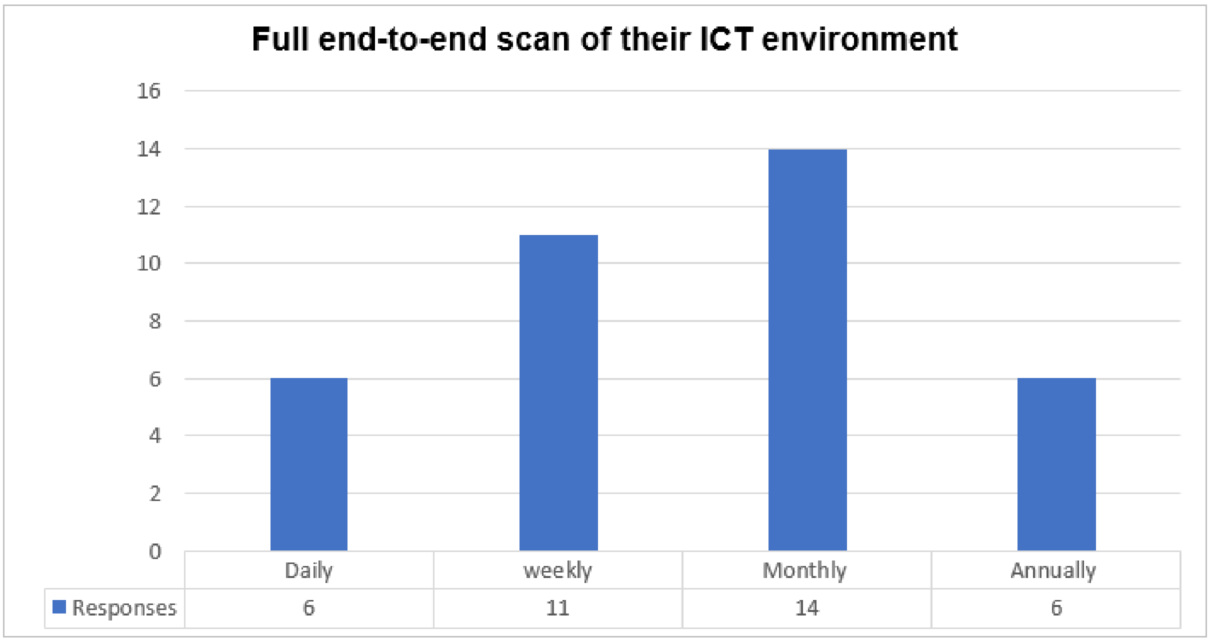


Figure 5.14: Full end-to-end environment scan

The mean of the three data sets are compared and indicated that participants highly rate the protection of information against threats in a security product. The highest data value of the standard deviation for this section indicates that high protection against threats in a security product is essential and imperative.

5.6.3 Descriptive statistics and executive funding

This section aimed to determine how well supported is the management of information security and the funding thereof at an executive level. The factor "how well does the management of information security and executives support the funding of information security" consists of three measurement items. The first item aimed to determine if enterprises believe their ICT network infrastructure is sufficiently secure against any vulnerabilities or attacks.

The second item aimed to determine if management needs to be convinced to invest in information security solutions. The third item aimed to determine if the board of directors of enterprises are concerned with the status and level of information security in the ICT environment.

Table 5.14 indicates the descriptive statistics of information security management and executive funding.

Item statistics			
	Mean	Std. deviation	N
Q25	1.71	0.78	37
Q29	2.26	1.12	37
Q42	1.77	0.62	37

Table 5.14: Information security management and executive funding

The question aimed to determine if enterprises believe their network is sufficiently secure. The Likert scale was used in this question: very likely, likely, neither likely nor unlikely, unlikely, and very unlikely. The standard deviation (SD=0.78) and mean (M=1.71) of the first item is indicated in this section. The high rating for the standard deviation indicates that the data is spread out.

Thus, the mean indicates that a larger number of participants indicated that the network infrastructure of the enterprises is sufficiently secure. The results indicate that 43% of the participants believe it is very likely that their network is sufficiently secure; 43 % believe it is likely that their network is secure; 11% believe it is neither likely nor unlikely, and 3% of the respondents believe it is unlikely. Thus, most of the participants believe their network is sufficiently secure. Figure 5.15 indicates the frequency of the security tools.

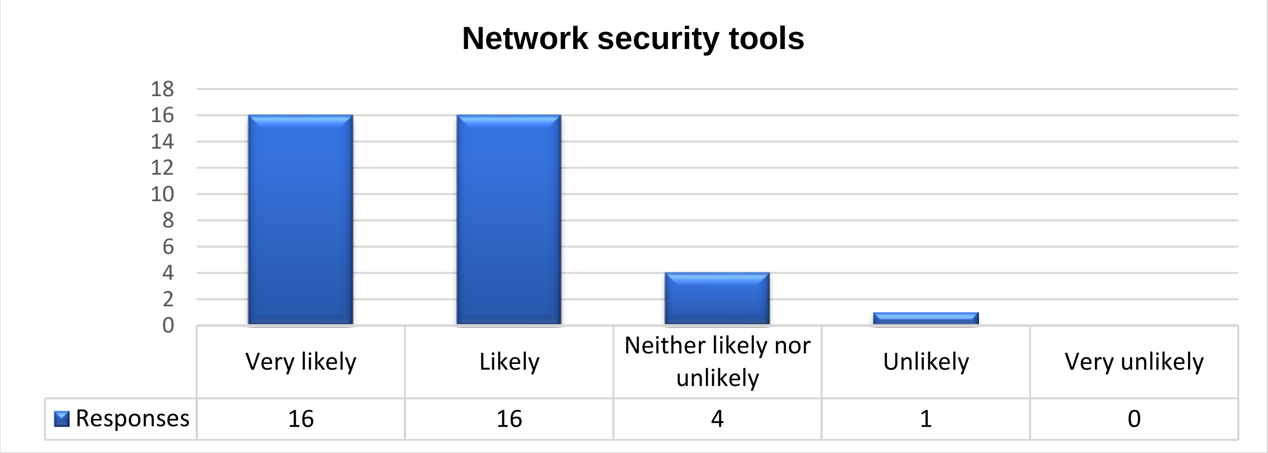
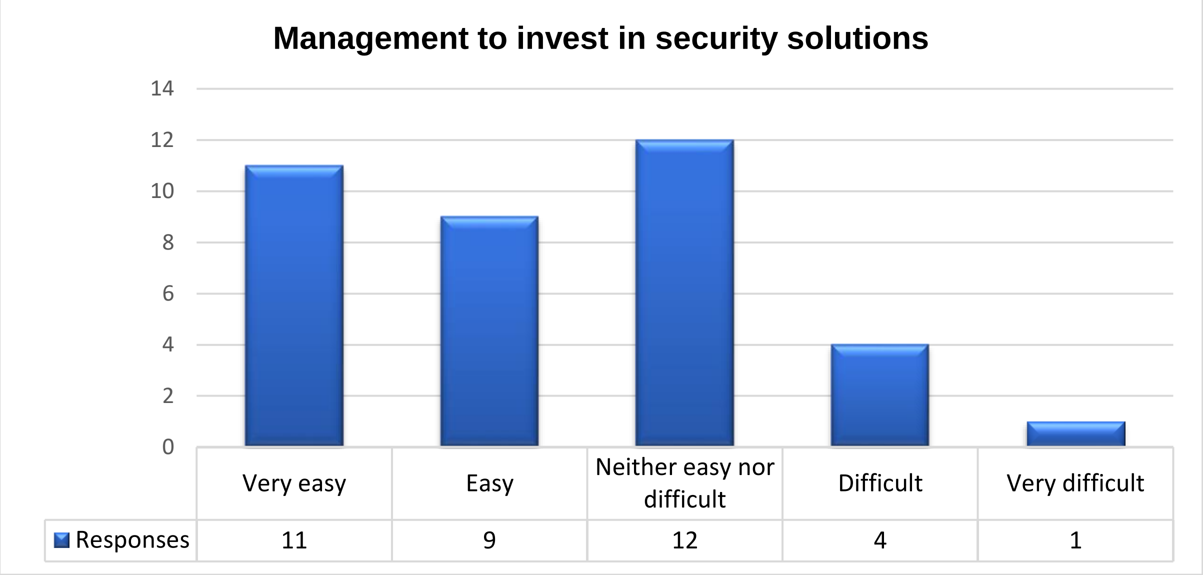


Figure 5.15: Network security tools

This question aimed to determine if enterprises believe it is difficult to convince management to invest in security solutions. The Likert scale was used in this question:

very easy, easy, neither easy nor difficult, difficult, and very difficult. The standard deviation (SD=1.12) and mean (M=2.26) for the second item indicates the data is spread out and dispersed from the mean. Thus, it can be stated that the high rating of the standard deviation indicates a wider spread of data.

The mean indicates that a larger number of participants believe that management needs to be convinced to invest in information security solutions. The results indicate that 30% of the participants believe it is Very Easy to convince management to invest in security solutions; 24% of participants believe it is Easy, 32% believe it is neither easy nor difficult, 11% believe it is difficult; 3% believes it is very difficult. Thus, most of the participants believe it is neither easy not difficult to convince management to invest in security solutions. Figure 5.16 indicates the frequency of management investing in security solutions.



	Very easy	Easy	Neither easy nor difficult	Difficult	Very difficult
■ Responses	11	9	12	4	1

Figure 5.16: Management to invest in security solutions

This question aimed to determine how concerned the board of directors were about information security. The scale consisted of four options: the most important priority, a top priority but not the most important, not very important, and not important at all. The standard deviation (SD=0.62) indicates that it was less spread for participants who believe that the board of directors invest in information security solutions. Thus, the mean of (M=1.77) indicates that the majority of participants believe that the board of directors invest in information security solutions.

Whilst a concentrated number of participants indicates that the board of directors are concerned with information security in the ICT environment. The results indicate that 32% of the participants stated that information security is the most important priority for the board of directors; 60% stated it is a top priority, but not the most important; 8% stated that it is not very important; whilst no one stated that information security is not important at all to the board of directors. The results indicate that most participants stated that information security is a top priority, but not the most important to the board of directors. Figure 5.17 indicates the frequency of the board of directors' interest in information security.

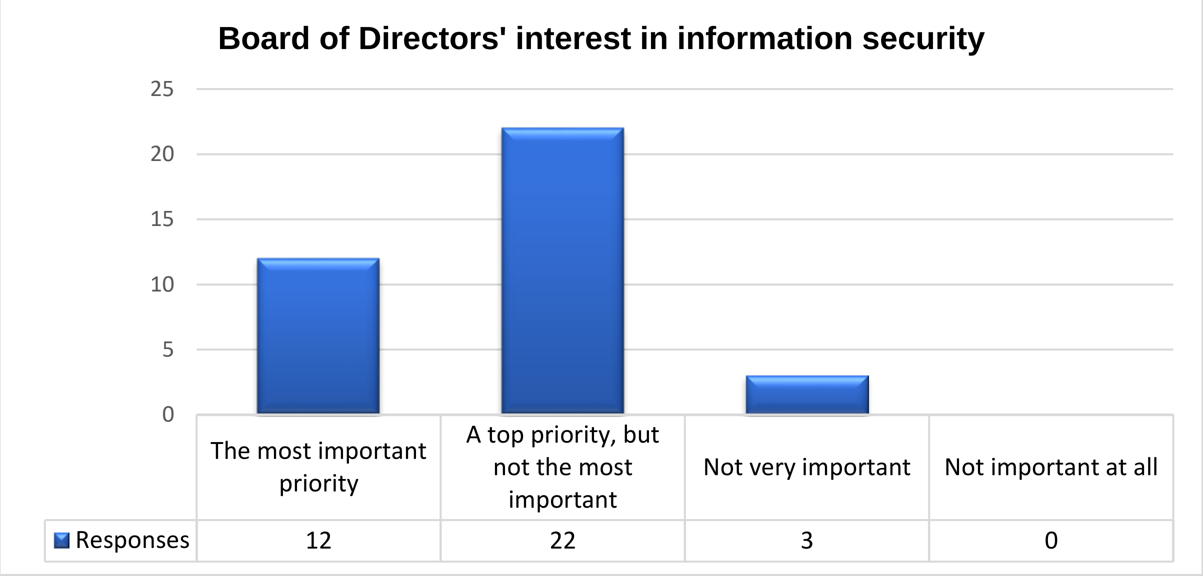


Figure 5.17: Board of directors' concern about information security

The mean of the three data sets are compared and indicates that participants highly rate the funding of information security and the security of the ICT environment. The highest data value of the standard deviation for this section indicates that several participants believe it is difficult to convince management to invest in security solutions.

5.6.4 Descriptive statistics and access control processes

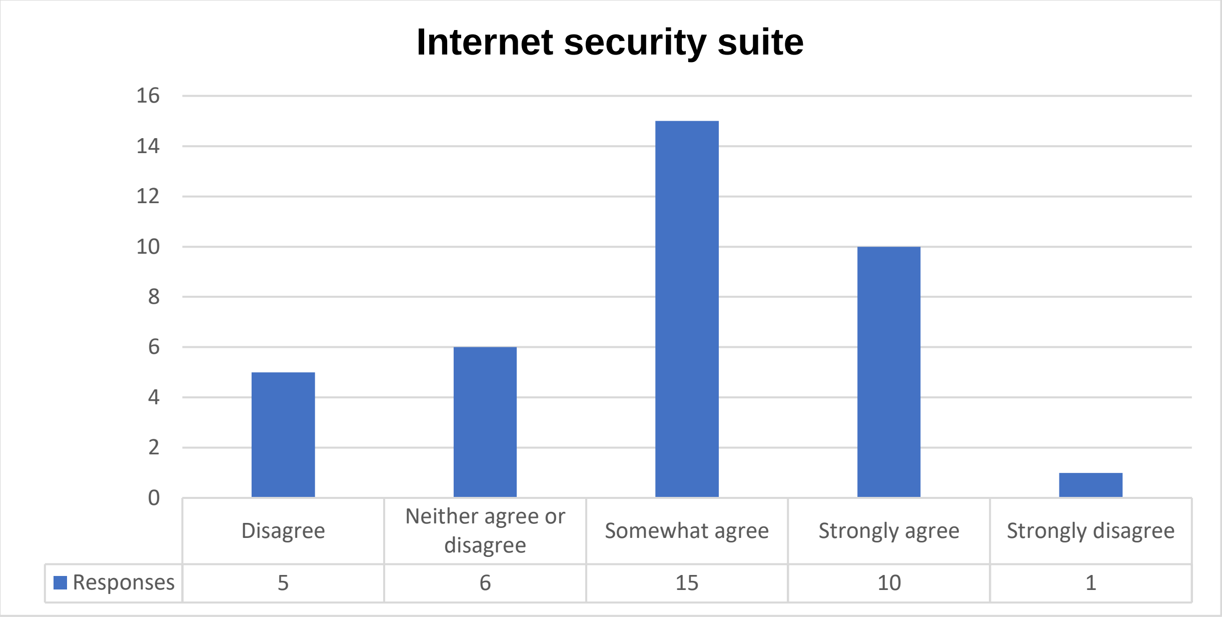
This section aimed to determine how well enterprises manage access control processes. The factor "access control processes" consists of three measurement items. The first item aimed to determine if enterprises believe their internet security suite offers more security to their ICT network infrastructure and sufficiently provide security against any vulnerabilities or attacks. The second item aimed to determine if enterprises have processes in place to authenticate users if there is a request to change a password or unlock a user account. The third item aimed to determine if enterprises share information on security attacks. Table 5.15 indicates the descriptive statistics access control processes.

Item statistics			
	Mean	Std. deviation	N
Q7	2.32	1.17	37
Q24	1.19	0.65	37
Q26	2.74	1.26	37

Table 5.15: Access control processes

The aim of question seven was to determine if enterprises believe their internet security suite offers better security to their ICT network infrastructure than their vendor's security product. The Likert scale was used in this question: disagree, neither agree or disagree, somewhat agree, strongly agree, and strongly disagree. The standard deviation (SD=1.17) and mean (M=2.32) of the first item is indicated, in this section. The high rating for the standard deviation indicates that the data is spread out. Thus, the mean indicates that a larger number of participants indicated that their security suite offers better security than their vendor's security product.

The results indicate that 41% of the participants somewhat agree that their internet security suite offers better security to their ICT network infrastructure, 27% strongly agree; 16% neither agree nor disagree; 14% disagree and 3% of the respondents strongly disagree. Thus, most of the participants agree that internet security suite offers better security to their ICT network infrastructure than their vendor's security product. Figure 5.18 indicates the internet security suite of enterprises.



	Disagree	Neither agree or disagree	Somewhat agree	Strongly agree	Strongly disagree
■ Responses	5	6	15	10	1

Figure 5.18: Network security suite

The aim of question twenty-four was to determine if enterprises have processes in place to authenticate users if there is a request to change a password or unlock a user account. The Likert scale was used in this question: very likely, unlikely, neither likely nor unlikely and likely. The standard deviation (SD=0.65) and mean (M=1.19) for the second item indicates the data is not spread out and not dispersed from the mean. Thus, it can be stated that the low rating of the standard deviation indicates a lower spread of data.

The mean indicates that a larger number of participants believe that their enterprises have security control processes in place. The results indicate that 89% of the participants believe it is very likely that their enterprises have control processes in place; 5% of participants believe neither likely nor unlikely, 3% believe it is unlikely and 3% believe it is very likely. Thus, most of the participants believe their enterprises have access control processes in place. Figure 5.19 indicates the access control processes.

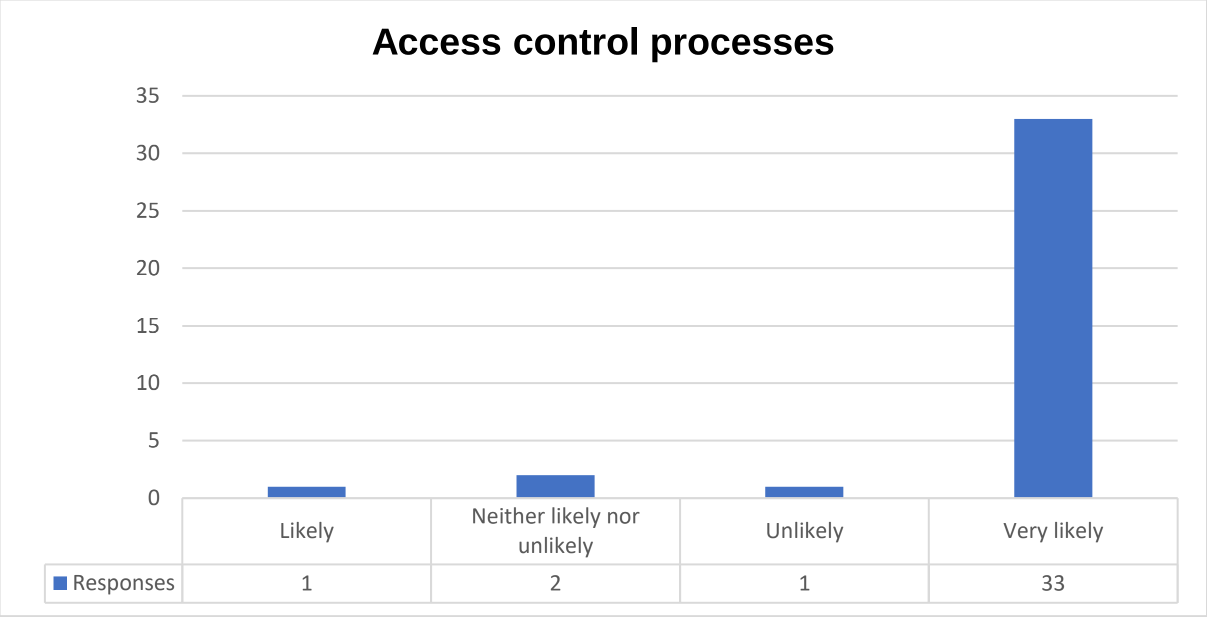


Figure 5.19: Access control process

This question aimed to determine if enterprises share information on information security attacks. The standard deviation (SD=1.26) indicates that it was less spread for participants who believe that the board of directors invest in information security solutions. Thus, the mean of (M=2.74) indicates that most participants do not believe that their enterprises share security information on cyber-attacks. Whilst a concentrated number of participants indicates that it is very unlikely.

The results indicated that 41% of the participants stated that it is likely that their enterprises share information on cyber-attacks; 27% stated it is unlikely; 11% stated that it is neither likely nor unlikely; 11% indicated that it is very likely and 11% indicated that it is very unlikely. Thus, the results indicated that most participants stated that it is likely that their enterprises share information on cyber-attacks with third parties. Figure 5.20 indicates the sharing of security information

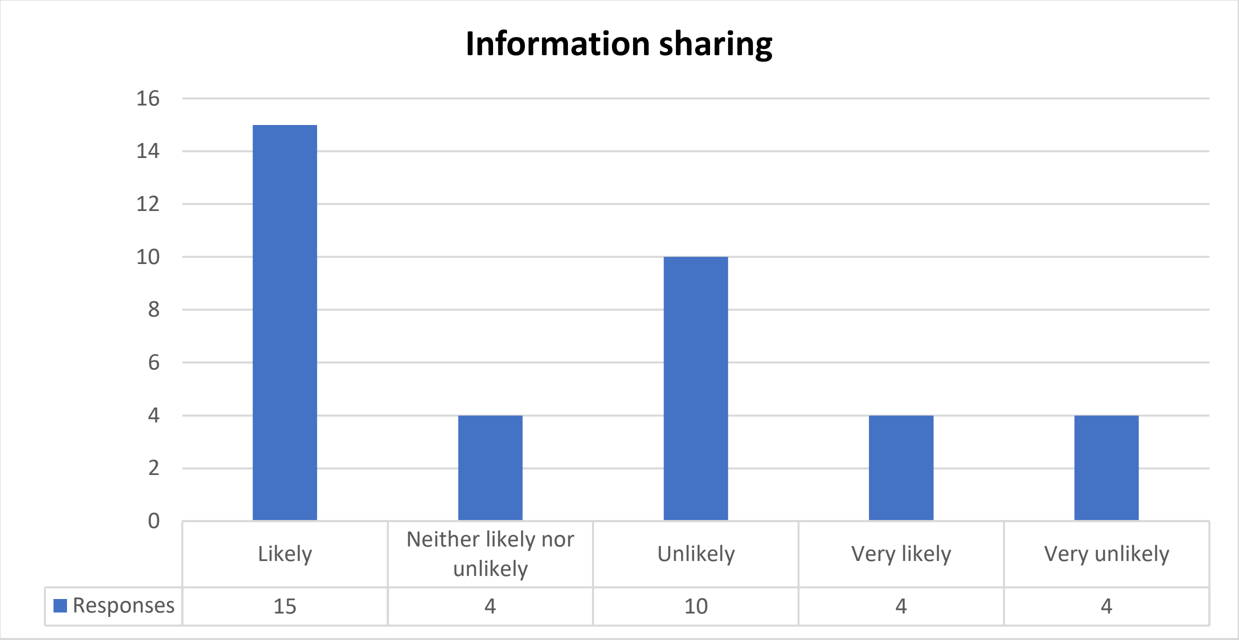


Figure 5.20: Information sharing

The mean of the three data sets are compared and indicates that participants believed that their enterprises have control processes in place.

5.7 PEARSON'S CORRELATION COEFFICIENT *(r)* OF VALID AND RELIABLE FACTORS

All the constructs showed a positive correlation (Table 5.16). It was noted that with information security tools in the ICT environment, information security protection features, information security management and access control processes that none of the correlations has a *p*-value less or equal to 0.05 (p<0.05), therefore there is no significant linear positive. The information security tools in the ICT environment correlation with information security protection features construct (r=0.127, n=36, p<.05) shows that all variables have a positive correlation. The *p*-value for the information security protection features is 0.461. This makes it a 46.1% confidence level in this correlation.

The Pearson's *r* for these factors was 1.61% (0.127^2). There is thus no significant positive relationship between information security tools in the ICT environment and information security protection features. The information security tools in the ICT environment correlation with information security management and executive funding construct (r=0.091, n=35, p<.05) shows that all variables have a positive correlation. The p-value for the information security management and executive funding is 0.091. Thus, there is a 9.10% level of confidence in this correlation. The Pearson's *r* for these factors was 0.83% (0.91^2).

There is no significant positive relationship between information security tools in the ICT environment and information security management and executive funding. The information security protection features correlation with information security management and executive funding construct (r=0.306, n=35, p<.05) shows that all variables have positive correlation. The *p* value for security policies is 0.306. Thus, there is 30.6% level of confidence in this correlation. The Pearson's *r* for these factors was 9.36% (0.306^2). There is thus no significant positive relationship between information security protection features and information security management and executive funding.

The access control processes in the ICT environment correlation construct (r=0.118, n=35, p<.05) shows that all variables have a positive correlation. The *p*-value for access control processes is 0.118. Thus, there is a 11.8% level of confidence in this correlation. The Pearson's *r* for these factors was 13.9% (0.118^2). There is no significant positive relationship between information security tools in the ICT environment and access control processes. The *p*-value for security policies is 0.306. Thus, there is a 30.6% level of confidence in this correlation. The Pearson's *r* for these factors was 9.36% (0.306^2). There is thus no significant positive relationship between information security protection features and information security management and executive funding.

Based on Pearson's *r*, it can be concluded that the variables were not significantly correlated. Furthermore, all the Pearson's *r* is positive 9.36% (0.306^2), which can conclude that as one variable increases in value, the second variable also increases in value. Similarly, as one value decreases in value, the second variable also decreases in value, which is called positive correlation.

Table 5.16 indicates the table of critical values: Pearson's correlation coefficient *r* between predictor and constant variables.

		Information security tools in the ICT environment	Information security protection features	Information security management and executive funding	Access Control Processes
Information security tools in the ICT environment	Pearson's *r* correlation	1	0.127	0.091	0.118
	Sig. (2-tailed)		0.461	0.605	0.500
	N	37	36	35	35
Information security protection features	Pearson's *r* correlation	0.127	1	0.306	0.245
	Sig. (2-tailed)	0.461		0.074	0.156
	N	36	36	35	35
Information security management and executive funding	Pearson's *r* correlation	0.091	0.306	1	0.233
	Sig. (2-tailed)	0.605	0.074		0.185
	N	35	35	35	34
Access Control Process	Pearson's *r* correlation	0.118	0.245	0.233	1
	Sig. (2-tailed)	0.500	0.156	0.185	
	N	35	35	34	35

Table 5.16: Correlation between predictor variables and constant variables

5.8 ONE-WAY ANOVA ANALYSIS

ONE-WAY ANOVA analysis is a statistical technique that examines the effects of one independent variable on a dependent variable that test for significance of the difference between census means. Thus, ANOVA measures the difference in the dependent variables mean value, compared with that of the independent variable (Zikmund & Babin, 2013b). For this study, one-way ANOVA was selected because it is a parametric hypothesis test that compares mean scores of two or more independent variables described by one factor, to determine if they are equal (Coussement, Demoulin & Charry, 2011).

A one-way ANOVA at the p<.05 was conducted to compare the effect of information security tools in the ICT environment used by enterprises in the mining industry. An analysis of variance showed that the effect of information security tools used in the ICT environment, by enterprises in the mining industry, showed a statistically significant difference between groups was determined by one-way ANOVA at the p<.05 level for the three conditions, *[F* (4,31) = 3.87, *p* = 0.012*]*. An analysis of variance showed that the effect of information security protection features used by enterprises in the mining industry showed no statistically significant difference between groups was determined by one-way ANOVA at the p<.05 level for the three conditions, (*F* (4,30) = 1.23, *p* = 0.318).

An analysis of variance showed that the effect of information security management and executive funding used by enterprises in the mining industry showed no statistically significant difference between groups was determined by one-way ANOVA at the p<.05 level for the three conditions, *[F* (4,29) = 2.23, *p* = 0.090*]*. An analysis of variance showed that the effect of access control processes used by enterprises in the mining industry showed no statistically significant difference between groups was determined by one-way ANOVA at the p<.05 level for the three conditions, *[F* (4,28) = 0.63, *p* = 0.665*]*. Table 5.17 indicates the one-way frequency ANOVA analysis.

One-way ANOVA analysis						
	Source	Sum of squares	df	Mean square	F	Sig.
Information security tools in the ICT environment	Between groups	3.682	4	0.921	3.868	0.012
	Within groups	7.378	31	0.238		
	Total	11.060	35			
Information security protection features	Between groups	1.551	4	0.388	1.232	0.318
	Within groups	9.439	30	0.315		
	Total	10.990	34			
Information security management and executive funding	Between groups	8.557	4	2.139	2.229	0.09
	Within groups	27.826	29	0.96		
	Total	36.382	33			
Access control processes	Between groups	1.156	4	0.289	0.602	0.665
	Within groups	13.939	29	0.481		
	Total	15.096	33			

Table 5.17: Reporting a one-way ANOVA

5.9 CHAPTER SUMMARY

The general aim of this study was to propose an information security governance framework for the mining industry of South Africa. This chapter introduced the methods used to analyse and interpret the data that was collected from the census group. The results were used in various tabulated analytical outputs to present and identify meaningful variables. The results from the research question provided the study with useful insights into the information security governance and efficiency of information security protection in the South African mining industry to propose an information security governance framework.

The online secured web-based questionnaire was tested in the South African mining industry, and the data collected were available to the researcher to test the validity and internal reliability of the constructs. EFA was used to determine the underlying factorial structure and the Cronbach Alpha was used to establish the internal reliability of the factors. From the initial item reduction on the constructs, four factors were derived to test the effectiveness of information security of the ICT environments in the South African mining industry, namely:

Factor 1 – Information Security Tools

Factor 2 – Security Protection Features

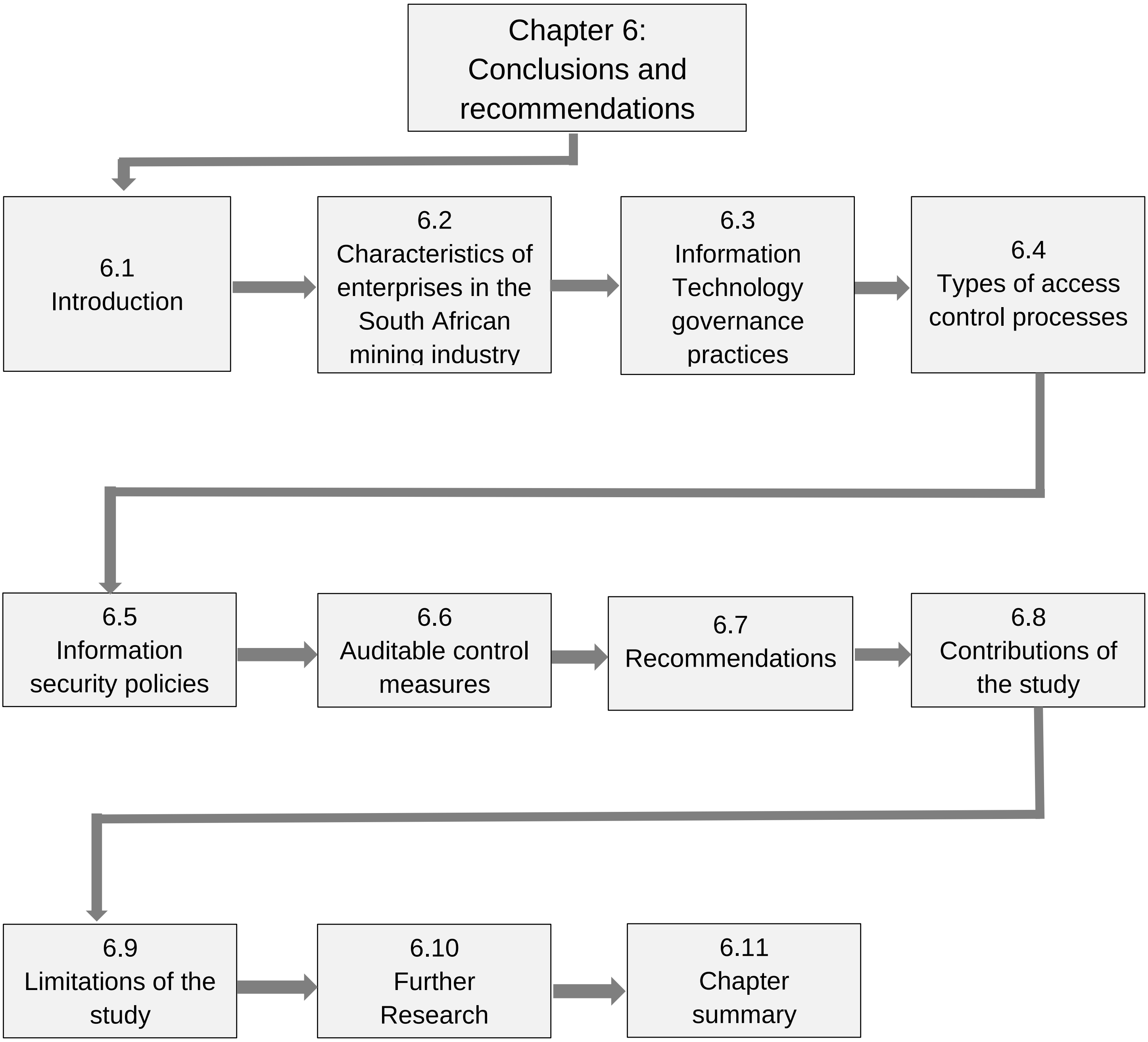
Factor 3 – Information security management

Factor 4 – Access control processes

The next chapter will outline the theoretical and practical contribution of the study, limitations of the study and make recommendations for further research. Chapter 6 will synthesise the analysis of the results to provide conclusions and recommendations.

CHAPTER 6: CONCLUSIONS AND RECOMMENDATIONS

This chapter discusses the conclusions and recommendations derived from the literature review and findings of this study. The discussion is followed by reviewing the characteristics of enterprises in the South African mining industry. The discussion reviews the contribution and limitations of the study and concludes with recommendations and further research proposals.


Chapter 6: Conclusions and recommendations
6.1 Introduction
6.2 Characteristics of enterprises in the South African mining industry
6.3 Information Technology governance practices
6.4 Types of access control processes
6.5 Information security policies
6.6 Auditable control measures
6.7 Recommendations
6.8 Contributions of the study
6.9 Limitations of the study
6.10 Further Research
6.11 Chapter summary

6.1 INTRODUCTION

This study examined cybersecurity and the probability of proposing an information security governance framework of ICT information systems in the South African mining industry and empirical research questions have been addressed. The proposed Information Security Governance Framework has been developed and discussed in chapter 6 which is a recommendation to enterprises. Furthermore, this chapter summarises the main findings, present general conclusions based on the findings of the research study and report its recommendations. Furthermore, this chapter will highlight the limitations of the study and suggest recommendations for future research studies.

Van den Berg, Van Zoggel, Snels, Van Leeuwen, Boeke, Van de Koppen, Van der Lubbe, Van den Berg and De Bos (2014) state that during the last 15-20 years, society has become strongly dependent on Information and Communication Technologies (ICT) systems with the creation of cyberspace. ICT refers to technologies that provide access to information through telecommunications. Moreover, due to the occurrence of several high-impact cybersecurity incidents, it is apparent that the new cyberspace not only offers benefits but also generates cyber-risks of all kinds. Thus, because of these developments, it has become necessary to balance cyber-opportunities and cyber-risks, (Van den Berg *et al.,* 2014).

6.2 CHARACTERISTICS OF ENTERPRISES IN THE SOUTH AFRICAN MINING INDUSTRY

South Africa is a world leader in mining. The country is famous for its abundance of mineral resources and accounts for a significant proportion of world production and reserves, making South African mining enterprises key players in the global industry (Kearney, 2012). The findings and the literature review indicate that most security professionals are Information and Communication Technology (ITC) and information security professionals. The results of this study indicate that South African mines have a presence throughout the country and are reliant on ICT tools and infrastructure as any other large corporation.

6.3 INFORMATION TECHNOLOGY GOVERNANCE PRACTICES

The aim of objective one was to determine if Information Technology (IT) governance practices were being used by enterprises in the mining industry. The IT governance practices that are used for this factor include but is not limited to information security protection tools and ICT environmental security scans which is significantly supported in this study. The findings and literature review are consistent with most studies, especially the IT governance that Lindros (2017) and Van Grembergen and De Haes (2018), point out as the management of IT security and protection tools, practices, and business processes in such a way that IT and business are integrated. The majority of the enterprises in this study conduct regular information security scans in their ICT environments.

Van Grembergen and De Haes (2018) state that in today’s global economy, enterprises have little choice but to invest in ICT security. The findings conversely support the literature review and findings in this study as it indicates that the majority of enterprises in the South African mining industry perform on-demand system software security scans for any vulnerabilities to align with information security protection practices. The implication of non-compliance with IT governance practices, essentially means that enterprises are at significant risk of losing their investments and missing key opportunities for growth, digital innovation, and market competitiveness (Van Grembergen & De Haes, 2018).

6.4 TYPES OF ACCESS CONTROL PROCESSES

The aim of objective two was to determine the types of information security access control processes that enterprises put in place to protect their information against any vulnerabilities. The study found three reliable factors that influence the information security access control processes significantly, namely, access control processes: protection in an antivirus security product and network security. The findings and literature review align significantly with the information security access control assessment, and as pointed out by Rouse (2018), who states that access control is a security technique that regulates *who* or *what* can be viewed or use resources in a computing environment. Moreover, access control is a fundamental concept in information security as it minimises risk to the enterprise.

The view of Rouse (2018), corroborate with the literature review and findings of this study, in support of information security access control assessments of which Martin (2018) states that access controls authenticate and authorise individuals to access the information they are allowed to see and use. The literature review and findings corroborate and support the view of Yeo, Cho, Kim & Vasilyevna (2008), who state that antivirus security products are multi-layered, integrated security software tool and perform well in conjunction with well-defined security policies. Moreover, according to Yeo *et al.* (2018), a software antivirus security product forms the foundation for effective enterprise security management.

The literature review and findings on network security, support the findings of this study, which is supported by Widup, Spitler, Hylender and Bassett (2018) who state that information security protection tools such as software, hardware and network security has defined features that are customised to enhance its functionality for optimal information security protection. Contrary to the excellent network security infrastructure in the South African mining industry, which is in accordance with Perkins (2018), who states that the management and executives in the South African mining industry are not easily convinced to fund security solutions.

Based on the literature review and findings of the factors in this section, it can thus be concluded that enterprises in the South African mining industry have an absolute appreciation and support for information security access control processes. Thus, enterprises in the South African mining industry should be encouraged to embrace the access control process to protect their critical information against any vulnerabilities. However, Martin (2018) states that the implication of weak or non-enforcement of information security access control policies exposes enterprises to risk with no data security, which could lead to data breaches. Martin (2018) states that in every data breach, information security access control policies are among the first controls that are investigated.

6.5 INFORMATION SECURITY POLICIES

The aim of objective three was to determine if enterprises in the South African mining industry have information security policies in place to govern their cybersecurity environment. The study found that there was one reliable factor that influenced the information security policies insignificantly. The results indicated that most enterprises did not have the required information security policies and governance documents in place and affected this finding negatively. There was a spread of governance documents amongst some enterprises, but this would not comply with audit and regulatory requirements.

This result was not significant, and it can therefore not be conclusively stated that enterprises are risk-averse and have the required and correct information security policies. It can thus be concluded that most if not all enterprises in the South African mining industry require information security policies as this will enable these enterprises to manage their IT governance processes effectively, efficiently and comply with audit and regulatory requirements. The information security governance framework that has been developed and presented in chapter 6 will rectify this deficiency.

6.6 AUDITABLE CONTROL MEASURES

The aim of objective four was to determine if enterprises in the South African mining industry have auditable control measures in place to govern their cybersecurity environment. The study found five valid and reliable factors that significantly influence the auditable control measures used by enterprises in the mining industry, namely information protection tools; system security updates; system security scans, antivirus security products, network security and access control processes in information security. Most of these findings were underpinned by auditable control measures, which is guided by IT information security governance frameworks.

The study further indicated that most of these factors positively influence the information security control measures to guard against any vulnerabilities in their ICT departments. However, the results of this factor, which were to determine if auditable control measures are in place, were weak and therefore not considered for further analysis. Although there was some evidence that suggests that auditable control measures are used, it is however not good enough for discussion. Auditable and general controls are normally reviewed by internal and external auditors, as they form the basis of the ICT control environment.

Based on the literature review and findings of this study, the auditable control measures were weak and unreliable. The implication of weak and unreliable auditable control measures according to Mar, Johannessen, Coates, Wegrzynowicz and Andreesen (2012) leads to negative audit findings and exposes the enterprise against information security risks and data vulnerabilities. Thus, some of these factors encourage the adoption of valid and reliable auditable control measures, which is guided by a policy, procedure, and controls in an information governance framework (Mar *et al.,* 2012). The information security governance framework that has been developed and presented in chapter 6 will rectify this deficiency.

6.7 RECOMMENDATIONS

The recommendations were reached based on the data analysis, literature, methodology, results, data analyses, findings, limitations, and conclusions that have become evident during the analysis of the statistical results. Enterprises in the South African mining industry should:

- Define and provide cybersecurity awareness programmes to enterprises.
- Ensure end-users are familiar with the Information security policies, standards, and procedures by using social media, intranet webpages, workshops, electronic mail, and meetings as these are the most widely used communication methods.
- Ensure security professionals and administrators are adequately trained and are aligned with new cyber-risk developments.
- Install and regularly update the antivirus computer software on all workstations and equipment in the ICT environment.

- Adopt effective cyber security standards throughout the ICT environment of the enterprise, including user workstations.
- Perform regular security penetration tests to test for any vulnerabilities within the ICT environment and system landscape.
- Enforce safe and secure password practices amongst computer users, as a large number of data breaches occur because of weak, lost or stolen user passwords.
- Ensure that the ICT environment is audited (internal and external) once a year for any security vulnerabilities.
- Ensure the board of directors and senior management support all information security programmes.
- Ensure funding is made available to support all information security programmes.
- Adopt valid and reliable information security policies and procedures to align with auditable control factors in an established ISG framework.
- Ensure that enterprises in the South African mining industry should:
  - Have ICT environmental recovery strategies defined and in place in the event of a security breach?
  - Have a full system backup and restoration strategy in place so that corrupt, deleted, or stolen data can be recovered.
  - Store backed data separately and test restores regularly.
  - Have security alerts defined and a procedure to act swiftly should there be a detection of an attempt to breach security?

6.8 CONTRIBUTION OF THE STUDY

This study aimed to determine if enterprises in the South African mining industry have a well-defined information systems security governance framework to mitigate any information security risks and vulnerabilities. To achieve this aim, the study established methods that enterprises in the South African mining industry use to protect sensitive and classified information in their ICT environments, which is critical for enterprises to achieve their strategic business objectives and attain growth opportunities. The study revealed that enterprises in the South African mining industry conform and comply with information security governance practices, however, there were deficiencies identified in these enterprises, namely, a lack of auditable control measures and security policies.

The study further established that information auditable control measures and security policies influenced the management of information security governance insignificantly. Moreover, the study established that there are factors that influence information security in the South African mining industry positively and negatively. Theoretically, this adds to the existing knowledge in the field of cybersecurity risks and mitigation controls, including information technology security governance, and policy and business process control frameworks. Practically, mining enterprises will have a list of cybersecurity risk factors, information security control frameworks, information security governance and risk mitigation controls, auditable policies and procedures as well as an information security governance framework that will help enterprises to protect their ICT environments more securely, efficiently and effectively.

6.9 LIMITATIONS OF THE STUDY

This study has the following limitations:

- The study was limited to the South African mining industry and may not be generalised to other industries, enterprises, or countries.
- The study was limited to one respondent per enterprise in the South African mining industry.
- The study only focussed on cybersecurity and no other business continuity strategies within ICT environments were considered for this study.

- The South African mining industry is diverse; however, it is concentrated to a limited amount of listed mining enterprises on the Johannesburg Stock Exchange.

The next section will outline further research options.

6.10 FURTHER RESEARCH

Based on the data analysis, literature, methodology, results, data analysis, findings, limitations and conclusions of this study, the following further studies may be conducted:

- Research cybersecurity throughout all industries and enterprises that are linked to a network environment, to encompass a more diverse research group in an enterprise ICT environment.

- Research the information security policy control documents that enterprises have in place.

- Research the benefit of implementing an IT governance control framework.

- Research studies can be expanded beyond the South African environment as this could be useful for enterprises that have a presence in other countries.

This section concludes with the chapter summary.

This study explored factors that could identify cyber security deficiencies in the South African mining industry. Moreover, the study developed and proposed an information security governance framework. To this point, this resulted in a limited number of participants who conducted the research survey.

6.11 CHAPTER SUMMARY

The conclusions of the literature review and empirical study were discussed to emphasise the accomplishments of the specific research objectives discussed in chapter 1 of this study. Conclusions regarding cyber security in the South African mining industry were outlined. The study further proposes developing an information security governance framework that security champions can review and align with their current frameworks or define a greenfield framework implementation.

The limitations identified areas that the researcher was unable to explore, however, these limitations were defined in future research studies. The study gives an empirical understanding by explaining which factors influence the management of cyber security within the mining industry in South Africa. The original contributions made and articulated by all the participants can now be used to support the adoption of an information security governance framework by enterprises in the South African mining industry. For this study, the primary objective was achieved with the development of an information security governance framework. The research journey was an invaluable knowledge seeking and gained experience and hope the reader find value in reading this dissertation.

REFERENCE LIST

Ablon, L., Libicki, M.C. & Golay, A.A. (2014). *Markets for cybercrime tools and stolen data: Hackers' bazaar.* Santa Monica, CA: Rand Publications.

Adams, M. & Makramalla, M. (2015). *Cyber security skills training: An attacker centric gamified approach*. Available from: http://timreview.ca/article/861 [9 June 2016]

Aggarwal, P., Arora, P., Neha, N. & Poonam, J. (2014). *Review on cybercrime and security*. Available from: http://mgijournal.com/PDF/REVIEW%20ON%20CYBER%20CRIME%20AND%20SECURITY.pdf [29 May 2016]

Agustini, M.Y.D.H. (2018). *Survey by knocking the door and response rate enhancement technique in international business research*. Available from: https://businessperspectives.org/images/pdf/applications/publishing/templates/article/assets/10327/PPM_2018_02_Agustini.pdf [12 July 2019]

Ahmad, A., Maynard, S.B. & Park, S. (2012). *Information security strategies: towards an organisational multi-strategy perspective*. USA: Springer.

Akhgar, B. & Brewster, B. (2016). *Combatting cybercrime and cyberterrorism*. AG Switzerland: Springer.

Akhgar, B., Staniforth, A. & Bosco, F. (Eds.) (2012). Cyber-crime and cyber terrorism investigators handbook. SearchSecurity/TechTarget (Bookshelf). Available from: http://searchsecurity.techtarget.com/feature/Cyber-Crime-and-Cyber-Terrorism-Investigators-Handbook. [10 June 2016].

Alfreds, D. (2015) Negligence the 'main reason' for cyber hacking..*FinTech24;* 10 July 2015. Available from: https://www.fin24.com/Tech/News/Negligence-the-main-reason-for-cyber-hacking-20150709. [23 July 2016].

Altheide, D.L. & Johnson, J.M. (1994). Criteria for assessing interpretive validity in qualitative research. In: Denzin, N.K. & Y. Lincoln, S. (Eds.) *Handbook of qualitative research.* Thousand Oaks, CA, US: Sage Publications.

Amir, Uzair. (2016). Anonymous hacks South African job portal against child labour. *HackRead News Platform*; February 11th, 2016. Available from: https://www.hackread.com/anonymous-hacks-south-african-job-portal-against-child-labour/. [16 March 2016].

Anastasiadou, S.D. (2011). Reliability and validity testing of a new scale for measuring attitudes toward learning statistics with technology. *Acta Didacta Napocensia;* 4(1); 2011. Available from: https://files.eric.ed.gov/fulltext/EJ1054957.pdf. [3 March 2019].

Andreasson, K. (Ed.) (2012). *Cybersecurity: Public sector threats and responses*. New York: Auerbach Publications.

Andress, J. & Winterfeld, S. (2011). *Cyber warfare: Techniques, tactics and tools for security practitioners*. Waltham, MA: Elsevier.

Antin, D. (2013). The South African mining sector: An industry at a crossroads. *Hanns Seidel Foundation Southern Africa; Economy Report South Africa;* December 2013*.* Available from: https://southafrica.hss.de/fileadmin/user_upload/Projects_HSS/South_Africa/170911_Migration/Mining_Report_Final_Dec_2013.pdf. [26 September 2016].

Antonopoulos, G.A. (2016). *Illegal entrepreneurship, organised crime and social control*. Switzerland: Springer International publishing.

Ashford, W. (2014). W*eb-based attacks double in 2013. Computer Weekly/News; 5 March, 2014*. Available from: http://www.computerweekly.com/news/2240215548/Web-based-attacks-double-in-2013-study-finds. [10 May 2016].

Ashford, W. (2014). *Over a hundred cyber criminals arrested in global operation*. *Computer Weekly/News; 28 November 2014*. Available from: http://www.computerweekly.com/news/2240235526/Over-a-hundred-cyber-criminals-arrested-in-global-operation. [10 July 2016].

Baan, P. (2014). *Enterprise information management*. New York, USA: Springer.

Babu, A.R., Singh, Y.P. & Sachdeva, R K. (2014). *Establishing a management information system*. *Food and Agriculture Organisation (FAO)/Digital Report, UN (Chapter 18).* Viewed: 23 November 2015. Available from: http://www.fao.org/docrep/w5830e/w5830e0k.htm.

Bailey, T., Del Miglio, A. & Richter, W. (2014). *The rising strategic risks of cyber-attacks. McKinsey Digital/McKinsey Quarterly; May 2014*. Available from: http://www.mckinsey.com/business-functions/business-technology/our-insights/the-rising-strategic-risks-of-cyberattacks. [2 March 2016]

Bandyopadhyay, Debasis. (2012). *Study of attitude and perception of medical students regarding the medical curriculum and syllabus in a teaching medical college of eastern India. Journal of Drug Delivery & Therapeutics*; 2(6):149-156; 2012. Available from: jddtonline.info/index.php/jddt/article/viewFile/604/352. [20 August 2016]

Bartholomew, D., Knott, M. & Moustaki, I. (2011). *Latent variables model and factor analysis*. 3rd Edition. London, UK: John Wiley & Sons.

Baum, S. & Mahizhnan, A. (2014). *E-Governance and social inclusion: Concepts and cases*. USA: IGI Global.

Baxter, R. (2016). Mine SA 2016: Facts and figures: Pocketbook. *Chamber of Mines of South Africa.* Available from: https://www.mineralscouncil.org.za/industry-news/publications/facts-and-figures/send/17-facts-and-figures/390-facts-and-figures-2016. [11 October 2016].

Bayazit, H. (2016). *The role of state ownership in media concentration*. Available from: http://www.citicolumbia.org/events/2015/whoowns.html. [11 June 2016].

Bayuk, J.L., Healey, J., Rohmeyer, P., Sachs, M.H., Schmidt, J. & Weiss, J. (2012). *Cyber security policy guidebook*. Hoboken, NJ: John Wiley & Sons/UK: Gower Publishing. [Charles Sturt University; Library Electronic Resources]. Available from: http://www.csuau.eblib.com.ezproxy.csu.edu.au/patron/Read.aspx?p=818205&pg=19. [17 June 2016].

Beal, V. (2016). Network security. *Webopedia/Browse Terms.* Available from: http://www.webopedia.com/TERM/N/network_security.html. [19 April 2016].

Beale, I. (2015). Lloyd's CEO: *Cyber-attacks cost companies $400 billion ever year. Fortune;* January 23, 2015. Available from: http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/. [14 June 2016].

Beck, R.B. (2014). *The history of South Africa*. 2nd Edition. California, USA: ABC-CLIO Press.

Beissel, S. (2016). *Cybersecurity investments*. Switzerland: Springer.

Bell, J. (2010). Doing your research project*. A guide for first time researchers in Education, Health and Social Science*. 5th Edition. Maidenhead, UK: Open University Press/McGraw-Hill.

Bellis, M. (2016). Inventors of the modern computer. *ThoughtCo.* [Updated: September 24, 2018.] Available from: http://inventors.about.com/library/weekly/aa091598.htm. [17 June 2016].

Benny, D.J. (2014). *Industrial espionage*. Boca Raton, FL, USA: CRC Press.

Bernik, I. (2014). *Cybercrime and cyber warfare*. NJ, USA: John Wiley & Sons.

Blair, B.T. (2015). *Information governance executive briefing book*. *Mimage/Opentext.com; Via Lumina.* Available from: http://mimage.opentext.com/alt_content/binary/pdf/Information-Governance-Executive-Brief-Book-OpenText.pdf. [11 October 2016].

Blair, J., Czaja, R.F. & Blair, E.A. (2013). *Designing surveys: A guide to decisions and procedures.* Sage Publications.

Bloomberg South Africa. (2014). South African economy contracts first time since 2009 recession*. Bloomberg/Business;* 27 May 2014. Available from: http://www.bloomberg.com/news/2014-05-27/south-african-economy-contracts-first-time-since-2009-recession.html. [16 June 2014].

Bodhani, A. (2013). Ethical hacking: Bad in a good way*. E & T Engineering and Technology*. Available from:

https://eandt.theiet.org/content/articles/2012/12/ethical-hacking-bad-in-a-good-way/. [17 December 2017].

Bourgeois, D.T. (2014). *Information systems for business and beyond*. Saylor.org/The Saylor Academy; Open Textbook Challenge. Available from: http://www.saylor.org/site/textbooks/Information%20Systems%20for%20Business%20and%20Beyond.pdf. [11 January 2016].

Bourgeois, D., & Bourgeois, D. T. (2014). *Information systems for business and beyond*. Available from: https://bus206.pressbooks.com/chapter/chapter-6-information-systems-security/. [30 October 2021].

Braekman, E., Berete, F., Charafeddine, R., Demarest, S., Drieskens, S., Gisle, L., Molenberghs, G., Tafforeau, J., Van der Heyden, J. & Van Hal, G. (2018). Measurement agreement of the self-administered questionnaire of the Belgian health interview survey. *PLOS ONE Peer-reviewed Journal: Public Library of Science.* Paper-and-pencil versus web-based mode. Available from: https://pdfs.semanticscholar.org/989c/dc46a1e5d91111da2de11eb26874072c0794.pdf?_ga=2.40870562.1024361234.1562107930-1547353483.1559571466. [21 February 2016].

Brand South Africa [Official Custodian of South Africa's Nation Brand]. (2014). *South Africa on mining investment attractiveness index.* Available from: https://www.brandsouthafrica.com/investments-immigration/business/investing/mining-050314. [29 May 2014].

Brems, M. (2017). A one-stop shop for principle component analysis. *Medium: Towards Data Science;* April 17, 2017. Available from: https://towardsdatascience.com/a-one-stop-shop-for-principal-component-analysis-5582fb7e0a9c. [7 March 2019].

Brenner, S.W. (2012). *Cybercrime and the law: Challenges, issues, and outcomes*. New England: Boston, MA: North Eastern University Press.

Brewster, B., Kemp, B., Galehbakhtiari, S. & Akhgar, B. (2015). *Cybercrime: attack motivations and implications for big data and national security*. Waltham, MA, USA: Elsevier.

Broadhurst, R., Grabosky, B., Alazab, M. & Chon, S. (2014). Organisation and cybercrime: An analysis of the nature of groups engaged in cybercrime. *International Journal of Cyber Criminology*; 8(1); January – June 2014. Available from: http://www.cybercrimejournal.com/broadhurstetalijcc2014vol8issue1.pdf. [4 May 2016].

Brodie, N. (2014). How does cyber-crime affect you. *Men's Health: Guy Skills Section;* 15 May 2014. Available from: http://www.mh.co.za/how-to/guy-wisdom/how-does-cybercrime-affect-you/. [11 May 2016].

Brown, I. & Marsden, C.T. (2013). *Regulating code: Good governance and better regulation in the information age*. London, England: MIT Press.

Brown, J.D. (2009). Choosing the right type of rotation in PCA and EFA. *Shiken: JALT Testing & Evaluation SIG Newsletter;* 13(3):20-25; November 2009. University of Hawai'I at Manoa: Statistics Corner.

Brown, K. (2015). In: Internet Society (2015). 2015 Global Internet Report (GIR): Mobile is key to fulfilling the promise of Internet connectivity for the next billion people. *Internet Society;* 7 July 2015. Available from: https://www.internetsociety.org/history/2015/internet-societys-2015-global-internet-report-mobile-is-key-to-fulfilling-the-promise-of-internet-connectivity-for-the-next-billion-people-2015-gir/. [27 April 2016].

Bryman, A. & Bell, E. (2011). *Business research methods.* 3rd Edition. New York: Oxford University Press.

Buecker, A., Amado, J., Druker, D., Lorenz, C., Muehlenbrock, F. & Tan, R. (2010). *IT security compliance management design guide*. 2nd Edition. USA: IBM Redbooks Publication.

Bullock, J.A., Haddow, G.D. & Coppola, D.P. (2013). *Introduction to homeland security: Principles of all-hazards risks*. MA, USA: Elsevier.

Burg, S.S. (2007). *An investigation of dimensionality across grade levels and effects on vertical linking of elementary grade mathematics achievement tests*. Unpublished doctoral thesis, University of North Carolina, Chapel Hill.

Available from: https://tspace.library.utoronto.ca/bitstream/1807/72948/1/Brochu_Pierre_201606_EdD_thesis.pdf. [24 August 2015].

Cable News Network (CNN). (2015). Nearly 1 million new malware threats released every day. *CNN Business/Money;* April 14, 2015;. Available from: http://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/. [12 August 2015].

Carter, W.A. & Zheng, D.E. (2015). The evolution of cyber security requirements for the U.S. financial industry. A Report of the Center for Strategic & International Studies (CSIS) Strategic Technologies Program; July 2015. Available from: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/150717_Carter_CybersecurityRequirements_Web.pdf. [28 June 2015].

Cattell, R.B. (1966). The scree test for the number of factors*. Multivariate Behavioral Research Journal*; 1(2), 1996. Available from: https://www.tandfonline.com/doi/abs/10.1207/s15327906mbr0102_10?journalCode=hmbr20. [29 March 2019].

Cevidalli, A. & Austen, J. (2010). The challenge of combating organised crime. *Computer Weekly;* December 2010. Available from: http://www.computerweekly.com/feature/A-new-approach-to-fighting-varied-types-of-cybercrime-cases. [11 May 2016].

Chamber of Mines of South Africa. (2011). Chamber of mines commends industry on safety initiatives*. Africa Business Communities;* 11 January 2011. Available from: https://africabusinesscommunities.com/news/chamber-of-mines-commends-industry-safety-initiatives/. [18 June 2014].

Chamber of Mines of South Africa. (2013). *Facts and figures*. Viewed: 18 June 2014, Available from: http://chamberofmines.org.za/media-room/facts-and-figures.

Chapple, K. (2016). Managing change in IT security policies. *TechTarget/SearchSecurity Network.* Available from:

http://searchsecurity.techtarget.com/tutorial/IT-security-policy-management-Effective-polices-to-mitigate-threats. [10 July 2016].

Charney, S. (2016). Cybersecurity norms for nation states-states and the global ICT industry. *Microsoft On The Issues: Official Microsoft Blog;* June 26, 2016. Available from: http://blogs.microsoft.com/on-the-issues/2016/06/23/cybersecurity-norms-nation-states-global-ict-industry/#sm.0001lrn1n1b70czh11aeu4qw89cxt. [18 July 2016].

Chen, J. (2014). "Salad words" spam run exploits unlikely resources. *TrendMicro/Security Intelligence Blog*; August 29, 2014. Available from: http://blog.trendmicro.com/trendlabs-security-intelligence/author/jeanchen/. [13 June 2016].

Chesley, D. (2016). Turnaround and transformation in cybersecurity: Key findings from The Global State of Information Security Survey 2016. *PRICEWATERHOUSECOOPERS (PWC),* United States. Available from: https://www.pwc.com/sg/en/publications/assets/pwc-global-state-of-information-security-survey-2016.pdf. [1 June 2016].

Chidambaram, V. (2012). The profile of a cyber-criminal. *TechAdvisor*, *IDG UK*; 13 January 2012. Available from: http://www.pcadvisor.co.uk/news/security/profile-of-cyber-criminal-3330068/. [13 April 2016].

Choucri, N. (2012). *Cyber politics in international relations*. In: Talihärm, A-M. (2013). Towards cyberpeace: Managing cyberwar through international cooperation. *UN Chronicle: The Magazine of the United Nations,* L(2); August 2013. Available from: http://unchronicle.un.org/article/towards-cyberpeace-managing-cyberwar-through-international-cooperation/. [11 June 2016].

Christensson, P. (2015). Internet definition. *TechTerms.com.* Viewed: 27 April 2016. Available from: https://techterms.com/definition/internet.

CISCO The Network. *Cisco 2014 Annual Security Report*. (2014). Released: January 16, 2014. Available from: https://www.cisco.com/c/dam/assets/global/UK/pdfs/executive_security/sc-01_casr2014_cte_liq_en.pdf. [11 September 2016].

Clarke, R.A. & Knake, R. (2012). *Cyber war: The next threat to national security and what to do about it*. New York: Ecco Publications.

Clemente, D. (2013). *Cyber security and global interdependence: What is critical?* London, UK: Royal Institute of International Affairs/Chatham House; February 2013. Available from: https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/0213pr_cyber.pdf. [22 June 2016].

Cohen, L., Manion, L. & Morrison, K. (2011). *Research methods in education*. 7th Edition. London: Routledge.

Collins, H. (2010). Creative research: *The theory and practice of research for the creative industries*. London: Thames & Hudson.

Coraggio, S., Rogers, J., Hilgeman, N. (2014). NIST cybersecurity framework: Implementing the framework profile. *Commercial Solutions: Booz-Allen-Hamilton.* Available from: http://www.boozallen.com/content/dam/boozallen/documents/Viewpoints/2015/07/nist-cybersecurity-framework.pdf. [16 January 2016].

Cortina, J.M. (1993). What is coefficient alpha*.* An examination of theory and applications. *Journal of Applied Psychology*; 78(1):98-104. Available from: https://pdfs.semanticscholar.org/2e9a/ccd64f810f9ae12ab35d905e43ecea35b85a.pdf. [25 March 2019].

Costello, A.B. & Osborne, J.W. (2005). Best practices in exploratory factor analysis: Four recommendations for getting the most from your analysis. *Practical Assessment Research & Evaluation [Peer-reviewed electronic journal].,* Viewed: 28 February 2019*.* Available from: http://pareonline.net/pdf/v10n7a.pdf.

Coulson, M. (2011). *An insider's guide to the mining sector*. UK: Harriman House.

Coussement, C., Demoulin, N. & Charry, K. (2011). *Marketing research with SAS enterprise guide*. England: Gower Publishing.

Cowan, D. (2015). Cybersecurity – *The failure of cyber security and the startups who will save us*. Available from: https://seriouslyvc.com/2015/01/the-failure-of-cyber-security-and-the-startups-who-will-save-us/. [17 May 2016].

Creswell, J. W. (2012). *Qualitative inquiry and research design*. 3rd Edition. Toronto, Canada: Sage.

Creswell, J.W. & Plano Clark, V.L. (2011). *Designing and conducting mixed methods research*. 2nd Edition. Los Angeles, USA: Sage Publications.

Criddle, L. (2016). What is social engineering? Examples & prevention tips. *Webroot: Smarter Cybersecurity.* Available from: https://www.webroot.com/za/en/resources/tips-articles/what-is-social-engineering. [11 May 2016].

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. & Baskerville, R. (2013). *Future directions for behavioural information security research*. Oxford, UK: Elsevier Advanced Technology Publications.

Davenport, J. (2013). *Digging deep: A history of mining in South Africa*. UK: Jonathan Ball Publishers.

Davis, A. (2015). Building cyber-resilience in supply chains. *Technology Innovation Management (TIM) Review;* April 2015. Available from: http://timreview.ca/sites/default/files/Issue_PDF/TIMReview_April2015.pdf. [9 June 2016].

De Beer J.H. (2015). *The history of geophysics in Southern Africa*. Stellenbosch, South Africa: Sun Press.

De Rebus. (2019). Do you have insurance for cybercrime? *De Rebus;* April 2019; Journal of the Law Society of South Africa. Article by Sedutla, M. Available from: http://www.derebus.org.za/do-you-have-insurance-for-cybercrime/ (See also: Law Society of South Africa., 2019.). [1 October 2019].

Dean, D., DiGrande, S., Field, D. & Zwillenberg, P. (2012). The digital manifesto. *The Boston Consulting Group (BCG);* January 2012. Available from: https://www.bcg.com/documents/file96476.pdf. [22 November 2015].

Deegan, B. (2009). King III at a glance: Steering Point. *PricewaterhouseCoopers (PWC): Corporate Governance Series.* September 2009. Available from: https://www.saica.co.za/Portals/0/documents/PWC%20SteeringPoint%20KingIII.pdf. [10 July 2016].

Denscombe, M. (2010). *Social research: Guideline for good practice*. 2nd Edition. Glasgow: Bell & Bain.

Department of Mineral Resources (DMR). (2014). *List of Licenced Mining Organisations.* Available from: http://www.dmr.gov.za/. [20 September 2014].

Department of Mineral Resources (DMR). (2016). *Mineral Resources.* Available from: http://www.gov.za/about-SA/minerals. [19 September 2016].

Department of Science and Technology (DST). (2014). *Technology innovation*. Available from: http://www.dst.gov.za/index.php/aboutresearch. [23 June 2014].

Department of State Security (DSS). (2015). *Budget Vote for Department of State Security*; by Hon. David Mahlobo MP, Minister of State Security, Parliament of Republic of South Africa. Cape Town, 5 May 2015. Available from: http://www.ssa.gov.za/Portals/0/SSA%20docs/Speeches/2015/State%20Security%20Budget%20Vote%2005%20May%202015.pdf. [17 August 2017].

DeVellis, R.E. (2006). *Scale development: theory and application. applied social science research method series*. Newbury Park: SAGE Publishers.

Deverell, J. (2014). Lock down cybersecurity or face another *Heartbleed* – or worse. *Conversation AU;* May 5, 2014*.* (Commonwealth Scientific & Research Organisation; CSIRO.) Available from: http://theconversation.com/lock-down-cybersecurity-or-face-another-Heartbleed-or-worse-26237. [12 June 2016].

Devi, S. & Rather, M.A. (2016). Emergence of cyber security and transformations in the world order (2016). *International Journal of Innovative Knowledge Concepts (IJIKC);* (4)3; March 2016*.* Available from: http://www.ijikc.co.in/index.php/ijikc/article/view/161. [23 June 2016].

Dicks, J. (2012).*Uncover the secret scams and tricks to profit in the world's largest financial market.* USA: McGraw-Hill.

Dodds, R. (2012). How does information security fit into a governance framework? *ISACA Online Journal, Past-issues.* Available from: http://www.isaca.org/Journal/Past-Issues/2005/Volume-4/Documents/jopdf054-how-does-info.pdf. [27 April 2014].

Dogaru, O. (2012). *Securing critical infrastructures*. Available from: https://www.academia.edu/14172231/osint_in_the_globalization_of_the_access_to_information. [9 June 2016].

Donnelly, C. (2015). *Chinese hackers to blame for 10-year cyber espionage campaign, says FireEye. Computer Weekly;* 13 April 2015. Available from: http://www.computerweekly.com/news/4500244242/Chinese-hackers-to-blame-for-10-year-cyber-espionage-campaign-says-FireEye. [9 July 2016].

Drolet, M. (2016). 5 Cybersecurity trends to watch for 2016. *CSO Online – News, analysis & research on security and risk management.* Available from: http://www.networkworld.com/article/3019235/security/5-cybersecurity-trends-to-watch-for-2016.html. [17 May 2016].

Dunham, R. (2018). Information security policies: Why they are important to your organisation. *Lindford & Co – CPA Firm.* April 25, 2018. Available from: https://linfordco.com/blog/information-security-policies/. [3 May 2019].

Dupont, B. (2013). Cyber security futures: How can we regulate emergence risks. Technology Innovation Management Review; 3(7):6-11. Available from: http://doi.org/10.22215/timreview/700. [22 June 2016].

Eardley, M. (2011). £16,8 billion lost to theft of corporate secrets in the UK. *Security SA/High Tech Security Solutions;* April 2011 [Cyber Security/Mining Industry]. Available from: http://www.securitysa.com/article.aspx?pklarticleid=6710 [See also: Security SA, 2011.]. [28 February 2015].

Edelbacher, M., Kratcoski, P.C. & Dobovsek, B. (2016). *Corruption, fraud, organised crime and the shadow economy*. NY, USA: CRC Press.

Elliot, M. (2014). Deep impact: Protecting mining operations from cyber-attacks*.* *Mining Technology;* 6 February 2014*.* Available from: http://www.mining-technology.com/features/featuremining-cyber-attacks-mike-elliott-ernst-young-4171663/. [28 June 2014].

Elis, N. (2014). Can big data predict the next cyber-attack? *The Jerusalem Post;* May 12, 2014. Available from: http://www.jpost.com/enviro-tech/can-big-data-predict-the-next-cyber-attack-351957. [7 May 2016].

Ellyatt, H. (2015). Top 5 cyber-security risks for 2015. *CNBC Tech*; 5 January 2015. Available from: http://www.cnbc.com/2014/12/19/top-5-cyber-security-risks-for-2015.html. [17 May 2016].

Ernst & Young Global (2013). Security incidents up for 51% of Canadian businesses, 2013 EY Survey. *EY.com: Building a better working world.* Available from: http://www.ey.com/CA/en/Newsroom/News-releases/2013-Global-Information-Security-Survey. [25 November 2015].

Ernst & Young (2013b). Cyber hacking and information security in mining. *EY.com: Building a better working world.* Available from: http://www.ey.com/GL/en/Industries/Mining---Metals/EY-Cyber-hacking-and-information-security-in-mining. [16 June 2014].

Ernst & Young Global (2013c). *Global Review 2013*. *EY.com: Building a better working world.* Available from: http://www.ey.com/Publication/vwLUAssets/EY_Global_review_2013/$FILE/EY_Global_review_2013.pdf. [13 June 2016].

Ernst & Young. (2014). *Cyber hacking and information security: mining and metals.* In*: Global Information Security Survey 2013/2014.* Available from: https://www.ey.com/Publication/vwLUAssets/EY-Cyber-hacking-and-information-security/$FILE/EY-Cyber-hacking-and-information-security.pdf. [16 August 2014].

Fabrigar, L.R., Wegener, D.T., MacCallum, R.C. & Strahan, E.J. (1999). Evaluating the use of exploratory factor analysis in psychological research. *Psychological*

Methods Journal; Psychological Methods, 4(3):272-299. Available from: https://psycnet.apa.org/record/1999-03908-004. [16 September 2019].

Fedderke, J. & Pirouz, F. (2013). *The role of mining in the South African economy.* Economic Research Southern Africa (ERSA), University of the Witwatersrand, Johannesburg, South Africa. Available from: http://www.econrsa.org/system/files/publications/policy_papers_interest/pp09_interest.pdf. [19 September 2016].

Felix, J., Joseph, C. & Ghorbhani, A. (2012). *Group behaviour metrics for p2p botnet detection in information and communications security*. In: Chim, T. & Yuen, T. (Eds.) *Information and Communications Security.* Vol. 7618, pp. 93-104. Berlin/Heidelberg, Germany: Springer.

Finklea, K. & Theohary, C.A. (2015). *Cybercrime: Conceptual issues for Congress and U.S. Law Enforcement*. Congressional Research Service; January 25, 2015. Available from: https://www.fas.org/sgp/crs/misc/R42547.pdf. [30 June 2016].

Finley, A. (Ed.) (2011). *Global Information Society Watch 2011: Internet rights and democratisation*. Goa, India: Dog Ears Books & Printing/South Africa: APC & Hivos. Available from: https://docplayer.net/120455762-Global-information-society-watch-2011.html. [3 June 2018].

Floyd, J. & Fowler, J.R. (2013). *Survey research methods*. Boston, USA: University of Massachusetts/Sage Publications.

Foody, M., Samara, M. & Carlbring, P. (2015). *A review of cyber bullying and suggestions for online psychological therapy*. *Science Direct;* September 2015; 2(3):235-242. Available from: http://www.sciencedirect.com/science/article/pii/S2214782915000251. [22 June 2016].

Forbes Custom. (2014). Cybersecurity – Confronting the threat of Shadow IT. *Forbes/Cybersecurity*; Article by: Prince, B.; 20 October 2014. Available from: http://www.forbes.com/custom/2014/10/20/cybersecurity/. [07 November 2014].

Fouka, G. & Mantzorou, M. (2011). What are the major ethical issues in conducting research? *Health Science Journal*, 5(1):3-14. Available from: http://www.hsj.gr/medicine/what-are-the-major-ethical-issues-in-conducting-research-is-there-a-conflict-between-the-research-ethics-and-the-nature-of-nursing.pdf. [17 August 2014].

Frank, C.B. (2015). Why is South Africa vulnerable to cyber-attacks. CapeTalk/567AM. 11 June 2015. In: Article by Ramphele, L. Available from: http://www.capetalk.co.za/articles/3231/why-is-south-africa-vulnerable-to-cyber-attacks. [8 March 2016].

Franks, P.C. (2013). *Records & information management*. USA: Neal-Schuman.

Fryer, V. (2015). In: *IT NEWS Africa.* South African companies plagued by cyber-attacks*. Security – Top Stories*; June 8, 2015. Available from: http://www.itnewsafrica.com/2015/06/south-african-companies-plagued-by-cyber-attacks/ (See also: IT News Africa.). [11 February 2016].

Gabel, D., Liard, B. & Orzechowski, D. (2015). Cyber risk: Why cyber security is important. *White & Case: Insight/Fintech/Technology Newsflash;* 1 July 2015. Available from: http://www.whitecase.com/publications/insight/cyber-risk-why-cyber-security-important. [27 June 2016].

Gad, M. (2014). Crimeware marketplaces and their facilitating technologies. *Technology Innovation Management (TIM) Review;* November 2014. Available from: http://timreview.ca/article/847. [6 June 2016].

Galvin, J.M. (2016). *Ground engineering, principles and practices for underground coal mining*. Switzerland: Springer International Publishing.

Gandel, S. (2015). Lloyd’s CEO: Cyber-attacks cost companies $400 billion every year. *Fortune;* January 23, 2015. Available from: http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/. [14 June 2016].

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q. & Laplante, P. (2011). Dimensions of cyber-attacks: cultural, social, economic, and political. *IEEE Technology & Society Magazine*; 30(1):28-38; Spring 2011. Available from: http://dx.doi.org/10.1109/MTS.2011.940293. [23 May 2016].

Garcia, T. (2019). *What are the information security controls*. Retrieved 30 October 2021. from https://reciprocity.com/resources/what-are-information-security-controls/.

Gartner Research Group. (2015). *Sourcing Governance Tames Complexity and Ensures Successful Multisourcing. Smarter With Gartner/Digital and Technology Trends;* May 26, 2015. Article contributor: Goasdaff, L. Available from: https://www.gartner.com/smarterwithgartner/governance-is-key-to-successful-multisourcing/. [7 May 2019].

Geers, K. (2011). *Strategic cyber security* Tallinn, Estonia: National Cooperative Cyber Defence Centre (CCDCOE); NATO Cooperative Cyber Defence Centre of Excellence.

Gercke, M. (2012). Understanding cybercrime: Phenomena, challenges and legal response. *ITU: Committed to Connecting the World.* Available from: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html. [3 November 2015].

Giles, J. (2015). Which organisations does POPI affect most? *Michalsons: Practical Legal Solutions – Focus Areas.* Available from: http://www.michalsons.co.za/focus-areas/privacy-and-data-protection/popi-act-protection-of-personal-information. [11 July 2016].

Gill, J. & Johnson, P. (2010). *Research methodology for managers*. 4th Edition. London: Sage.

Godin, S. & Imbeau, A. (2014) *Cybersecurity in modern critical infrastructure environments*. Canada: Québec.

Goodman, M. (2015) *Future crimes: Inside the digital underground and the battle for our connected world*. London: Transworld Digital.

Goodrich, M. & Tamassia, R. (2014). *Introduction to computer security*. 1st Edition. England: Pearson.

Gordhan, P. (2012) – See: Republic of South Africa (2012).

Government Gazette Number 37067, 2013. Republic of South Africa. (2013). *Protection of Personal Information Act, No. 4 of 2013. Cape Town.* Available from: http://www.justice.gov.za/legislation/acts/2013-004.pdf. [29 July 2016].

Gragido, W., Molina, D., Pierce, J. & Selby, N. (2012) *Blackhatonomics: An inside look at the economics of cybercrime*. Waltham, MA: Elsevier.

Granneman, J. (2013). Top 7 IT security frameworks and standards: Choosing the right one. *SearchSecurity/TechTarget.* Available from: http://searchsecurity.techtarget.com/tip/IT-security-frameworks-and-standards-Choosing-the-right-one. [12 January 2015].

Granville, K. (2015). 9 Recent cyberattacks against big businesses. *New York Times.* February 5, 2015. Available from: http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html?_r=1. [23 April 2016].

Grau, D. & Kennedy, C. (2014). TIM Lecture Series – The business of cybersecurity. *Technology Innovation Managemant (TIM) Review;* April 2014. Available from: http://timreview.ca/article/785. [13 May 2016].

Greene, S.S. (2014) *Security program and policies: Principles and practices*. 2nd Edition. USA: Pearson Education.

Griffith, C. (2015). Modernisation – a vital step in building a sustainable mining industry in South Africa. *Mining Indaba 2015 Speech; AngloAmerican*. Available from: http://southafrica.angloamerican.com/~/media/Files/A/Anglo-American-South-Africa-V2/documents/aa-mining-indaba-2015-speech-chris-griffith.pdf. [1 October 2016].

Griffith, E. (2016). What is Cloud computing? *PC Magazine Reviews*. May 3, 2016. Available from: http://www.pcmag.com/article2/0,2817,2372163,00.asp. [26 May 2016].

Griffiths, J. (2015). *Cybercrime costs the average U.S. firm $15 million a year*. *CNN/Money/Technology*. Available from: http://money.cnn.com/2015/10/08/technology/cybercrime-cost-business/. [29 June 2016].

Grigsby, A. (2014). Coming soon: Another country to ratify the Budapest convention. *Blog: Net Politics & Digital and Cyperspace Policy Program/Council on Foreign Relations;* December 11, 2014. Available from: http://blogs.cfr.org/cyber/2014/12/11/coming-soon-another-country-to-ratify-to-the-budapest-convention/. [2 May 2016].

Guinn, J. (2014a). Why you should adopt the NIST cybersecurity framework. PricewaterhouseCoopers (PWC). Available from: https://www.pwc.com/us/en/increasing-it effectiveness/publications/assets/adopt-the-nist.pdf. [10 January 2016].

Guinn, J. (2014b). Increasing IT effectiveness. *PricewaterhouseCoopers (PWC).* Available from: https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf. [1 July 2016].

Hair, J.F., Celsi, W., Money, M.W., Samouel, A.H. & Page, M. (2011). *Essentials of business research methods*. 2nd Edition. Armonk, New York: M.E. Sharpe.

Halder, D. & Jaishankar, K. (2011). Cyber-crime and the victimisation of women: laws, rights and regulations. *IGI Global.* Available from: http://www.igi-global.com/book/cyber-crime-victimization-women/50518#table-of-contents. [16 May 2016].

Han, C. & Dongre, R. (2014). What motivates cyber-attackers. *Technology Innovation Management (TIM) Review; October 2014.*Available from: http://timreview.ca/sites/default/files/article_PDF/HanDongre_TIMReview_October2014.pdf. [13 June 2016].

Hancock, T. (2016). Information security governance: Guidance for Boards of Directors and Ececutive Management. 2nd Edition. *IT Governance Institute; Knowledge Center.* Available from: https://www.isaca.org/Knowledge-Center/Research/Documents/Information-Security-Govenance-for-Board-of-Directors-and-Executive-Management_res_Eng_0510.pdf. [26 January 2019].

Harvey, C. & Press, J. (2013). *International competition and industrial change*. NY, USA: Routledge Press.

Harvey, C. (2014). $480m Bitcoin cyber-heist makes history. *Mail & Guardian;* March 7, 2014. Available from: http://mg.co.za/article/2014-03-06-480m-bitcoin-cyberheist-makes-history. [23 November 2015].

Hathaway, M.E. & Klimburg, A. (2012). *Preliminary considerations on national security*. In: Klimburg, A. (Ed.) (2012). *National Cyber Security Framework Manual.* Tallinn, Estonia: National Cooperative Cyber Defence Centre (CCDCOE). Available from: http://belfercenter.ksg.harvard.edu/files/hathaway-klimburg-nato-manual-ch-1.pdf. [7 June 2016].

Hathaway, O.A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W. & Spiegel, J. (2012). The Law of Cyber-Attack. *California Law Review;* 100:817. University of Pennsylvania. Available from: https://www.law.upenn.edu/live/files/6479-hathaway-oona-et-al-the-law-of-cyber-attack. [6 June 2017].

Haynes, M.C., Ryan, N., Saleh, M., Winkel, A.F. & Ades, V. (2017). Contraceptive knowledge assessment: methodological issue on reliability analysis. ScienceDirect; 96(4); October 2017. Available from: https://www.sciencedirect.com/science/article/pii/S001078241730058. [16 March 2019].

Holt, T.J. & Bossler, A.M. (2016). *Cybercrime in progress*. New York, USA: Routledge.

Houck, M., Crispino, F. & McAdam, T. (2012). *The science of crime scenes*. UK: Oxford.

Howe, W. (2016). A brief history of the Internet. *WaltHowe.com;* Updated: 23 August 2016. Available from: http://www.walthowe.com/navnet/history.html. [27 May 2016].

Hughes, G. (2015). *Information and communications technology policy*. Available from: https://home.greens.org.nz/policy/information-technology. [21 October 2016].

Humphreys, E.J. (2013). The new cyber warfare. *ISO;* 9 October 2013. Viewed: 11 January 2016. Available from:

http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref1785.

Ifinedo, P. (2013). Information systems security: An empirical study of the effects of socialization, influence, and cognition*. ScienceDirect; 51(1):69-79;* January 2014***.*** Available from: http://dx.doi.org/10.1016/j.im.2013.10.001. [17 August 2019].

Information Systems Audit and Control Association (ISACA*) (2010). Fundamentals of IT Governance Based on ISO/IEC 38500. Article by Hamidovich, H. 2010. ISACA Journal Online. Available from: https://www.isaca.org/Journal/archives/2010/Volume-5/Documents/10v5-online-fundamentals.pdf. See also: Information Technology Governance Institute (ITGI). (2010.). (See also: ISACA, 2010.). [9 September 2019].

Information Technology Solutions (ITS). (2014). *Paladion OnDemand.* Available from: http://www.paladion.net/IT_availability_solutions.html. [7 August 2014].

Information Technology Governance Institute (ITGI). (2010a). Fundamentals of IT governance based on IS Johannesburg Securities Exchange, 2011, Annual Report. Available from: http://www.isaca.org/About-ISACA/IT-Governance-Institute/Pages/default.aspx. [1 June 2014].

Information Technology Governance Institute (ITGI). ISACA. (2010b). Fundamentals of IT Governance Based on ISO/IEC 38500. Article by: Hamidovich, H. 2010. ISACA Journal Online. Available from: https://www.isaca.org/Journal/archives/2010/Volume-5/Documents/10v5-online-fundamentals.pdf. (See also: ISACA, 2010.). [9 August 2019].

Information Technology Governance Institute (ITGI) (2012). – See: Spremic, M. (2012).

Information Technology Governance Institute [TGI], ISACA. (2014). IT Governance Roundtable: Defining IT Governance. ISACA Research. Available from: http://www.isaca.org/Knowledge-Center/Research/Documents/Defining-IT-Governance-Brisbane-Australia_res_Eng_0810.pdf. (See also: ISACA, 2014.). [21 July 2019].

Institutional Review Board (IRB) Guidebook. (2018). Chapter III: Basic IRB Review. Available from: https://biotech.law.lsu.edu/research/fed/ohrp/gb/irb_chapter3.htm. [29 November 2016].

International Police Criminal Organization (INTERPOL). (2015a). *Cybercrime*. Available from: http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime. [3 December 2015].

International Police Criminal Organization (INTERPOL). (2015b). Connecting police for a safer world*. INTERPOL; Strategy.* Available from: Access link used: http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime. [27 May 2015].

Internet Society (2015). 2015 Global Internet Report (GIR): Mobile is key to fulfilling the promise of Internet connectivity for the next billion people. *Internet Society;* Available from: https://www.internetsociety.org/history/2015/internet-societys-2015-global-internet-report-mobile-is-key-to-fulfilling-the-promise-of-internet-connectivity-for-the-next-billion-people-2015-gir/ [See also: Brown, K. (2015).]. [27 April 2016].

ISACA. (2010.) Fundamentals of IT Governance Based on ISO/IEC 38500. Article by Hamidovich, H. (2010). *ISACA Journal Online.* Available from: https://www.isaca.org/Journal/archives/2010/Volume-5/Documents/10v5-online-fundamentals.pdf. See also: Information Technology Governance Institute (ITGI). (2010.). (See also: Information Systems Audit and Control Association (ISACA), 2010.). [3 May 2019].

ISACA. (2014.) IT Governance Roundtable: Defining IT Governance. ISACA Research. Available from: http://www.isaca.org/Knowledge-Center/Research/Documents/Defining-IT-Governance-Brisbane-Australia_res_Eng_0810.pdf. (See also: Information Technology Governance Institute [TGI], 2014.). [16 March 2019].

ISO/IEC 27000. (2014/revised 2018). Key International Standard for information security revised. Revised by: Lewis, B.;. Available from: https://www.iso.org/news/ref2266.html. [1 March 2018].

IT News Africa. (2015). In: *South African companies plagued by cyber-attacks. Security/Top Stories;* Available from: http://www.itnewsafrica.com/2015/06/south-african-companies-plagued-by-cyber-attacks/ [See also: Fryer, V. (2015).]. [11 February 2016].

ITWEB Network Access Control (20140. Cyber security skills shortfall a 'national emergency'. *CSIR.* Available from: http://www.itweb.co.za/index.php?option=com_content&view=article&id=142701:Cyber-security-skills-shortfall-a-national-emergency-. [3 May 2015].

Jabbour, M.A. (2016). Importance of cyber security. *World Justice Project/Blog; October 21, 2012.* Viewed: 23 June 2016. Available from: http://worldjusticeproject.org/blog/importance-cyber-security. [23 June 2016].

Janssen, C. (2015). Cybercrime, *Techopedia – where IT and business meet.* Available from: http://www.techopedia.com/definition/2387/cybercrime. [29 May 2015].

Jardine, E. (2015). Global cyberspace is safer than you think: Real trends in cybercrime. *CIGI/Chatham House/The Royal Insitute of International Affairs; Global Commission on Internet Governance;* 16; July 2015. Available from: https://ourinternet-files.s3.amazonaws.com/publications/no-16_Web.pdf. [2 February 2016].

Jewkes, Y. & Yar, M. (2011). *Handbook of internet crime*. NY, USA: Routledge Publishing.

Johannesburg Securities Exchange (2012). *Annual Report 2012.* Available from: http://financialresults.co.za/2012/jse_ar2011/. [1 June 2014].

Johannesburg Stock Exchange (2015). *Share sector listing*. Available from: http://sharenet.co.za/listall.phtml~s=00. [14 June 2015].

Johnson, L. & Lamb, A. (2013). Evaluating Internet resources. *EduTap; Professional Development Resources for Educators & Librarians.* Available from: http://eduscapes.com/tap/topic32.htm. [11 June 2016].

Johnson, R. (2015). *Security policies and implementation issues*. 2nd Edition. Burlington, MA, USA: Jones & Bartlett.

Jones, H.S. & Muller, A. (2013). *The South African economy 1910-1990*. NY, USA: St. Martin’s Press.

Jones, S. (2015). Global tensions increase cyber threat. Available from: http://www.ft.com/home/europe. [13 March 2016]

Julian, T. (2014). Defining moments in the history of cyber-security and the rise of incident response. *Infosecurity Magazine (Strategy/Insight/Technology).* Available from: http://www.infosecurity-magazine.com/opinions/the-history-of-cybersecurity/. [21 June 2016].

Juniper Research (2015). Cyber-crime will cost business over $2 trillion by 2019. *Juniper Research/Press Releases;* 12 May 2015. Available from: http://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion. [24 June 2016].

Kalayci, S. (2006). *SPSS applied multivariate statistical techniques*. Ankara: Asil Publication. Available from: http://dergipark.ulakbim.gov.tr/ilkonline/article/view/5000037824. [6 April 2019].

Kalloniatis, C. (2012). Modern information systems. *IntechOpen;* June 13, 2012.. Available from: http://www.intechopen.com/books/modern-information-systems. [5 January 2016].

Kappos, D.J. & Passman, P. (2015). Cyber espionage is reaching crisis levels. *Fortune;* December 12, 2015. Available from: http://fortune.com/2015/12/12/cybersecruity-amsc-cyber-espionage/. [10 July 2016].

Kapur, M., Dhupia, S. & Gupta, S. (2014). Cyber-crime Survey Report 2014. *KPMG.* Available from: https://www.kpmg.com/IN/en/IssuesAndInsights/ArticlesPublications/Documents/KPMG_Cyber_Crime_survey_report_2014.pdf. [20 May 2016].

Kaspersky (2015) Could your business survive a cryptor. *KasperskyLab/Business.* Available from: https://media.kaspersky.com/pdf/guard-against-crypto-ransomware-kaspersky-guide.pdf. [17 June 2016].

Kaspersky (2015). Kaspersky Security Bulletin 2015. *KasperskyLab/Business.* Available from: https://securelist.com/files/2015/12/Kaspersky-Security-Bulletin-2015_FINAL_EN.pdf. [17 June 2016].

Kaspersky (2016). Internet security center. *Kaspersky/Resource Center.* Available from: http://www.kaspersky.co.za/internet-security-center. [6 Mach 2016].

Kearney, L. (2012). Mining and minerals in South Africa. *Brand South Africa;* 16 August, 2012. Available from: https://www.brandsouthafrica.com/investments-immigration/business/economy/mining-and-minerals-in-south-africa. [19 August 2014].

Kelly, R. (2015). Report finds increasing evidence of cyber-attacks penetrating networks. *The Journal/Transforming Education Through Technology;* 23 June 2015. Available from: https://thejournal.com/articles/2015/06/23/report-identifies-increasing-evidence-of-cyber-attacks-penetrating-networks.aspx. [22 November 2015].

Khan, J. (2013). What is cyber-crime? *Byte-Notes/Introduction to Computing.* Available from: http://www.byte-notes.com/what-cyber-crime. [11 May 2016].

Khanse, A. (2014). Types of cybercrime acts and preventive measures. *TheWindowsClub/Security.* Available from: http://www.thewindowsclub.com/types-cybercrime. [12 May 2016].

Khosrow-Pour, M. (2015). *Encyclopaedia of information science and technology*. 3rd Edition. USA: IGI.

King III Report (2010). King Report on corporate governance in South Africa. *Institute of Directors South Africa (IODSA).* Available from: http://www.iodsa.co.za/?kingIII. [16 July 2014].

King III Report (2010). King Report on Corporate Governance in South Africa. *Institute of Directors South Africa (IODSA).* Available from: http://www.iodsa.co.za/?kingIII. [3 April 2016].

Klimburg, A. (Ed.) (2013). *National cyber security framework manual*. Tallinn, Estonia: NATO CCD COE Publication (ccdcoe-at-ccdcoe.org).

Klotz, A. (2013). *Migration and national identity in South Africa*. NY, USA: Cambridge University Press.

Kobie, N. (2015) What is the internet of things. *The Guardian/Tech;* 6 May 2015. Available from: https://www.theguardian.com/technology/2015/may/06/what-is-the-internet-of-things-google. [10 May 2016].

Kohler, U. & Kreuter, F. (2005). *Data analysis using strata*. College Station, Texas: Stata Press.

Kohnke, A., Shoemaker, D. & Sigler, K.E. (2016). *The complete guide to cyber security risk and controls*. Boca Raton, USA: CRC Press.

Korhonen, J.J., Hiekkanen, K. & Mykkänen, J. (2012). *Information security governance.* In: Gupta, M., Walp, J. & Sharman, R. (Eds.) *Strategic and practical approaches for information security governance: Technologies and applied solutions* (pp. 53-66). Hershey, PA: IGI Global. doi: 10.4018/978-l-4666-0197-0.ch004.

Korzeniowski, P. (2016). The new IT security threat coming to your data center. *SearcDataCenter/Essentail Guide.* Available from: http://searchdatacenter.techtarget.com/tip/The-new-IT-security-threat-coming-to-your-data-center. [24 June 2016].

Kosich, D. (2016). Hacking and cyber-attacks: The new threat for mining*. Australian Mining;* August 11, 2016*.* Available from: https://www.australianmining.com.au/?s=Hacking+and+cyber-attacks. [29 April 2017].

Kouns, J. & Minoli, D. (2010). *Information technology risk management in enterprise environments*. Canada: John Wiley & Sons.

Kshetri, N. (201)., *The global cybercrime industry*. Heidelberg/Dordrecht/New York, USA: Springer.

Kumar, A. (2011). Understanding computer security – types of computer security. *Bright Hub Media Articles.* Available from: http://www.brighthub.com/computing/smb-security/articles/61722.aspx. [2 June 2016].

Kumar, V. (Ed.) (2013). *Fundamentals of pervasive information management systems*. 2nd Edition. Hoboken, NJ: John Wiley & Sons.

Lai, L.K.H & Chin, K.S. (2014). Development of a Failure Mode and Effects Analysis Based Risk Assessment Tool for Information Security. *Industrial Engineering & Management Systems;* 13(1):87-100. Korean Institute of Industrial Engineers. Available from: http://www.iemsjl.org/journalarticle.php?code=1679. [3 June 2016].

Langer, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy,* 9(3):49-51. Available from: http://dx.doi.org/10.1109/msp.2011.67. [23 May 2016].

Lanjouw, P., L. (2016). *Combining census and survey data to study spatial dimensions of poverty: A case study of Ecuador*. Available from: https://books.google.co.za/books?id=kYLpzgEACAAJ&dq=census+and+survey&hl=en&sa=X&redir_esc=y. [5 May 2022].

Law Society of South Africa. (2019). Do you have insurance for cybercrime? *De Rebus;* Journal of the Law Society of South Africa; April 2019. Article by Sedutla, M. Available from: http://www.derebus.org.za/do-you-have-insurance-for-cybercrime/ (See also: De Rebus, 2019.). [20 April 2020].

Ledergerber, M. & Knouff, M. (2012). Information governance reference model. *IGRM IT/Duke Law*; March 31, 2015. Available from: https://www.edrm.net/papers/igrm-it-viewpoint/. [6 October 2016].

Ledesma, R.D., Valero-Mora, P. & Macbeth, G. (2015). The scree test and the number of factors: a dynamic graphics approach. *The Spanish Journal of Psychology;* 18/E11; Viewed: 2 March 2019. Available from:

https://www.cambridge.org/core/journals/spanish-journal-of-psychology/article/scree-test-and-the-number-of-factors-a-dynamic-graphics-approach/FD59EBE07263C51BCD8742A1060DD7D4. [17 March 2015].

Lee, C.K. & Sidhu, M.S. (2013). *Computer aided engineering education: New learning approaches and technologies*. *IGI Global.* Available from: http://www.igi-global.com/chapter/computer-aided-engineering-education/80294. [20 October 2016].

Lee, T.B. (2014). Internet-maps. *Vox Media*; June 2, 2014. Available from: http://www.vox.com/a/internet-maps. [1 June 2016].

Leedy, P.D. & Ormrod, J. E. (2010). *Practical research: Planning and design.* 9th Edition. Upper Saddle River, NJ: Merril.

Leiner, B.M., Cerf, V.G., Clark, D.D., Kahn, R.E., Kleinrock, L., Lynch, D.C., Postel, J., Roberts, L.G. & Wolff, S. (2012). Brief history of the Internet. *Internet Society;* 13 September 2017. Available from: http://www.internetsociety.org/brief-history-internet. [1 February 2016].

Lever, J., Krywinski, M. & Altman, N. (2017). Principal component analysis*. Nature Methods 14:641-642;* 29 June 2017. Available from: https://www.nature.com/articles/nmeth.4346. [10 March 2019].

Levitz, P., Crootof, R., Perdue, W. & Hathaway, O.A. (2012). The law of cyber-attack. *California Law Review;* 100(4). August 2012. Available from: http://www.californialawreview.org/?s=The+law+of+cyber-attack. [5 June 2016].

Li, Qing. (2013). A novel Likert scale based on fuzzy sets theory. *Expert Systems with Applications*; 40(5):1609-1618; April 2013. Available from: https://www.researchgate.net/publication/257404665_A_novel_Likert_scale_based_on_fuzzy_sets_theory. [3 March 2019].

Lichem, W. (2016). The United Nations and sciences. *UN Chronicle.* Available from: http://unchronicle.un.org/article/strong-un-based-digital-bridge/. [15 June 2016].

Liell-Cock, S., Graham, J. & Hill, P. (2009). IT governance aligned to King III. *IT Governance Network;* 7 September 2009. Available from: https://www.itgovernance.co.za/itgov_a2_king3.pdf. [16 April 2018].

Linacre, J.M. (2005). *A user's guide to WINSTEPS Rasch-model computer programs*. Chicago: Winsteps.

Lindros, K. (2017). *What is IT governance? A formal way to align IT & business strategy*. *CIO;* Available from: https://www.cio.com/article/2438931/governanceit-governance-definition-and-solutions.html. [21 May 2019].

Locke, G. (2011). Cybersecurity, innovation and the nternet economy. Docplayer.net/*Department of Commerce/Internet Policy Task force, USA.* June 2011. Available from: http://docplayer.net/2409873-Cybersecurity-innovation-and-the-internet-economy.html. [3 November 2015].

Lucas, R.E.B. (2014). *International handbook on migration and economic development*. Cheltenham, UK: Edward Elgar Publishing Limited.

Lyne, J. (2014). Security thread trends in 2015: Predicting what cybersecurity will look like in 2015 and beyond. *Sophos/Media Library.* Available from: https://www.sophos.com/threat-center/medialibrary/PDFs/other/sophos-trends-and-predictions-2015.pdf. [12 August 2015].

Macauley, J., Buckalew, L. & Chung, G. (2015). *Internet of Things in Logistics*. Troisdorf, Germany: DHL Trend Research and Cisco Consulting Services. Available from: http://www.dhl.com/content/dam/Local_Images/g0/New_aboutus/innovation/DHLTrendReport_Internet_of_things.pdf. [16 May 2016].

Macfarlane, A.S. (2001). The implementation of new technology in Southern African mines: Pain or panacea. *SAIMM – Journal of the South African Institute of Mining and Metalurgy;* May/June 2001*.* Available from: https://www.saimm.co.za/Journal/v101n03p115.pdf. [8 October 2016].

Mackey, R.E. (2011). Information security risk assessment frameworks. SearchSecurity/TechTarget; Available from:

http://searchsecurity.techtarget.com/magazineContent/Information-security-risk-assessment-frameworks. [12 January 2016].

MacLennan, A. (2014). *Information governance and assurance, reducing risk, promoting policy*. Croydon, UK: Facet Publishing.

Maddison, M. & Boichat, P. (2013). *Cyber security and mining: A boardroom issue.* London: DeLoitteLLP.

Magutu, T.O., Ondimu, G.M. & Ipu, C.J. (2011*).* Effects of cybercrime on state security: Types, impact and mitigations with fiber optic deployment in Kenya. . *Journal of Information Assurance & Cybersecurity;* 20 July 2011. Available from: http://www.ibimapublishing.com/journals/JIACS/2011/618585/618585.html. [27 April 2016].

Maiuro, R.D. (2015). *Perspectives on cyberstalking, victims, perpetrators and cyberstalking*. NY, USA :Springer Publishing.

Maleske, M. (2012). 8 Ways SOX changed corporate governance. *InsideCounsel;* 1 January 2012. Available from: http://www.insidecounsel.com/2012/01/01/8-ways-sox-changed-corporate-governance. [18 October 2016].

Malhotra, N.K. (2004). *Marketing research: An applied orientation*. 4th Edition. New Jersey: Pearson.

Mallery, J.C. (2011). *A strategy for cyber defense*. (Earlier title [2009]: *Multi-spectrum evaluation frameworks and metrics for cyber security and information assurance*). Paper presented at the MIT/Harvard Cyber Policy Seminar, Cambridge, MA.

Manilal, B. (2016). *Information and communication technologies*. *TIA*. Available from: https://www.tia.org.za/information-and-communications-technologies/. [9 March 2019].

Manoske, A. (2013). *How does cyber warfare work*? *Forbes;* 18 July 2013*.* Available from: http://www.forbes.com/sites/quora/2013/07/18/how-does-cyber-warfare-work/. [26 June 2016].

Mar, S., Johannessen, R., Coates, S., Wegrzynowicz, K. & Andreesen, T. (2012). *Global Technology Audit Guide: Information Technology Risk and Controls*. 2nd Edition. Montreal, Canada: The Institute of Internal Auditors. Available from: https://chapters.theiia.org/montreal/ChapterDocuments/GTAG%201%20-%20Information%20technology%20controls_2nd%20ed.pdf. [20 March 2019].

Marsan, C. (2015). In: The Internet of things – an overview. Understanding the issues and challenges of a more connected world. *Internet Society;* October 2015. Viewed: 17 June 2016. Available from: https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151014_0.pdf. [17 June 2016].

Martin, J.A. (2018). What is access control? A key component of data security. *CSO Feature;* February 5, 2018. Available from: https://www.csoonline.com/article/3251714/what-is-access-control-a-key-component-of-data-security.html. [19 April 2019].

Martin, G. (2018). The world is running out of gold: Mining experts warn discoveries are shrinking. *MSN/Daily Mail;* 13 July 2018. Available from: https://www.msn.com/en-us/money/markets/the-world-is-running-out-of-gold-mining-experts-warn-discoveries-are-shrinking/ar-AAA0Jep?index=1&li=BBgzzfc. [27 May 2016].

Martin, W.G. (2013). *South Africa and the world economy: Remaking race, state and region*. NY, USA: UR Press.

Mataranyika, M. (2016). *Here's how hackers hit African organisations*. *Fin24/TecNews;* 28 June 2016. Available from: http://www.fin24.com/Tech/News/heres-how-hackers-hit-african-organisations-20160628. [4 September 2016].

Mazumdar, C., Barik, M.S. & Sengupta, A. (2010). Enterprise information system security: A life-cycle approach. (Chapter 1.11.) *IGI Global*. Available from: http://www.irma-international.org/viewtitle/48540/. [22 April 2014].

McAfee. (2014). Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II. *CSIS/AmazonaNews*. Available from: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf. [22 June 2016].

McClelland, R. (2015). *Critical infrastructure resilience strategy*. *Australian Government.* Available from: https://www.ag.gov.au/RightsAndProtections/CyberSecurity/Pages/default.aspx. [18 November 2015].

McCulloch, J. (2012). *South Africa's gold mines & the politics of silicosis*. Rochester, NY, USA: Boydell & Brewster.

McGee, J.A., Byington, J.R. (2013). How to counter cybercrime intrusions. Wiley Online Library; Journal of Corporate Accounting & Finance; 24(5); 19 June 2013. Available from: http://onlinelibrary.wiley.com/doi/10.1002/jcaf.21874/abstract. [28 May 2016].

McGraw-Hill Dictionary of Computing and Communications. (2016). Viewed: 22 June, 2016.

McGuire, M. (2013). Cyber-dependent crimes. Research Report 75. *UK Government: Home Office.* October 2013. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/horr75-chap1.pdf. [12 April 2016].

McGuire, C.F. (2015). The expanding cyber security threat. *Technology Innovation Management Review (TIM).* Available from: http://timreview.ca/sites/default/files/Issue_PDF/TIMReview_March2015.pdf. [8 June 2016].

McKenna, A. (2011). *The history of Southern Africa*. NY, USA: Britannica Educational Publishing.

McLellan, C. (2015). Cybersecurity in 2015: What to expect. *ZDNET: Security and privacy – New challenges.* Available from: http://www.zdnet.com/article/cybersecurity-in-2015-what-to-expect/. [19 May 2016].

McPhee, C. & Bailetti, T. (2013). Cybersecurity. (Editorial.) *Technology Innovation Management Review (TIM);* August 2013. Available from: http://timreview.ca/article/710. [23 June 2016].

McWay, D.C. & Rhia, J.D. (2014). *Today's health information management*. 2nd Edition. New York, USA: Cengage.

Mehan, J. (2014). *Cyberwar, cyberterror, cybercrime and cyberactivism*. Cambridgeshire, UK: IT Governance Publishing.

Mellado, D. (2013). *IT security governance innovations: Theory and research*. USA: IGI Global.

Mendenhall, W., Beaver, RJ. & Beaver, B.M. (2013). *Introduction to probability & statistics*. 14th Edition. Boston, USA: Brooks/Cole/Cengage Learning.

Menell, R. (2015) South African innovation sets pace for mining industry. *Brand South Africa;* Available from: https://www.brandsouthafrica.com/investments-immigration/business/trends/innovations/mining-innovation-100215. [29 March 2018].

Mercer, E. (2016). Causes of cyber-crime. *ItStillWorks Website.* Available from: http://techin.oureverydaylife.com/causes-cyber-crime-1846.html. [19 June 2016].

Metivier, B. (2016) Seven characteristics of a successful information security policy. *Sage Data Security/Sage Advice – Cybersecurity Blog.* Available from: https://www.sagedatasecurity.com/blog/seven-characteristics-of-a-successful-information-security-policy. [16 May 2018].

Michalson, L. (2010). What is information security law? *Michalsons; Information Security Law;* September 17, 2010*.* September 17, 2010*.* Available from: http://www.michalsons.co.za/blog/what-is-information-security-law/961. [21 January 2016].

Michalson, L. (2015). The Cybercrimes and Cyber Security Bill, South Africa: Overview. *Michalsons; Focus Areas.* Viewed: 23 July 2016. Available from:

http://www.michalsons.co.za/blog/cybercrimes-and-cybersecurity-bill-the-cac-bill/16344. [23 July 2016].

Miller, L.C. (2014) *Cybersecurity for dummies*. Canada: John Wiley & Sons.

Mills, A.J., Durepos, G. & Wiebe, E. (2010). *Encyclopaedia of case study research.* Volumes I & II. CA, USA: Thousand Oaks.

Mining IQ. Cyber Security (2011). Increased risk in the mining sector. *IQPC/Cyber Security Hub.* Available from: http://www.miningiq.com/mining/articles/cyber-security-increased-risk-in-the-mining-sector/. [14 February 2014].

Mitchell, B. (2016). How to set up your mobile device security. Be safe, no matter where you are. *LifeWire: Tech Untangled;* article by Archambault, M. (updated: April 11, 2019). Available from: https://www.lifewire.com/set-up-mobile-device-security-4589497. [28 September 2017].

Mohr, P. (2014). Hopes raised for a more bullish mining sector*. Mining Weekly/Creamer Media;* 24 January 2014; article by: Rees, S. Available from: http://www.miningweekly.com/article/chinese-us-macroeconomic-developments-raise-hopes-for-a-more-bullish-mining-sector-2014-01-24-1. [24 June 2014].

Moore, A. & Edwards, L.J. (2014)*. Cyber self-defence: Expert advice to avoid online predators*, identity theft, and cyberbullying. UK: Lyon Press.

Moore, R. (2011). *Cybercrime: Investigating high-technology computer crime*. New York, USA: Routledge.

Morgan, J. (2014). A simple explanation of the Internet of things. *Forbes;* May 13, 2014. Available from: http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#65a606bf6828. [10 May 2016].

Morgan, S. (2016). Cyber Crime Costs Projected To Reach $2 Trillion by 2019. Forbes; January 17, 2016. Available from: https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#38954b713a91. [15 June 2016].

Morley, D. (2015). *Understanding computers in a changing society*. 6th Edition. CT, USA: Wadsworth/Cengage Learning.

Moskowitz, R. (2014). Network intrusion: methods of attack. *RSA Conference/Where the world talks security;* December 25, 2014 (contributor: Moskowitz, R). Available from: https://www.rsaconference.com/blogs/network-intrusion-methods-of-attack. [18 June 2016].

Mostert, H. (2012). *Mineral law principles & policies in perspective*, Juta and Co. Ltd, Claremont, Cape Town

Murray, M. (2013). Top 5 cyber-crimes. *American Institute of CPAs (AICPA).* Available from: http://www.aicpa.org/InterestAreas/ForensicAndValuation/Resources/ElectronicDataAnalysis/DownloadableDocuments/Top-5-CyberCrimes.pdf. [11 June 2016].

Myers, M. (2013). *Qualitative research in business & management*. 2nd Edition. London: SAGE.

Naggar, R. (2015). The creativity canvas: A business model for knowledge and idea management. *Technology Innovation Management (TIM) Review;* 5(7):50-58, July 2015. Available from: http://timreview.ca/article/914. [23 May 2016].

Napitupulu, D., Kadar, J.A. & Jati, R.K. (2017). Validity testing of technology acceptance model based on factor analysis approach. *Indonesian Journal of Electric Engineering & Computer Science;* 5(3):697-704; March 2017. Computer Sciences Faculty, University of Borobudur, Indonesia. Available from: https://pdfs.semanticscholar.org/88d5/3e446041f2560ab8548ac1509e2f1c6a60f2.pdf. [16 August 2018].

National Initiative for Cyber Security Education. (2014). *Best Practices for Planning a Cybersecurity Workforce White Paper*. (Department of Homeland Security, USA*.) National Initiative for Cybersecurity Careers and Studies (NICCS);* August 4, 2014. Available from: http://niccs.us-cert.gov/sites/default/files/documents/files/Best%20Practices%20for%20Plann ing%20a%20Cybersecurity%20Workforce_062813_v4.2_FINAL_NICE%20branded_0.pdf. [13 August 2015].

Nelson, C. (2016). Companies need a holistic approach to cyber security that keeps up with innovation. *TRUE – Digital & Social Media;* (12); August 2016. Available from: http://fleishmanhillard.com/2015/04/true/companies-need-a-holistic-approach-to-cybersecurity-that-keeps-up-with-innovation/. [23 June 2017].

Nemati, H.R. (2014). *Analyzing security, trust, and crime in the digital world*. PA, USA: IGI.

Nesbitt, J. (2015). Top 3 cyber security risks for 2015. *IT GUYS.* February 6, 2015. Available from: http://okcitguys.com/top-3-cyber-security-risks-for-2015/. [2 July 2016].

Newman, G.R., Clarke, R.V. (2011). *Superhighway robbery*. 6th Edition. NY, USA: Routledge.

Nunnally, J. & Bernstein, L. (1994). *Psychometric theory*. New York: McGraw-Hill.

O'Callaghan, J. (2015). Beware the coffee shop hacker: New breed of cyber-criminal spies on your laptop by listening to signals even when it's offline. *Daily Mail: Mail Online;* 9 January 2015. Available from: http://www.dailymail.co.uk/sciencetech/article-2903261/Beware-coffee-shop-hacker-New-breed-cyber-criminal-spies-laptop-listening-signals-s-offline.html. [24 June 2016].

Oerting, T. (2014). Dark markets downed in international anti-cyber-crime operation. *Computer Weekly;* 7 November 2014. Available from: http://www.computerweekly.com/news/2240234303/Dark-markets-downed-in-international-anti-cyber-crime-operation. [9 July 2016].

Ogiela, L. & Ogiela, M.R. (2014*).* Cognitive systems for intelligent business information management in cognitive economy. *International Journal of Information Management;* 34(6):751-760; Elsevier. Available from: https://www.sciencedirect.com/science/article/pii/S0268401214000863?via%3Dihub. [21 November 2017].

Oleszek, W.J., Oleszek, M.J., Rybicki, E. & Heniff, B. *Congressional procedures and the policy process.* (2015). 10th Edition. Washington, DC: CQ Press.

Oluga, S.O., Ahmad, A.B.H., Alnagrat, A.J.A., Oluwatosin, H.S., Sawad, M.O.A. & Mukta, N.A.B. (2014). An overview of contemporary cyberspace activities and the challenging cyberspace crimes/threats. *International Journal of Computer Science and Information Security (IJCSIS);* 12(3); March 2014. Available from: https://www.academia.edu/11750708/An_Overview_of_Contemporary_Cyberspace_Activities_and_the_ChallengingCyberspace_Crimes_Threats?auto=download. [6 June 2016].

Onifade, O.J., Osunade, O.O. & Oyedele, O.E. (2014). Internet secrecy laws and its implications on developing nations*. International Journal of Internet of Things 2014*, 3(1):8-17. Available from: http://www.sapub.org/global/showpaperpdf.aspx?doi=10.5923/j.ijit.20140301.02. [4 June 2016].

Osborne, G. (2015). Chancellor's Speech to GCHQ on Cyber Security. *Her Majesty's Treasury, Government Communications Headquarters,* November 17, 2015. Available from: https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security. [3 May 2016].

Overfelt, M. (2016). *The next big threat in hacking – data sabotage*. *CNBC; The Pulse @1 Market;* March 9, 2016. Available from: http://www.cnbc.com/2016/03/09/the-next-big-threat-in-hacking--data-sabotage.html. [18 October 2016].

Oxford English Living Dictionaries. (2016). Definition of psychology in English. Available from: https://en.oxforddictionaries.com/definition/psychology. [11 October 2016].

Paganini, P. (2013). The cyber-crime ecosystem, resources, motivations and methods. *Security Affairs;* 3 July 2013. Available from: http://securityaffairs.co/wordpress/15884/cyber-crime/fortinets-2013-cybercrime-report-the-cybercrime-ecosystem.html. [19 June 2016].

Paladion. (2012) Manage risk, manage growth. *Paladion/High Speed Security Defense.* Available from: http://www.paladion.net/paladionlabs.html. [27 April 2014].

Pande, R. & Van der Wiede, T.P. (2012). *Globalisation, technology diffusion and gender disparity*. USA: IGI.

Parliament of The Republic of South Africa. (2017). *Department of Telecommunications and Postal Services: Cybersecurity.* Cape Town: Research Unit; Parliamant of South Africa. Available from: http://pmg-assets.s3-website-eu-west-1.amazonaws.com/170822Cybersecurity. [18 April 2018].

Parmar, B. (2013). Employee negligence: The most overlooked vulnerability. *ScienceDirect/Elsevier;* 2013(3):18-20; March 2013. Available from: https://www.sciencedirect.com/science/article/pii/S1361372313700307?via%3Dihub. [9 June 2016].

Perkins, E. (2018). Top cybersecurity trends for 2018*. Gartner Research: Webinar/On-Demand.* Available from: https://www.gartner.com/en/webinars/3841563/top-cybersecurity-trends-for-2018. [2 February 2019].

Perkins, G. (2012). The Basics of Information Security Guidebook: Security Classification. *Province of British Columbia, Canada/Office of the Chief Information Officer.* Available from: http://www.cio.gov.bc.ca/local/cio/informationsecurity/pdf/BasicsInfoSecurityGuidebook.pdf. [17 August 2014].

Peterson, A. (2016). Hackers caused a blackout for the first time, researchers say. *Hachers 360^{0}/NDTV;* January 6, 2016. Available from: http://gadgets.ndtv.com/internet/features/hackers-caused-a-blackout-for-the-first-time-researchers-say-786136. [18 March 2016].

Pett, M., Lackey, N. & Sullivan, J. (2003). *Making sense of factor analysis*. Thousand Oaks, CA: Sage Publications.

Ponemon Institute. (2015). *2015 Cost of cyber-crime study. HIPAA Journal;* October 8, 2015. Available from: https://www.hipaajournal.com/2015-ponemon-cost-of-cyber-crime-study-8138/. [24 June 2016].

Praxiom Research Group. (2014). Information security definitions. *Praxiom;* November 12, 2013. Available from: http://www.praxiom.com/iso-27000-definitions.htm#Monitoring. [29 May 2015].

PricewaterhouseCoopers (PwC). (2018). Reported global economic crime hits record levels; cybercrime, cost and accountability concerns rising. Available from: https://www.pwc.com/gx/en/news-room/press-releases/2018/reported-global-economic-crime-hits-record-levels-cybercrime-cost-and-accountability-concerns-risi.html. [22 February 2018].

Quinlan, C. (2011). Business research methods. Andover, Hamphire, UK: Cengage Learning.

Radu, R., Chenou, J.-M. & Weber, R.H. (Eds.) (2014). *The evolution of global Internet governance*. Heidelberg/Berlin, Germany: Springer-Verlag.

Raiche, G., Wallis, T.A., Magis, D., Riopel, M. & Blais, J.G. (2013). Non-graphical solutions for Cattell’s scree test. *Hogrefe Publishing; Methodology (2013);* 9: 23-29. Available from: https://econtent.hogrefe.com/doi/full/10.1027/1614-2241/a000051. [11 March 2019].

Ralph, P. (2014). Heartbleed patched but security time bomb is ticking. *The Conversation;* April 14, 2014. Available from: http://theconversation.com/Heartbleed-patched-but-security-time-bomb-is-still-ticking-25582. [12 June 2016].

Rasool, F. (2012). Postbank hacked for R42m. *ITWeb;* 16 January 2012. Available from: http://www.itweb.co.za/index.php?option=com_content&view=article&id=50608. [23 November 2015].

Rausand, M. (2014). *Reliability of safety-critical systems, theory and applications*. Hoboken, New Jersey: John Wiley & Sons.

Remenyi, D., Williams, B., Money, A. & Swartz, E. (1998). Doing research in business and management: An introduction to process and method. *Sage Knowledge/Online.* Available from: http://dx.doi.org/10.4135/9781446280416. [14 May 2015].

Republic of South Africa. (2012). *Budget Speech*: Minister Pravin Gordhan. 22 February 2012. *South African Government; Newrooms/Speeches.* Available from: http://www.gov.za/speeches/budget/index.html#budget2012. [1 June 2014].

Resnik, P. (2011). *Semantic similarity in taxonomy: An information-based measure and its application to problems of ambiguity in natural language.* Journal of Artificial Intelligence Research, 11:95-130. Available from: http://arxiv.org/abs/1105.5444v1. [19 August 2014].

Rhodes-Ousley, M. (2013). *Information security: The complete reference.* 2nd Edition. USA: McGraw-Hill.

Ribiere, V. & Worasinchai, R. (Eds.) (2013). Proceedings of the International Conference on Management, Leadership and Governance. *ISSUU/Digital Publishing Platform;* IKI-SEA, Bangkok University, Thailand; 7-8 February 2013. Available from: https://issuu.com/acpil/docs/icmlg-13-proceedings.3. [18 March 2018].

Richet, J.-L. (2015). *Cybersecurity policies and strategies for cyberwarfare prevention*. USA: IGI Global. Available from archive: https://archive.org/stream/ThreatMitigationAndDetectionOfCyberWarfareAndTerrorismActivities/Threat%20Mitigation%20and%20Detection%20of%20Cyber%20Warfare%20and%20Terrorism%20Activities_djvu.txt. [7 May 2018].

Riley, J. (2016). What is ICT? *Tutor2u/Study Notes/Business Reference Library.* Available from: http://www.tutor2u.net/business/reference/what-is-ict. [5 June 2016].

Rizzo, F. (2016). Corporate Governance and King III. *KPMG South Africa/Frank Rizzo IT Advisory.* Available from:

https://assets.kpmg.com/content/dam/kpmg/pdf/2016/07/Corporate-Governance-and-King-III.pdf. [10 July 2016].

Roberts, L.D., Indermaur, D. & Spiranovic, C. (2013.) Fear of cyber-identity theft and related fraudulent activity. *Taylor-Francis Online: Psychiatry, Psychology and Law;* 20(3):315-328; 2013. Available from: https://www.tandfonline.com/doi/abs/10.1080/13218719.2012.672275. [12 May 2018].

Robinson, R.M. (2016). The growing threat of cyber extortion. *SecurityIntelligence;* September 21, 2016. Available from: https://securityintelligence.com/the-growing-threat-of-cyber-extortion/. [21 October 2016].

Rogers, M.K. (2010). *The psyche of cybercriminals: A psycho-social perspective*. In: Ghosh, G. & Turrini, E. (Eds.) Cybercrimes: A Multidisciplinary Analysis. Berli, Germany: Springer-Verlag.

Roman, A. (2014). King III Report: How South Africa revolutionised corporate governance. *Convene (Don't just meet – convene);* May 8, 2014. Available from: https://www.azeusconvene.com/articles/south-africa-revolutionize-corporate-governance. [18 July 2016].

Rondganger, L. (2007) Scorpions catch cyber crook in the act. *IOL News;* 5 April, 2007. Available from: http://www.iol.co.za/news/south-africa/scorpions-catch-cyber-crook-in-the-act-321869. [26 February 2016].

Roscini, M. (2014). *Cyber operations and the use of force in international law*. UK: Oxford University Press.

Rose, S., Spinks, N. & Canhoto, A.I. (2015). *Management research: Applying the principles*. 1st Edition. New York: Routledge.

Rouse, M. (2015a). Cybercrime. *TechTarget/SearchSecurity Network*. Available from: http://searchsecurity.techtarget.com/definition/cybercrime. [29 May 2015].

Rouse, M. (2015b). ICT (information and communication technology, or technologies). *TechTarget/SearchSecurity Network.* Available from:

http://searchcio.techtarget.com/definition/ICT-information-and-communications-technology-or-technologies. [10 May 2016].

Rouse, M. (2016). What is Phishing? *TechTarget/SearchSecurity Network.* Available from: http://searchsecurity.techtarget.com/definition/phishing. [11 May 2016].

Rubenstein, D. (2014). Nation-state cyber espionage and its impacts. *Washington University of St. Louis; McKelvey School of Engineering* (A paper written under the guidance of Prof. Raj Jain). Available from: http://www.cse.wustl.edu/~jain/cse571-14/ftp/cyber_espionage/. [20 June 2016].

Rubin, A. & Babbie, E. (2011). *Research methods for social work*. Belmont, CA: Brooks-Cole Cengage.

Ruscio, J. & Roche, B. (2012). Determining number of factors to retain in an exploratory analysis using comparison data of known factorial structure. *Psychological Assessment*, 24(2):282-292; June 2012. Available from: https://psycnet.apa.org/buy/2011-22371-001. [12 July 2019].

Salim, N. (2015) The Internet of Things: The next intruder in security. *Fingent/Shaping the Future;* Spetember 15, 2015. Available from: https://www.fingent.com/blog/the-internet-of-things-the-next-intruder-in-security. [10 May 2016].

Samani, R. (2016) 3 Key security challenges for the Internet of Things. *McAfee;* October 29, 2014. Available from: http://www.securingtomorrow.com/blog/knowledge/3-key-security-challenges-internet-things/. [10 May 2016].

Samuel, A. (2012). Research design and methodology: Part 1. *Samuel Learning; Research Methods.* Available from: http://www.samuellearning.org/research_methods/week_4_researchdesignandmethodologypt1_2012.pdf. [17 August 2014].

Santillan, M. (2015). Dozens of vulnerabilities in firmware shows lack of proper security practices. *TripWire/State of Security;* August 12, 2014. Available from: http://www.tripwire.com/state-of-security/latest-security-news/dozens-of-vulnerabilities-in-firmware-devices-show-lack-of-proper-security-practices/. [6 May 2016].

Sauerberg, R. (2012). Customer relationship information technology internal control and security framework. *ISACA/Journal Online, Volume 2.* Available from: http://www.isaca.org/Journal/Past-Issues/2012/Volume-2/Documents/jol12v2-Customer-Relationship.pdf. [22 April 2014].

Saunders, M., Lewis, P. & Thornhill, A. (2012). *Research methods for business students*. 6th Edition. UK: Pearson.

Sawada, E. & Managi, S. (2013). Effects of technological change on non-renewable resources extraction and exploration. *Springer Open; Journal of Economic Structures, 3(1),* 24 May 2013. Available from: https://journalofeconomicstructures.springeropen.com/articles/10.1186/2193-2409-3-1. [22 June 2014].

Schneier, B. (2014). The Internet of Things is wildly insecure and often unpatchable. *Schneier on Security;* January 6, 2014*.* Available from: https://www.schneier.com/essays/archives/2014/01/the_internet_of_thin.html. [29 November 2016].

Schniederjans, M.J., Schniederjans, D.G. & Starkey, C.M. (2015)*. Business analytics principles, concepts and applications with SAS*. Upper Saddle River, New Jersey: Pearson Education.

Schönrock-Adema, J., Heijne-Penninga, M., Van Hell, E.A. & Cohen-Schotanus, J. (2009). Necessary steps in factor analysis: Enhancing validation studies of educational instruments. *NCBI Resources/Med Teach;* 31(6): e226-232; June 2009. Available from: https://www.ncbi.nlm.nih.gov/pubmed/19089728. [10 April 2018].

Schwalbe, K. (2014). *Information technology project management.* USA: Cengage Learning.

Security SA/High Tech Security Solutions. (2011). Article by: Eardley, M. £16,8 billion lost to theft of corporate secrets in the UK. *Security SA/High Tech Security Solutions;* April 2011 [Cyber Security/Mining Industry]. Available from:

http://www.securitysa.com/article.aspx?pklarticleid=6710 [See also: Eardley, 2011.]. [18 February 2015].

Serriere, F. (2015). Where is the internet? *Vox Media.* May 14, 2015. Available from: http://www.vox.com/cards/the-internet/where-is-the-internet. [3 May 2016].

Sexton, M. (2017). *A comprehensive approach to support the external auditor of the small and medium audit firm, to address evolving information technology control risks of an auditee*. Dissertation presented in partial fulfilment of the requirements for the degree Master of Commerce (Computer Auditing) at Stellenbosch University, South Africa*.* Available from: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwjInL-H7rvjAhVOb1AKHQG5ARIQFjAAegQIABAC&url=https%3A%2F%2Fscholar.sun.ac.za%2Fbitstream%2Fhandle%2F10019.1%2F101420%2Fsexton_comprehensive_2017.pdf%3Fsequence%3D1%26isAllowed%3Dy&usg=AOvVaw1zhow4fQyKdW1ByIA32geI. [19 March 2018].

Shakarian, P., Shakarian, J. & Ruef, A. (2013)*. Introduction to cyber-warfare – A multidisciplinary approach*. Elsevier, USA: Syngress Publications.

Shekharan, U. & Bougie, R. (2010). *Research methods for business: A skill building approach*. 5th Edition. New Delhi: John Wiley.

Shinder, D. (2010). IT Security. *TechRepublic/Tech & Work;* July 19, 2010. Available from: http://www.techrepublic.com/blog/it-security/profiling-and-categorizing-cybercriminals/. [12 April 2016].

Shostack, A. (2014). Threat modelling: *Designing for security*. Canada: John Wiley & Sons.

Siegel, L.J. (2013). *Criminology theories, patterns, and typologies.*11th Edition. CT, USA: Wadsworth Cengage Learning.

Simon, M.K. & Goes, J. (2013). *Dissertation and scholarly research: A practical guide to start & complete your dissertation, thesis, or formal research project.* USA: Erin Joyner.

Singer, P.W., Friedman, A. (2014). *Security and cyber war what everyone needs to know*. NY, USA: Oxford University Press.

Singh, A.S. (2014). Conducting case study research in non-profit organisations. *Qualitative Market Research: An International Journal;* 17(1):77-84. Available from: https://www.emerald.com/insight/content/doi/10.1108/QMR-04-2013-0024/full/html. [19 March 2018].

Siponen, M.T., Pahnila, S. & Mahmood, M.A. (2010). Compliance with information security: An empirical investigation*. Computer*, 43(2):64-71; February 2010. Available from: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5410711&url=http%3A%2F%2Fieeexplore.ieee.org%2Fstamp%2Fstamp.jsp%3Ftp%3D%26arnumber%3D5410711. [7 May 2014].

Sloan, R.H. & Warner, R. (2014). *Unauthorised access: The crisis in online privacy and security*. NY, USA: CRC Press.

Smallwood, R.F. (2014). *Information governance, concepts, definitions, and principles.* John Wiley & Sons.

Smit, C. (2015). The role of mining in the South African economy. *KPMG South Africa Blog* (*contribution by Smit, C.*)*.* Available from: https://www.sablog.kpmg.co.za/2013/12/role-mining-south-african-economy/. [17 September 2016].

Snow, G.M. (2012). Cybercrimes. *National Crime Prevention Council (NCPC)/Resources.* Available from: http://archive.ncpc.org/resources/files/pdf/internet-safety/13020-Cybercrimes-revSPR.pdf. [1 June 2016].

Softpedia News. (2016). Mining sector has faced 17 major cyber-incidents in the past six years. Over 20 entities affected by cyber-attacks*. Softpedia News;* Jun 29, 2016: Article by Cimpanu, C. Available from: https://news.softpedia.com/news/mining-sector-faced-17-major-cyber-incidents-in-the-past-six-years-505783.shtml. [2 April 2018].

Solyom, J., Bertram, S. (2015). The cyber security outlook for 2015. *Computer Weekly.* Available from: http://www.computerweekly.com/opinion/The-cyber-security-outlook-for-2015. [15 May 2016].

Somekh, B. & Lewin, C. (2011). *Theory and methods in social research*. 2nd Edition. London, EC1Y: Sage Publications Ltd.

Sorman, A. (2018). *4 Effective methods to increase your survey response rates*. *CMO Nation/Marketo.com/Demand Generation.* Available from: https://blog.marketo.com/2017/01/4-effective-methods-to-increase-your-survey-response-rates.html. [12 July 2019].

South Africa Yearbook 2012/13. *Economy.* Department: Government Communication and Information. Pretoria: Government Printing Works.. Retrieved from: http://www.gcis.gov.za/sites/www.gcis.gov.za/files/docs/resourcecentre/yearbook/2012/06%20Economy%20.pdf. [19 July 2014].

South African Centre for Information Security (2014). Information security. *South African Centre for Information Security (SACfIS).* Available from: http://www.sacfis.co.za/infosecov.htm. [20 June 2014].

South African Government (2015). Minister David Mahlobo: Media briefing on State Security 2015/16 Budget Vote. *South African Government/News Room/Media Statements.* Available from: http://www.gov.za/speeches/minister-david-mahlobo-state-security-dept-201516-budget-vote-5-may-2015-0000. [2 April 2015].

South African Institute of Chartered Accountants (SAICA). (2010). King Report on corporate governance*. SAICA/Technical/Legal and Governance.* Available from: https://www.saica.co.za/Technical/LegalandGovernance/King/tabid/2938/language/en-ZA/Default.aspx#king3. [18 June 2014].

South African Minerals to Metals Research Institute (SAMMRI). (2009). SAMMRI Proposal. *SAMMRI.com.* Available from: http://www.sammri.com/wp-content/uploads/2011/07/SAMMRI-Proposal.pdf. [28 May 2014].

South African Minerals to Metals Research Institute (SAMMRI). (2014). The South African mining industry*. SAMMRI.com.* Available from: http://www.sammri.com/?page_id=33. [16 August 2014].

South African Reserve Bank (2012). Annual Economic Report – 2012. *South African Reserve BankPublications.* Available from: https://www.resbank.co.za/Publications/Detail-Item-View/Pages/Publications.aspx?sarbweb=3b6aa07d-92ab-441f-b7bf-bb7dfb1bedb4&sarblist=21b5222e-7125-4e55-bb65-56fd3333371e&sarbitem=5095. [22 June 2014].

South African Yearbook 2012/13. Mineral Resources. *SA Government Resource Centre/gcis.gov.za.* Available from: http://www.gcis.gov.za/sites/www.gcis.gov.za/files/docs/resourcecentre/yearbook/2012/16%20Mineral%20Resources_0.pdf. [11 June 2014].

Spremic, M. (2012). Measuring IT Governance Performance: A research study on CobiT- based regulation framework usage. *International Journal of Mathematics and Computers in Simulation*, 6:17-25. Available from: https://www.researchgate.net/publication/292640805_Measuring_IT_Governance_Performance_A_research_study_on_CobiT-_based_regulation_framework_usage. [1 June 2018].

Stair, R.M. & Reynolds, G.W. (2012). *Principles of information systems: A managerial approach*. 10th Edition. Boston, MA: Cengage Learning.

Stewart, J.N. (2017). *Cisco 2017 Annual Cyber Security Report*. Available from: https://www.cisco.com/c/m/en_au/products/security/offers/annual-cybersecurity-report-2017.html. [29 March 2018].

Stroie, E.R. & Rusu, A.C. (2011). Security risk management – Approaches and methodology. *Informatica Economic; 15(1); 2011*. Available from: http://revistaie.ase.ro/content/57/21%20-%20Stroie,%20Rusu.pdf. [11 December 2015].

Stoll, M., Felderer, M. & Breu, R. (2012) *Information Management for Holistic, Collaborative Information Security.* Systems, Computing Sciences and Software Engineering (SCSS2010), 211-224. Springer.

Sugarman, E. (2014). Cybersecurity is a severe and growing challenge for government contractors. *Forbes Now (US Edition);* 26 July 2014. Available from: https://www.forbes.com/sites/elisugarman/2014/08/26/cybersecurity-is-a-severe-and-growing-challenge-for-government-contractors/#5aee883c728e. [30 August 2016].

Survey Monkey (2014). Survey your target market*. SurveyMonkey/Resources..* Viewed: 18 August 2014. Available from: https://www.surveymonkey.com/resources/identify-and-reach-your-target-market-with-surveys/. [18 August 2014].

Sutherland, C. (2016) Know the cyber-security risks of smart homes. *Memeburn/Internet of Things;* 8 April 2016. Available from: http://memeburn.com/2016/04/know-the-cyber-security-risks-of-smart-homes/. [9 June 2016].

Symantec Corporation. (2013). 2013 Norton Report. *Symantec/Newsroom.* Available from: https://www.symantec.com/about/newsroom/press-kits/norton-report-2013. [26 January 2015].

Symantec Corporation (2015). 2016 Internet Security Threat Report, Volume 21*. Symantec;* April 2016.. Available from: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf. [17 June 2016].

Tabachnick, B.G. & Fidell, L.S. (2007). *Using multivariate statistics*. 5th Edition. Boston, MA: Allyn & Bacon.

Talabis, M. & Martin, J.. (2013). *Information security risk assessment toolkit*. MA, USA: Elsevier.

Talbot, D. (2015). Cyber-espionage nightmare. *MIT Technology Review;* June 10, 2015. Available from: https://www.technologyreview.com/s/538201/cyber-espionage-nightmare/. [9 July 2015].

Tamarkin, E. (2015). The AU's cyber-crime response. *Institute for Security Studies (ISS);* Policy Brief 73; January 2015. Available from: https://www.issafrica.org/uploads/PolBrief73_cybercrime.pdf. [26 June 2016].

Tarakanov, D. (2016). PlugX Malware: A good hacker is an apologetic hacker. *Kaspersky;* March 10, 2016. Available from: https://securelist.com/blog/virus-watch/74150/plugx-malware-a-good-hacker-is-an-apologetic-hacker/. [12 May 2016].

Tavakol, M. & Dennick, R. (2011). Making sense of Cronbach's Alpha. *International Journal of Medical Education (IJME);* 2: 53-55; 27 June 2011. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4205511/. [3 March 2019].

Technology Innovation Agency (2016). The Mining Sector Innovation Strategies Implementation Plan 2012/13 – 2016/17. *TIA/Innovation Tomorrow Together/Department of Science and Technology.* Available from: http://pmg-assets.s3-website-eu-west-1.amazonaws.com/TIA_Revised_APP_2016-2017_FY_Master_2016.pdf. [17 September 2016].

Techopedia (2014). Cybercrime. *Technopedia/Dictionary.* Available from: https://www.techopedia.com/definition/2387/cybercrime. [22 November 2015].

Teffo, C. (2016). Chamber of Mines. Available from: http://www.chamberofmines.org.za/. [11 October 2016].

Thompson, T. (2015). Cyber security risks series: Roundup. *Breacher Report – SS8 Website;* September 8th, 2015. Available from: http://blog.ss8.com/3539/. [21 June 2016].

Tolica, E.K., Sevrani, K. & Gorica, K. (2015). ICT sector and the importance of ICT infrastructure management. *Springer Link (SpringerBriefs in Business).* Available from: http://link.springer.com/chapter/10.1007%2F978-3-319-17196-8_2. [30 June 2016].

Trading Economics. (2014). South Africa Current Account to GDP. *TradingEconomics/South Africa.* Available from: http://www.tradingeconomics.com/south-africa/current-account-to-gdp. [22 June 2014].

Trainor, J. (2016). Counting that cyber threat. New US cyber security policy codifies Agency roles. *Department of Justice, Federal Bureau of Investigation (FBI). FBI News/Cyber Security;* July 26, 2016. Available from: https://www.fbi.gov/news/stories/new-us-cyber-security-policy-codifies-agency-role. [20 October 2016].

Trim, P. & Upton, D. (2013). *Cyber security culture*. New York, USA: Gower Publishing.

Trim, P. & Yang-Im, Lee. (2014). 1st Edition. *Cyber security management: A governance, risk and compliance framework.* New York, USA: Gower Publishing.

Tropina, T. & Callanan, C. (2015). *Self and co-regulation in cybercrime, cyber security and national security*. Heidelberg, NY: USA Springer.

Uma, M. & Padmavathi, G. (2013). A survey on various cyber attacks and their classification. *International Journal of Network Security;* 15(5):390-396; September 2013. Available from: http://ijns.jalaxy.com.tw/contents/ijns-v15-n5/ijns-2013-v15-n5-p390-396.pdf. [8 June 2016].

University of South Africa (UNISA) (2012). Policy on research ethics. *University of South Africa (UNISA)*. Available from: https://www.unisa.ac.za/static/corporate_web/Content/Library/Library%20services/research%20support/Policy%20on%20Research%20Ethics.pdf. [1 June 2014].

Urban, T. (2015). The AI revolution: The road to superintelligence. *WAIT BUT WHY*; January 22, 2015. Available from: http://waitbutwhy.com/2015/01/artificial-intelligence-revolution-1.html. [3 May 2016].

Uzair, Amir. (2016). Anonymous hacks South African job portal against child labour. *HackRead News Platform*; February 11th, 2016. Available from: https://www.hackread.com/anonymous-hacks-south-african-job-portal-against-child-labour/. [16 March 2016].

Vacca, J.R. (Ed.) (2013). *Computer and information security handbook*. 2nd Edition. Amsterdam, Netherlands: Elsevier/Morgan Kaufmann.

Vacca, J.R. & Rudolf, K. (2011). *System forensics, investigation, and response*. United States: Sudbury, MA: Jones & Bartlett Learning.

Valacich, J.S. & Schneider, C. (2013). *A global perspective of information technology.* Pearson.

Valli, C., Martinus, I. & Johnstone, M. (2014). Small to Medium Enterprise Cyber Security Awareness: An Initial Survey of Western Australian Business. *Proceedings of the 2014 International Conference on Security and Management*, 71-75, CSREA Press.

Van den Berg, J., Van Zoggel, J., Snels, M., Van Leeuwen, M., Boeke, S., Van de Koppen, L., Van der Lubbe, J., Van den Berg, B. & De Bos, T. (2014). *On the emergence of cyber security science and its challenges for cyber security education*. Paper at the NATO STO/IST-122 Symposium; October 13-14 2014; Tallinn: Estonia.

Van den Berg, L. (2015). The effect of theft on critical infrastructure. *IRMSA Risk Report 2015; Failure/Shortfall of critical infrastructure.* Available from: https://c.ymcdn.com/sites/irmsa.site-ym.com/resource/resmgr/2015_Risk_Report/Low_Res_IRMSA_South_Africa_R.pdf. [17 September 2016].

Van der Meulen, N.S. (2011). *Financial identity theft: Context, challenges and countermeasures.* The Hague, Netherlands: Asser Press.

Van der Meulen, R. (2015). Gartner says 6.4 billion connected “things” will be in use in 2016, up 30 percent from 2015. *Gartner/Newsroom/NewsReleases;* November 10, 2015. Available from: http://www.gartner.com/newsroom/id/3165317. [10 May 2016].

Van der Stroep, S.W. & Johnson, D.D. (2010). *Research methods for everyday life: Blending qualitative and quantitative approaches.* USA: John Wiley & Sons.

Van Grembergen, W. & De Haes, S. (Eds.) (2012). *Business strategy and applications in enterprise IT governance*. Hershey, PA, USA: IGI Global.

Van Griethuijsen, R.A.L.F, Van Eijck, M., Haste, H., Den Brok, P., Skinner, N.C., Mansour, N., Gencer, A.S. & BouJaoude, S. (2015). Global patterns in students' views of science and interest in science*. Research in Science Education;* 45(4):581-603. Available from: https://link.springer.com/article/10.1007/s11165-014-9438-6. [8 March 2018].

Van Heerden, J. (2016). In: Moyo, A. Standard Bank heist modus operandi 'not new'. *ITWeb/IT in Banking;* 24 May 2016. Available from: http://www.csoonline.com/article/2125140/metrics-budgets/it-risk-assessment-frameworks--real-world-experience.html#1. [22 July 2016].

Violino, B. (2010). IT risk assessment frameworks: Real-world experience*. CSO/Compliance/Risk;* May 3, 2010. Available from: http://www.csoonline.com/article/2125140/metrics-budgets/it-risk-assessment-frameworks--real-world-experience.html#1. [12 January 2016].

Volz, D. (2015). Cyber-attacks loom as growing corporate credit risk – Moody's. *Reuters/Intel;* November 23, 2015. Available from: http://www.reuters.com/article/cybersecurity-moodys-idUSL1N13I1U120151123. [18 March 2016].

Von Solms, B. (2012). In: Rasool, F. IT in Government: Postbank heist signals policy gap. *IT Web/IT in Government;* 23 January 2012. Available from: http://www.itweb.co.za/index.php?option=com_content&view=article&id=50818. [27 May 2015].

Von Solms, B. (2014). In: Brodie, N. How does cybercrime affect you? *Mens Health (Guy Skills Subsection);* 15 May 2014*.* Available from: http://www.mh.co.za/how-to/guy-wisdom/how-does-cybercrime-affect-you/. [3 June 2016].

Von Solms, B. (2014). In: Jones, G. South Africa neglects alarming effect of cybercrime. *BusinessLIVE;* 14 January 2014. Available from: http://www.bdlive.co.za/business/2014/01/14/south-africa-neglects-alarming-effect-of-cybercrime. [29 May 2015].

Von Solms, B. (2015). How South Africa is fighting cyber-crime*. The Conversation;* 21 November 2015. Available from: http://mybroadband.co.za/news/security/145009-how-south-africa-is-fighting-cyber-crime.html?utm_source=dlvr.it&utm_medium=twitter. [9 March 2016].

Wall, D.S. (2012). *Enemies within: Redefining the insider threat in organisational security policy*. UK: Palgrave Macmillan.

Wallace, M. & Webber, L. (2015). *IT governance policies & procedures*. NY, USA: Wolters Kluwer.

Walliman, N. (2011). *Research methods: The basics.* New York: Routledge,

Warren, P. & Streeter, M. (2013). *Cyber-crime & warfare: all that matters*. Available from: https://books.google.co.za/books?id=DbWOaNRrJJUC&printsec=frontcover#v=onepage&q&f=false. [10 July 2016].

Weathington, B.L., Cunningham, C.J.L. & Pittenger, D.J. (2012). *Understanding business research*. New Jersey: Wiley.

Weckert, J. & Lucas, R. (2013). *Professionalism in the information and communication technology industry*. Australia: ANU E Press.

Weiers, R.M. (2008) *Introduction to business statistics*. 6th Edition. USA: Cengage Learning.

Welman, J.C., Kruger, S.J. & Mitchell, L. (2009). *Research methodology*. 2nd Edition. Cape Town: Oxford University Press.

Wechsler, H. (2015). Cyberspace security using adversarial learning and conformal prediction. *Intelligent Information Management*; 7(4);2015. Available from: http://file.scirp.org/Html/2-8701339_57866.htm. [24 June 2016].

Weston, R. (2012). *Gold: A world survey*. NY, USA: Routledge.

White, S. (2014). Global cyber-attacks rose 48% in 2014. *Journal of Accountancy;* October 8, 2014. Available from:

http://www.journalofaccountancy.com/news/2014/oct/201411089.html. [22 November 2015].

Widup, S., & Spitler, M., Hylender, D. & Bassett, G. (2018). 2018 Verizon Data Breach Investigations Report. Verizon Enterprise Solutions. Available from: https://www.researchgate.net/scientific-contributions/2092370455_Gabriel_Bassett; doi: 10.13140/RG.2.1.2632.7124. [16 July 2019].

Williams, G.F. (2011). *The diamond mines of South Africa*. NY, USA: Cambridge University Press.

Williams, J. (2015) What is cyber crime? *Study.com; Criminal Justice Course 101: Intro to Criminal Justice.* Available from: from http://study.com/academy/lesson/what-is-cyber-crime-definition-types-examples.html. [21 November 2015].

Williams, R. (2014). Cyber-crime costs global economy $445 bn annually. *The Telegraph, UK;* 9 June 2014. Available from: http://www.telegraph.co.uk/technology/internet-security/10886640/Cyber-crime-costs-global-economy-445-bn-annually.html. [21 June 2016].

Wilshusen, G.C. (2012). *Cybersecurity: Threats impacting the nation: Congressional testimony*. USA: Diane Publishing.

Wilson, J. (2013). *Essentials of business research: A guide for doing your research project*. 2nd Edition. London: Sage.

Wori, O. (2014). Computer crimes: Factors of cybercriminal activities. *International Journal of Advanced Computer Science and Information Technology2014*, 3(1):51-67. Available from: http://www.technical.cloud-journals.com/index.php/IJACSIT/article/download/Tech-136/pdf. [10 June 2016].

World Economic Forum (WEF). (2015). *Global Risks 2015 – Insight Report.* 10th Edition. Geneva, Switzerland: World Economic Forum.

Yar, M. (2013). *Cybercrime and society*. 2nd Edition. London: Sage Publications.

Yeo, S., Cho, E., Kim, J. & Vasilyevna, N. (2008). Malware and antivirus deployment for enterprise IT security. In: *Ubiquitous Multimedia Computing, International Symposium;* 2008: 252-255. Available from: https://doi.ieeecomputersociety.org/10.1109/UMC.2008.58. [19 March 2018].

Yin, R.K. (2003). *Case study research: Design and methods*. 3rd Edition. London: Sage.

Yu, T. & Richardson, J.C. (2018). An exploratory factor analysis and reliability analysis of the Student Online Learning Readiness (SOLR) instrument. *Online Learning*, 19(5), December 2015. Available from: https://files.eric.ed.gov/fulltext/EJ1085767.pdf. [12 July 2019].

Zakon, R.H. (2016). Hobbes' Internet timeline. *Zakon.org.* Available from: http://www.zakon.org/robert/internet/timeline/. [3 May 2016].

Zandbergen, P. (2016). What is the history of the Internet? *Study.com; Business 109/Intro to computing.* Available from: http://study.com/academy/lesson/what-is-the-history-of-the-internet-origins-timeline.html. [3 May 2016].

Zapo, G. (2015). Cybercrime affects more than 431 million adult victims globally. *INQUISITR;* February 22, 2015. Available from: http://www.inquisitr.com/1862348/cybercrime-affects-431-million-adult-victims-globally/. [18 June 2016].

Zeltser, L. (2015) How antivirus works: Virus detection techniques. *SearchSecurity/TechTarget; Problem Solve.* Available from: http://searchsecurity.techtarget.com/tip/How-antivirus-software-works-Virus-detection-techniques. [10 July 2016].

Zereini, F. & Wiseman, C.L.S. (2015). *Platinum metals in the environment*. Berlin/Heidelberg: Springer-Verlag.

Zikmund, W.G., Babin, B.J., Carr, C.J. & Griffin, M. (2013). *Business research methods*. 9th Edition. Canada: Erin Joyner.

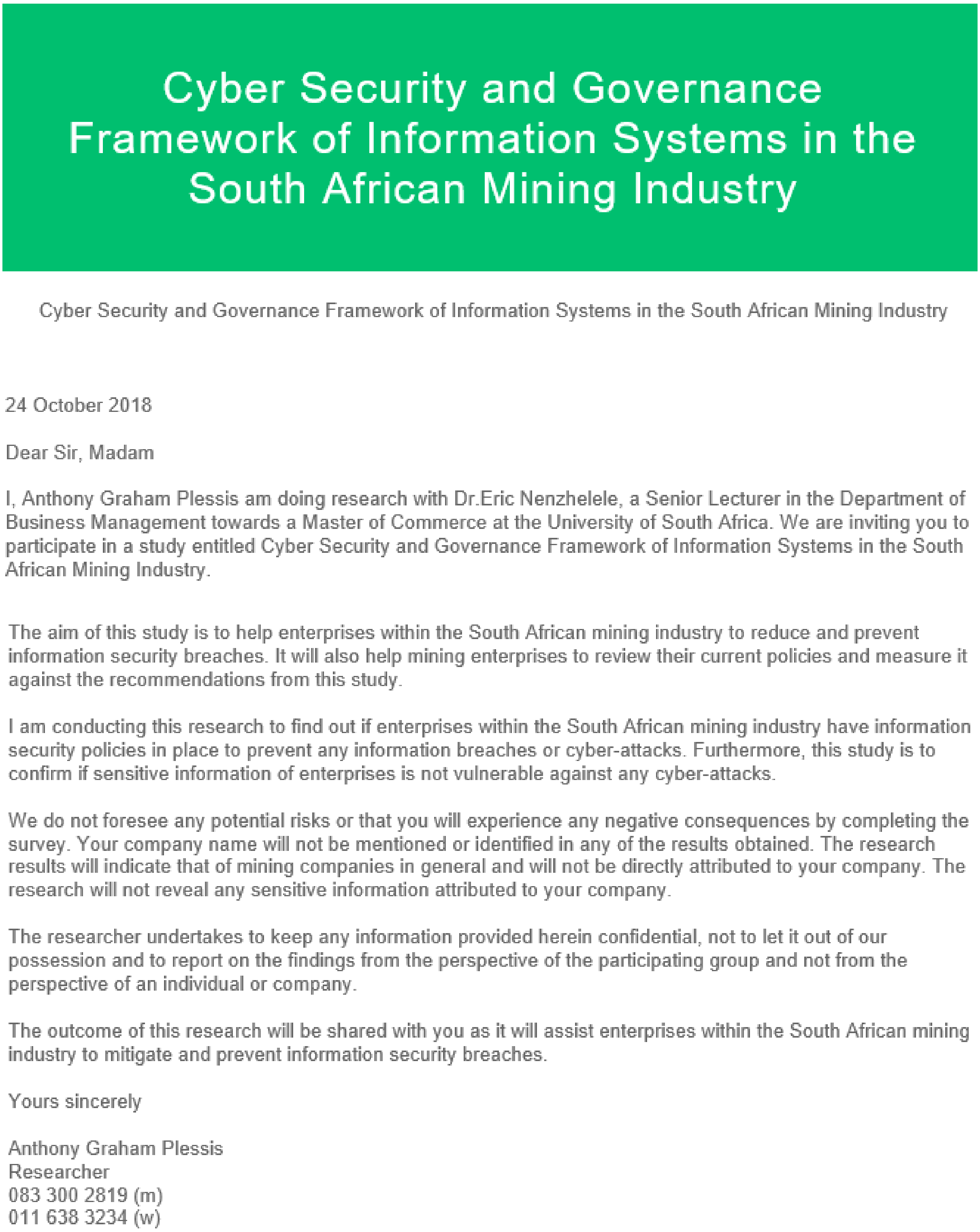
Zikmund, W.G. & Babin, B.J. (2013b). *Essentials of marketing research*. 5th Edition. Mason, OH, USA: South Western/Cengage Learning.

Zimmer, C. (2012). *A planet of viruses*. USA: University of Chicago Press.

Zimmermann, K.A. & Emspak, J. (2014). Internet history timeline. *LIVESCIENCE*. Available from: http://www.livescience.com/20727-internet-history.html. [3 May 2016].

APPENDIX A: FINAL QUESTIONNAIRE

INFORMATION SECURITY IN THE SOUTH AFRICAN MINING INDUSTRY



Cyber Security and Governance Framework of Information Systems in the South African Mining Industry

Cyber Security and Governance Framework of Information Systems in the South African Mining Industry

24 October 2018

Dear Sir, Madam

I, Anthony Graham Plessis am doing research with Dr.Eric Nenzhelele, a Senior Lecturer in the Department of Business Management towards a Master of Commerce at the University of South Africa. We are inviting you to participate in a study entitled Cyber Security and Governance Framework of Information Systems in the South African Mining Industry.

The aim of this study is to help enterprises within the South African mining industry to reduce and prevent information security breaches. It will also help mining enterprises to review their current policies and measure it against the recommendations from this study.

I am conducting this research to find out if enterprises within the South African mining industry have information security policies in place to prevent any information breaches or cyber-attacks. Furthermore, this study is to confirm if sensitive information of enterprises is not vulnerable against any cyber-attacks.

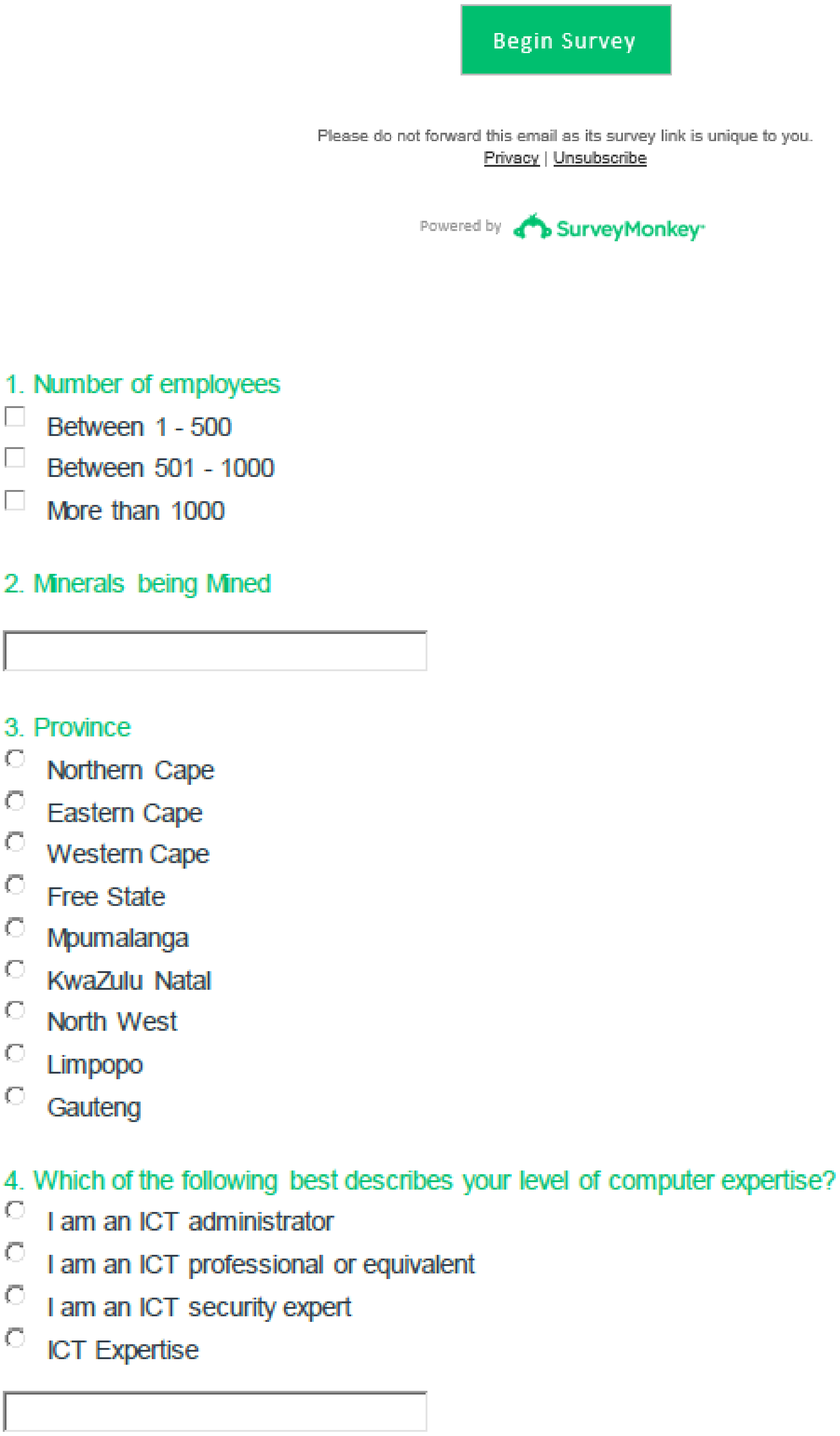
We do not foresee any potential risks or that you will experience any negative consequences by completing the survey. Your company name will not be mentioned or identified in any of the results obtained. The research results will indicate that of mining companies in general and will not be directly attributed to your company. The research will not reveal any sensitive information attributed to your company.

The researcher undertakes to keep any information provided herein confidential, not to let it out of our possession and to report on the findings from the perspective of the participating group and not from the perspective of an individual or company.

The outcome of this research will be shared with you as it will assist enterprises within the South African mining industry to mitigate and prevent information security breaches.

Yours sincerely

Anthony Graham Plessis
Researcher
083 300 2819 (m)
011 638 3234 (w)



Please do not forward this email as its survey link is unique to you.
Privacy | Unsubscribe

1. Number of employees

- □ Between 1 - 500
- □ Between 501 - 1000
- □ More than 1000

2. Minerals being Mined

□

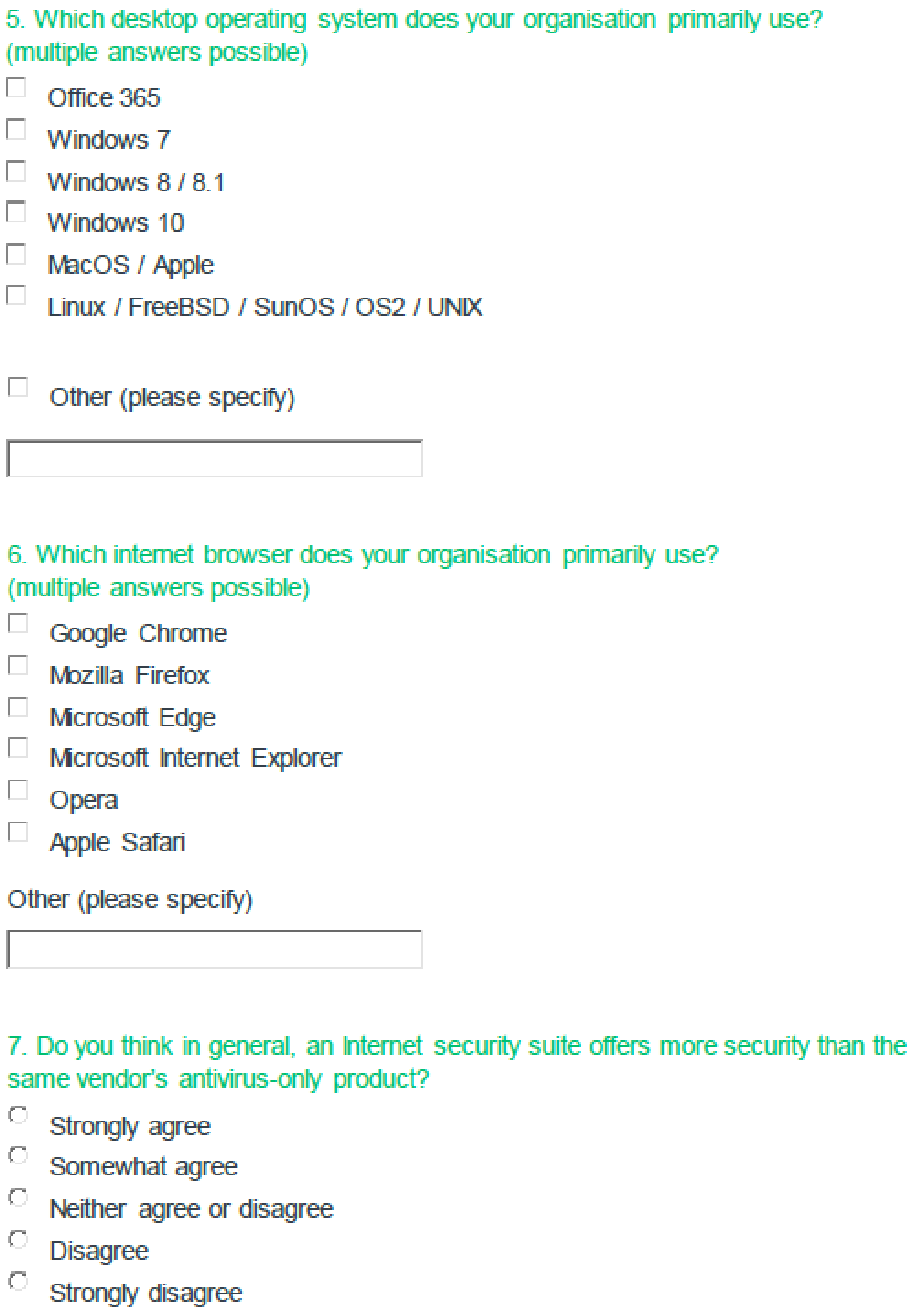
3. Province

- ○ Northern Cape
- ○ Eastern Cape
- ○ Western Cape
- ○ Free State
- ○ Mpumalanga
- ○ KwaZulu Natal
- ○ North West
- ○ Limpopo
- ○ Gauteng

4. Which of the following best describes your level of computer expertise?

- ○ I am an ICT administrator
- ○ I am an ICT professional or equivalent
- ○ I am an ICT security expert
- ○ ICT Expertise

□



5. Which desktop operating system does your organisation primarily use? (multiple answers possible)

□ Office 365
□ Windows 7
□ Windows 8 / 8.1
□ Windows 10
□ MacOS / Apple
□ Linux / FreeBSD / SunOS / OS2 / UNIX

□ Other (please specify)

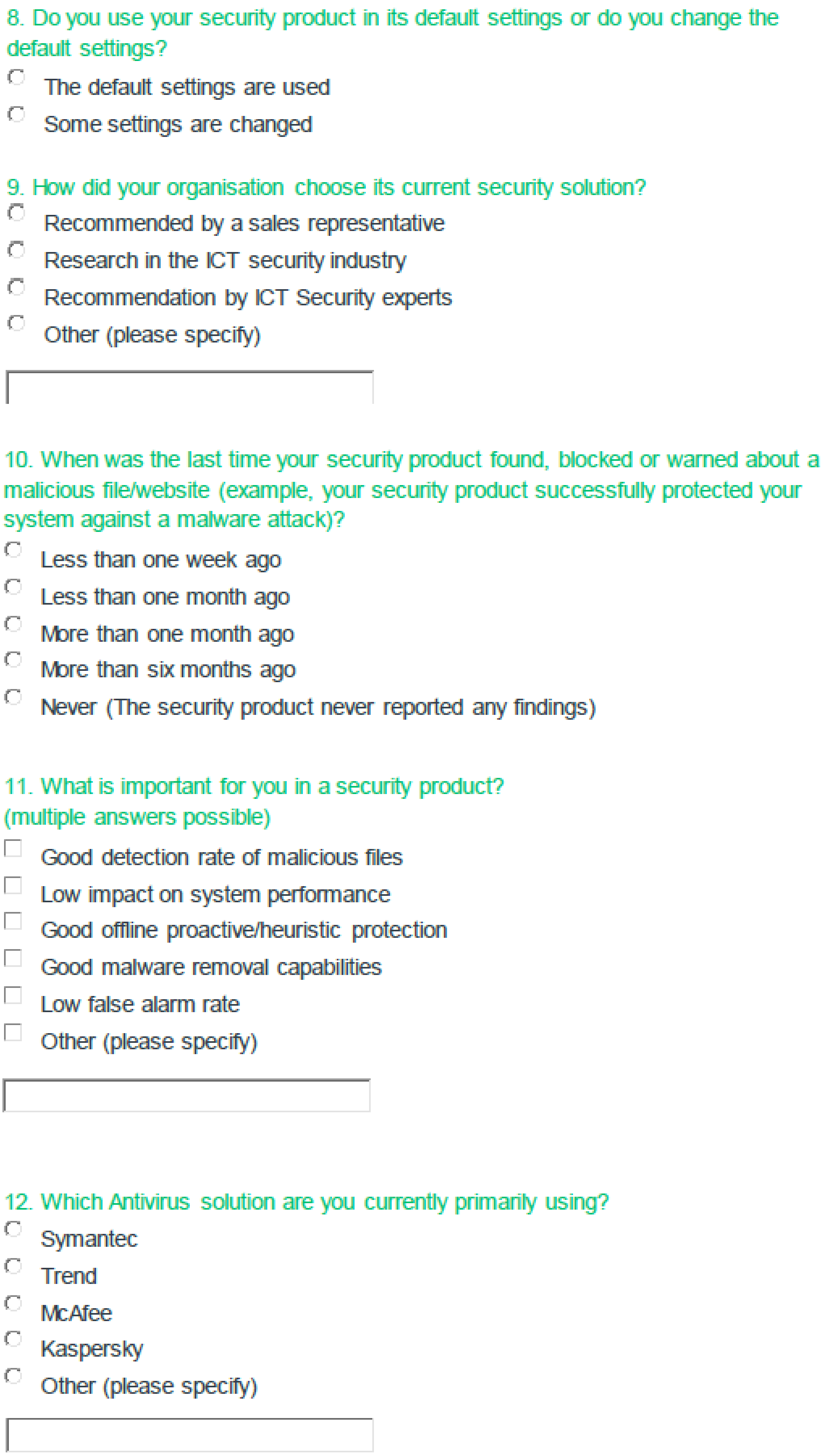
6. Which internet browser does your organisation primarily use? (multiple answers possible)

□ Google Chrome
□ Mozilla Firefox
□ Microsoft Edge
□ Microsoft Internet Explorer
□ Opera
□ Apple Safari

Other (please specify)

7. Do you think in general, an Internet security suite offers more security than the same vendor's antivirus-only product?

○ Strongly agree
○ Somewhat agree
○ Neither agree or disagree
○ Disagree
○ Strongly disagree



8. Do you use your security product in its default settings or do you change the default settings?

○ The default settings are used

○ Some settings are changed

9. How did your organisation choose its current security solution?

○ Recommended by a sales representative

○ Research in the ICT security industry

○ Recommendation by ICT Security experts

○ Other (please specify)

10. When was the last time your security product found, blocked or warned about a malicious file/website (example, your security product successfully protected your system against a malware attack)?

○ Less than one week ago

○ Less than one month ago

○ More than one month ago

○ More than six months ago

○ Never (The security product never reported any findings)

11. What is important for you in a security product?
(multiple answers possible)

□ Good detection rate of malicious files

□ Low impact on system performance

□ Good offline proactive/heuristic protection

□ Good malware removal capabilities

□ Low false alarm rate

□ Other (please specify)

12. Which Antivirus solution are you currently primarily using?

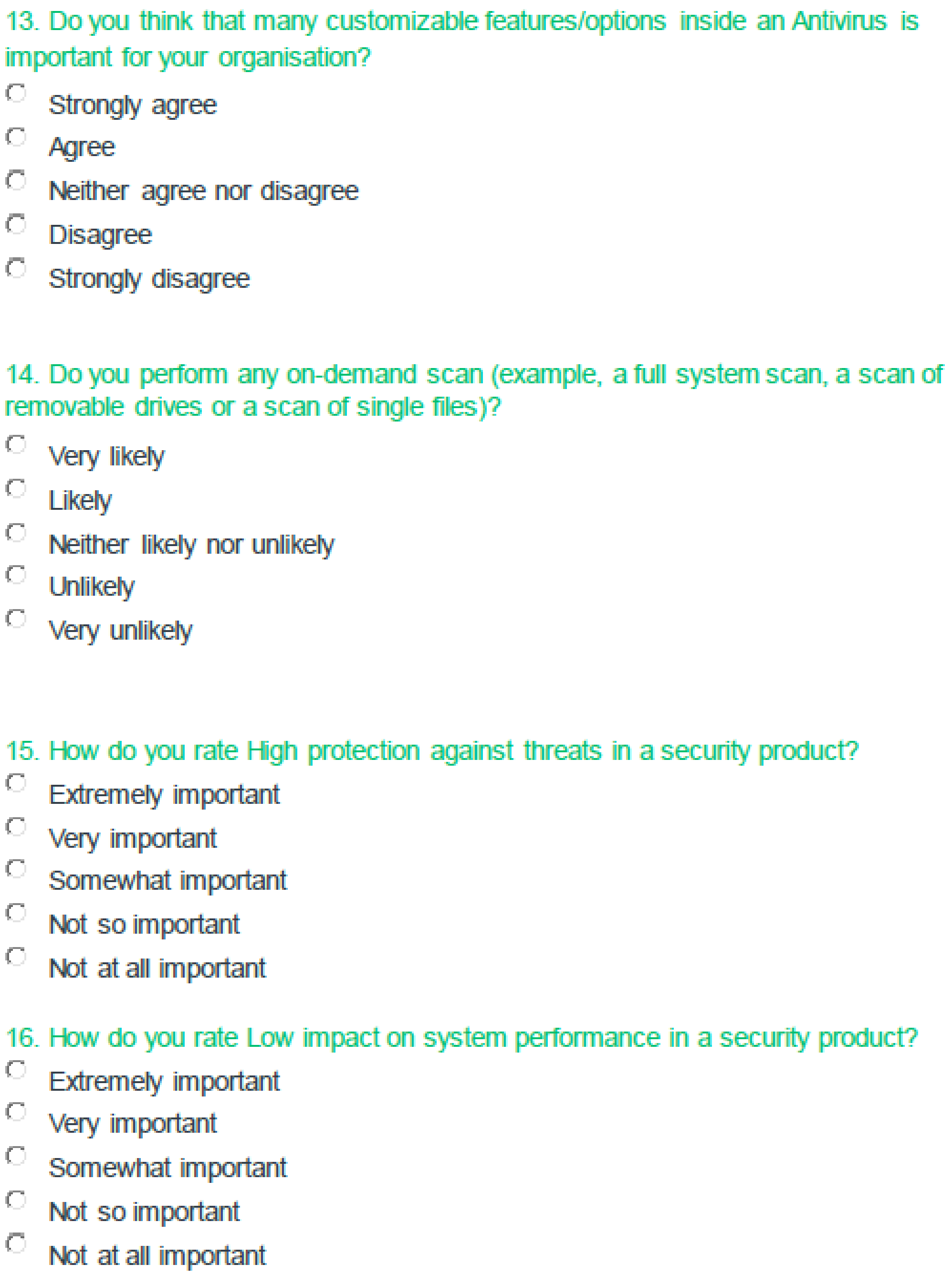
○ Symantec

○ Trend

○ McAfee

○ Kaspersky

○ Other (please specify)



13. Do you think that many customizable features/options inside an Antivirus is important for your organisation?

○ Strongly agree
○ Agree
○ Neither agree nor disagree
○ Disagree
○ Strongly disagree

14. Do you perform any on-demand scan (example, a full system scan, a scan of removable drives or a scan of single files)?

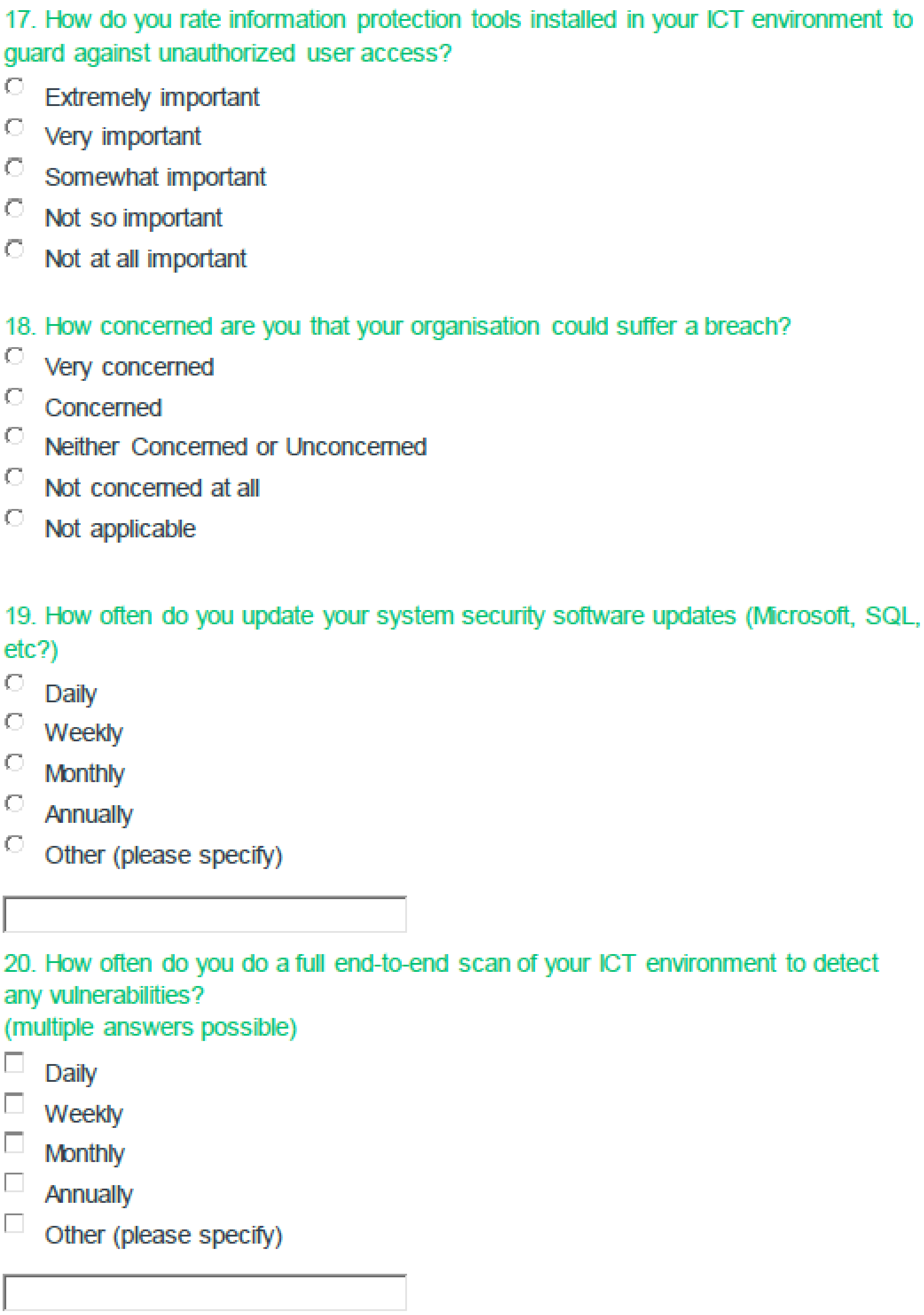
○ Very likely
○ Likely
○ Neither likely nor unlikely
○ Unlikely
○ Very unlikely

15. How do you rate High protection against threats in a security product?

○ Extremely important
○ Very important
○ Somewhat important
○ Not so important
○ Not at all important

16. How do you rate Low impact on system performance in a security product?

○ Extremely important
○ Very important
○ Somewhat important
○ Not so important
○ Not at all important



17. How do you rate information protection tools installed in your ICT environment to guard against unauthorized user access?

○ Extremely important
○ Very important
○ Somewhat important
○ Not so important
○ Not at all important

18. How concerned are you that your organisation could suffer a breach?

○ Very concerned
○ Concerned
○ Neither Concerned or Unconcerned
○ Not concerned at all
○ Not applicable

19. How often do you update your system security software updates (Microsoft, SQL, etc?)

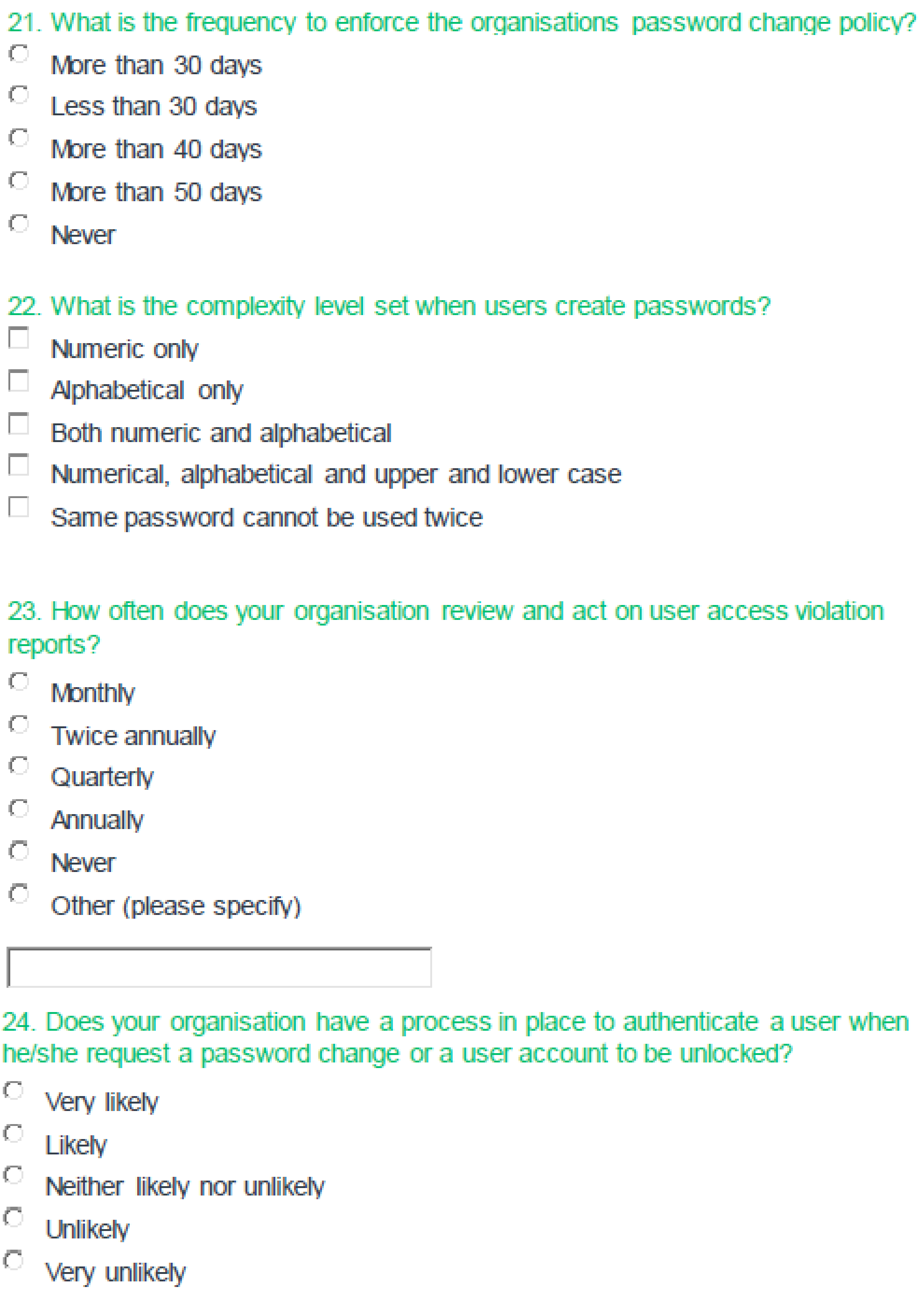
○ Daily
○ Weekly
○ Monthly
○ Annually
○ Other (please specify)

____

20. How often do you do a full end-to-end scan of your ICT environment to detect any vulnerabilities?
(multiple answers possible)

□ Daily
□ Weekly
□ Monthly
□ Annually
□ Other (please specify)

____



21. What is the frequency to enforce the organisations password change policy?

○ More than 30 days
○ Less than 30 days
○ More than 40 days
○ More than 50 days
○ Never

22. What is the complexity level set when users create passwords?

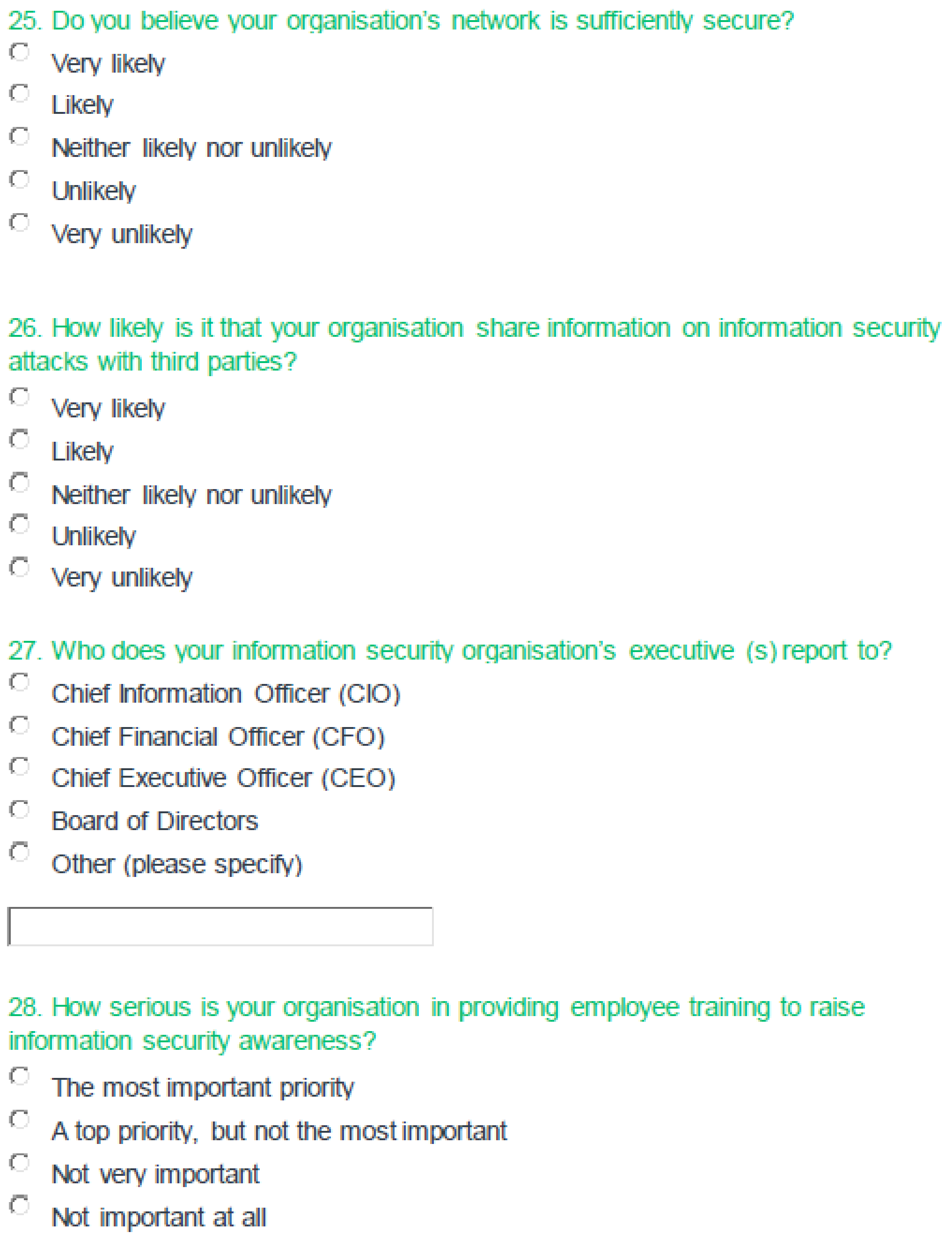
□ Numeric only
□ Alphabetical only
□ Both numeric and alphabetical
□ Numerical, alphabetical and upper and lower case
□ Same password cannot be used twice

23. How often does your organisation review and act on user access violation reports?

○ Monthly
○ Twice annually
○ Quarterly
○ Annually
○ Never
○ Other (please specify)

24. Does your organisation have a process in place to authenticate a user when he/she request a password change or a user account to be unlocked?

○ Very likely
○ Likely
○ Neither likely nor unlikely
○ Unlikely
○ Very unlikely



25. Do you believe your organisation's network is sufficiently secure?

○ Very likely
○ Likely
○ Neither likely nor unlikely
○ Unlikely
○ Very unlikely

26. How likely is it that your organisation share information on information security attacks with third parties?

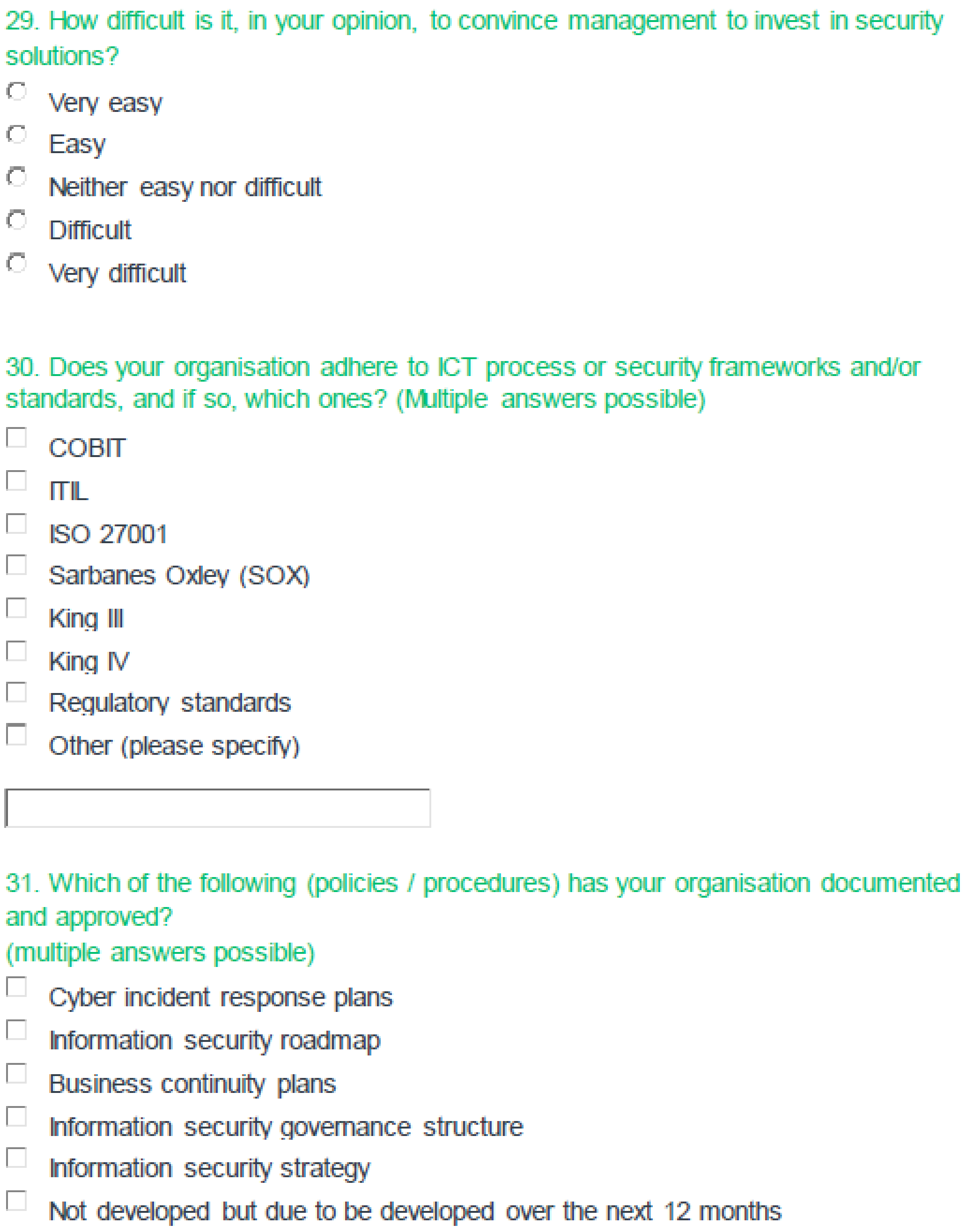
○ Very likely
○ Likely
○ Neither likely nor unlikely
○ Unlikely
○ Very unlikely

27. Who does your information security organisation's executive (s) report to?

○ Chief Information Officer (CIO)
○ Chief Financial Officer (CFO)
○ Chief Executive Officer (CEO)
○ Board of Directors
○ Other (please specify)

28. How serious is your organisation in providing employee training to raise information security awareness?

○ The most important priority
○ A top priority, but not the most important
○ Not very important
○ Not important at all



29. How difficult is it, in your opinion, to convince management to invest in security solutions?

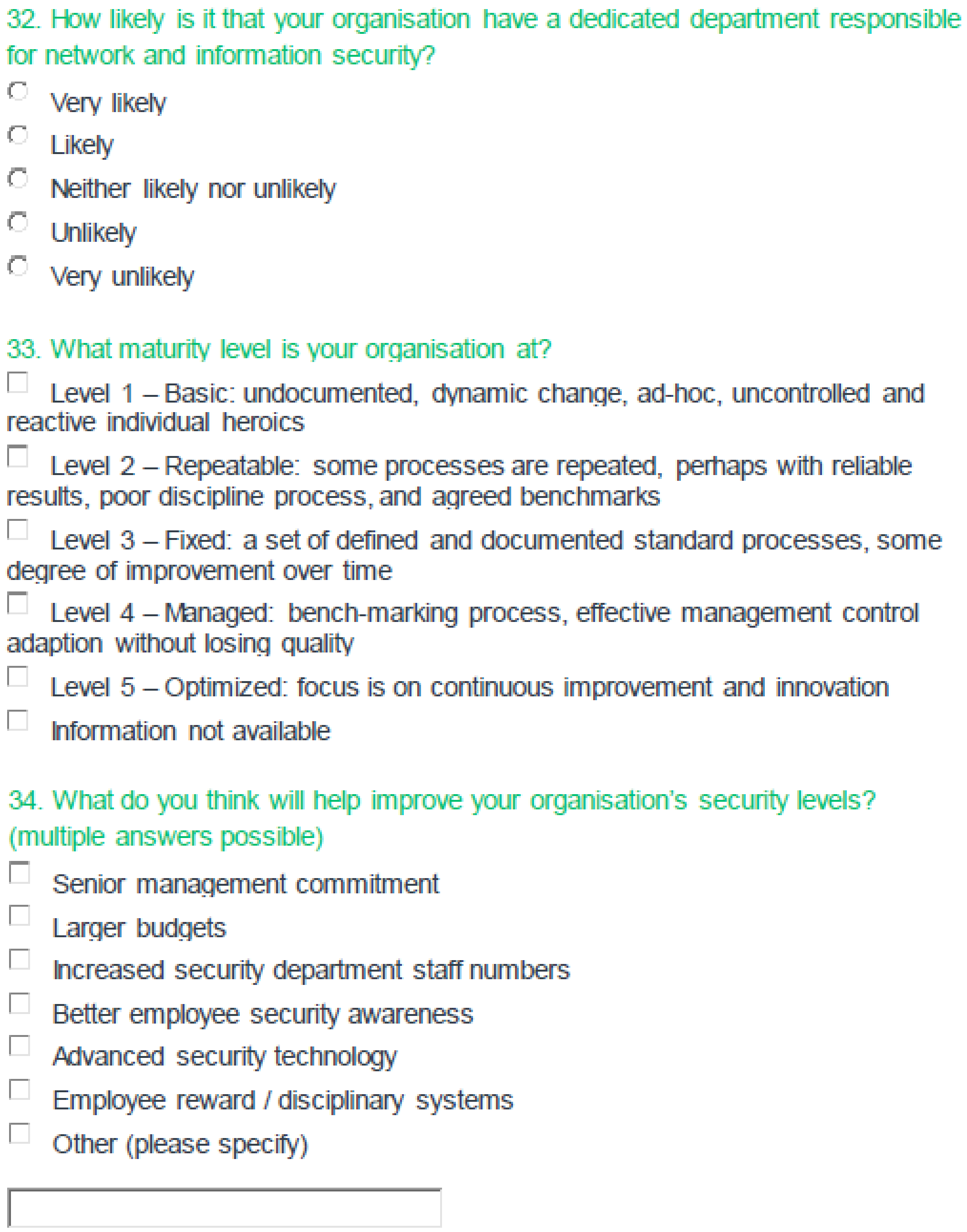
○ Very easy
○ Easy
○ Neither easy nor difficult
○ Difficult
○ Very difficult

30. Does your organisation adhere to ICT process or security frameworks and/or standards, and if so, which ones? (Multiple answers possible)

□ COBIT
□ ITIL
□ ISO 27001
□ Sarbanes Oxley (SOX)
□ King III
□ King IV
□ Regulatory standards
□ Other (please specify)

31. Which of the following (policies / procedures) has your organisation documented and approved?
(multiple answers possible)

□ Cyber incident response plans
□ Information security roadmap
□ Business continuity plans
□ Information security governance structure
□ Information security strategy
□ Not developed but due to be developed over the next 12 months



32. How likely is it that your organisation have a dedicated department responsible for network and information security?

○ Very likely

○ Likely

○ Neither likely nor unlikely

○ Unlikely

○ Very unlikely

33. What maturity level is your organisation at?

□ Level 1 – Basic: undocumented, dynamic change, ad-hoc, uncontrolled and reactive individual heroics

□ Level 2 – Repeatable: some processes are repeated, perhaps with reliable results, poor discipline process, and agreed benchmarks

□ Level 3 – Fixed: a set of defined and documented standard processes, some degree of improvement over time

□ Level 4 – Managed: bench-marking process, effective management control adaption without losing quality

□ Level 5 – Optimized: focus is on continuous improvement and innovation

□ Information not available

34. What do you think will help improve your organisation's security levels? (multiple answers possible)

□ Senior management commitment

□ Larger budgets

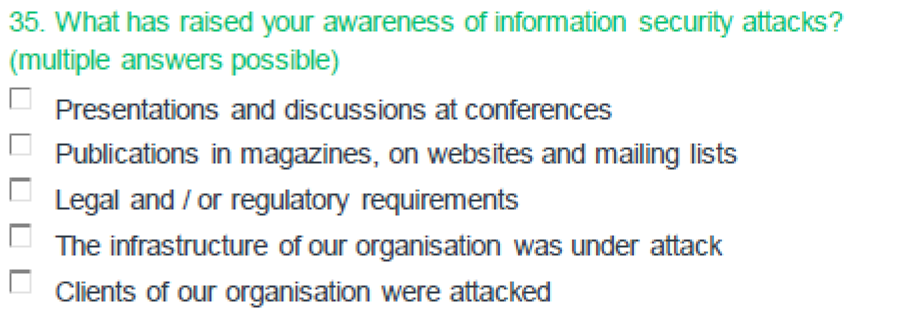
□ Increased security department staff numbers

□ Better employee security awareness

□ Advanced security technology

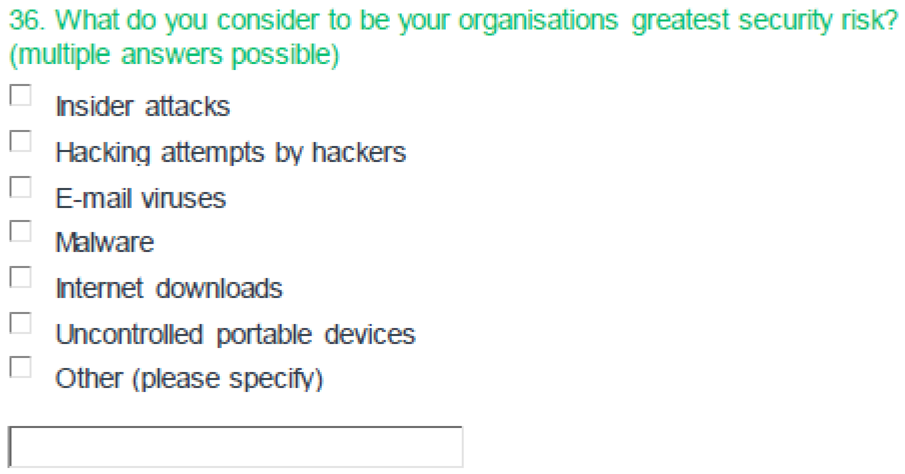
□ Employee reward / disciplinary systems

□ Other (please specify)



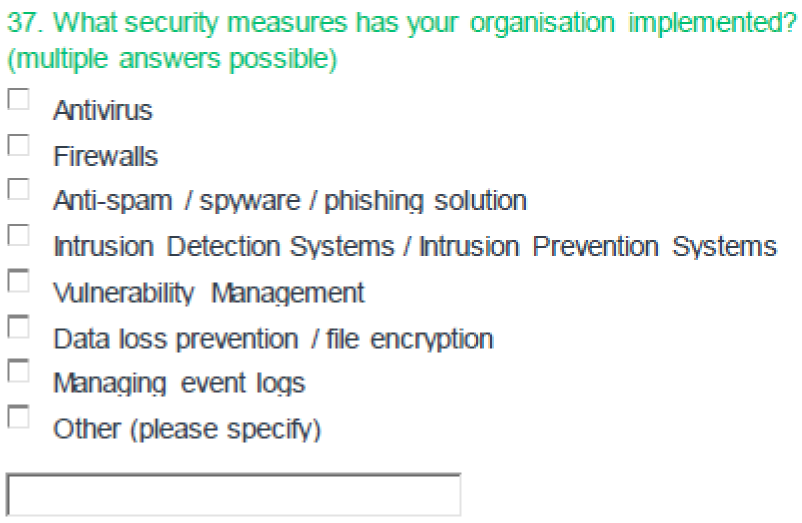
35. What has raised your awareness of information security attacks? (multiple answers possible)

□ Presentations and discussions at conferences
□ Publications in magazines, on websites and mailing lists
□ Legal and / or regulatory requirements
□ The infrastructure of our organisation was under attack
□ Clients of our organisation were attacked



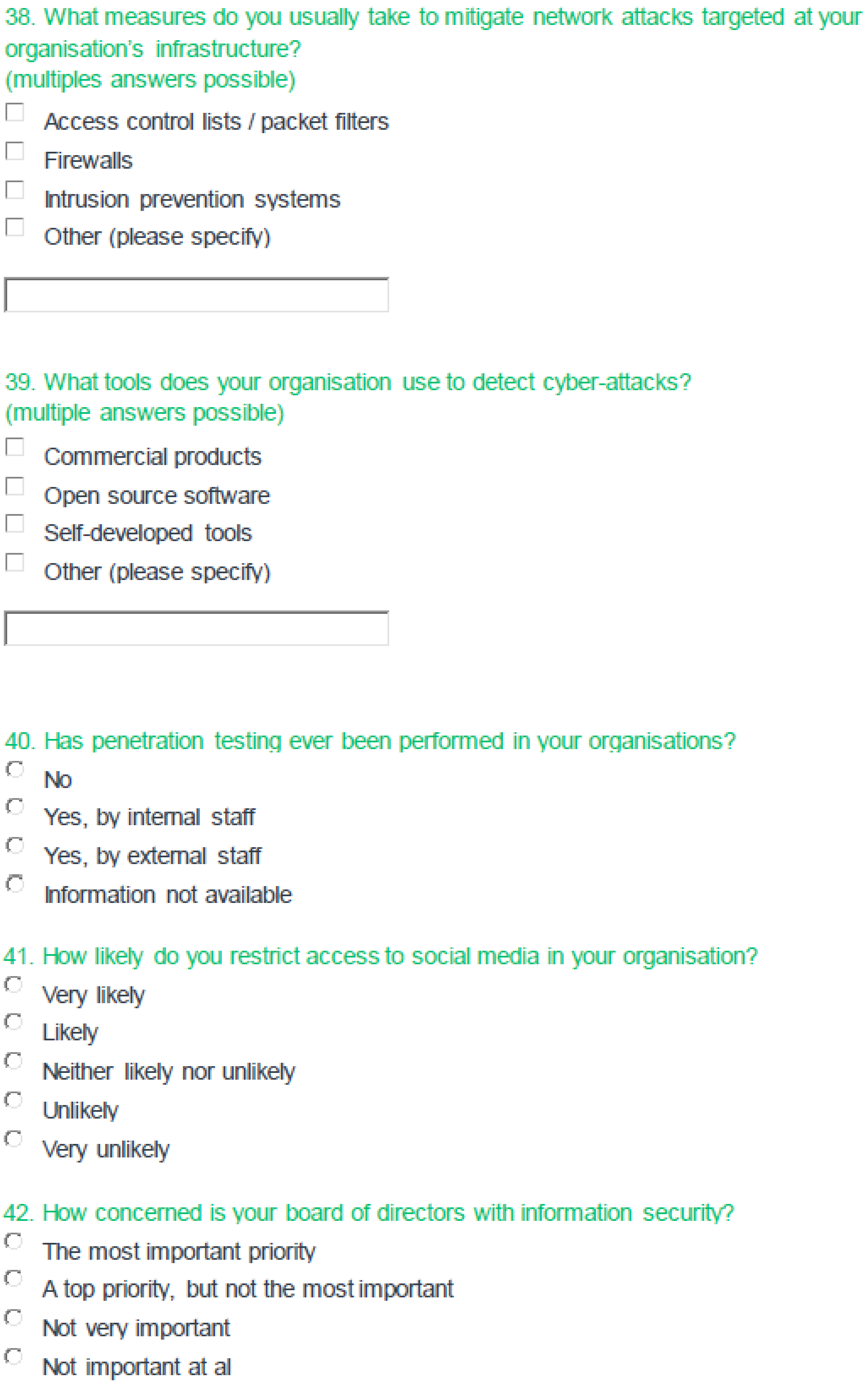
36. What do you consider to be your organisations greatest security risk? (multiple answers possible)

□ Insider attacks
□ Hacking attempts by hackers
□ E-mail viruses
□ Malware
□ Internet downloads
□ Uncontrolled portable devices
□ Other (please specify)



37. What security measures has your organisation implemented? (multiple answers possible)

□ Antivirus
□ Firewalls
□ Anti-spam / spyware / phishing solution
□ Intrusion Detection Systems / Intrusion Prevention Systems
□ Vulnerability Management
□ Data loss prevention / file encryption
□ Managing event logs
□ Other (please specify)



38. What measures do you usually take to mitigate network attacks targeted at your organisation's infrastructure?
(multiples answers possible)

☐ Access control lists / packet filters
☐ Firewalls
☐ Intrusion prevention systems
☐ Other (please specify)

39. What tools does your organisation use to detect cyber-attacks?
(multiple answers possible)

☐ Commercial products
☐ Open source software
☐ Self-developed tools
☐ Other (please specify)

40. Has penetration testing ever been performed in your organisations?

○ No
○ Yes, by internal staff
○ Yes, by external staff
○ Information not available

41. How likely do you restrict access to social media in your organisation?

○ Very likely
○ Likely
○ Neither likely nor unlikely
○ Unlikely
○ Very unlikely

42. How concerned is your board of directors with information security?

○ The most important priority
○ A top priority, but not the most important
○ Not very important
○ Not important at al

APPENDIX B: INITIAL QUESTIONNAIRE BEFORE VALIDATION

INFORMATION SECURITY IN THE SOUTH AFRICAN MINING INDUSTRY

BY ANTHONY PLESSIS (M.COM STUDENT AND PRINCIPAL RESEARCHER)

SUPERVISED BY: DR ERIC NENZHELELE

FINAL YEAR FUNDED BY: SAIFM/IMARA Bursary Schemes

Request for permission to conduct research at De Beers Group of Companies

Cyber Security and Governance Framework of Information Systems in the South African Mining Industry

20 April 2018

Mr. Derrick Oberholzer

Specialist Threat Management, Global IM

Dear Mr. Oberholzer,

I, Anthony Graham Plessis am doing research with Dr. Eric Nenzhelele, a Senior Lecturer in the Department of Business Management towards a Master of Commerce at the University of South Africa. We are inviting you to participate in a study entitled **Cyber Security and Governance Framework of Information Systems** in the South African Mining Industry.

The aim of this study is to help enterprises within the South African mining industry to reduce and understand information security breaches. It will also help mining enterprises to review their current information security processes and measure it against the recommendations from this study.

I am conducting this research to find out if enterprises within the South African mining industry have information security processes in place to prevent any information breaches or cyber-attacks. Furthermore, this study is to confirm if sensitive information of enterprises is not vulnerable against any cyber-attacks.

Your company has been selected as a participant in this research because it meets all the requirements of this research in terms of Information Security as well as its Information Communication and Technology infrastructure which are the components that enable modern computing. The feedback given, will assist in formulating a framework to guard against the vulnerabilities of information within the South African mining industry.

The contact details of your company were obtained from your company internet web site and annual reports. I have also found your details on Linked-in and or Information security interest groups, information security peer review forums and technical and professional community user groups to obtain the contact details of Information Security Administrators or Information custodians. This questionnaire will be sent to the Information Security Administrators or custodians of the selected companies.

We do not foresee any potential risks or that you will experience any negative consequences by completing the survey. Your company name or any other information pertaining to you will not be mentioned or identified in any of the results obtained. The research results will indicate that of mining companies in general and will not be directly attributed to your company. The research will not reveal any sensitive information attributed to your company.

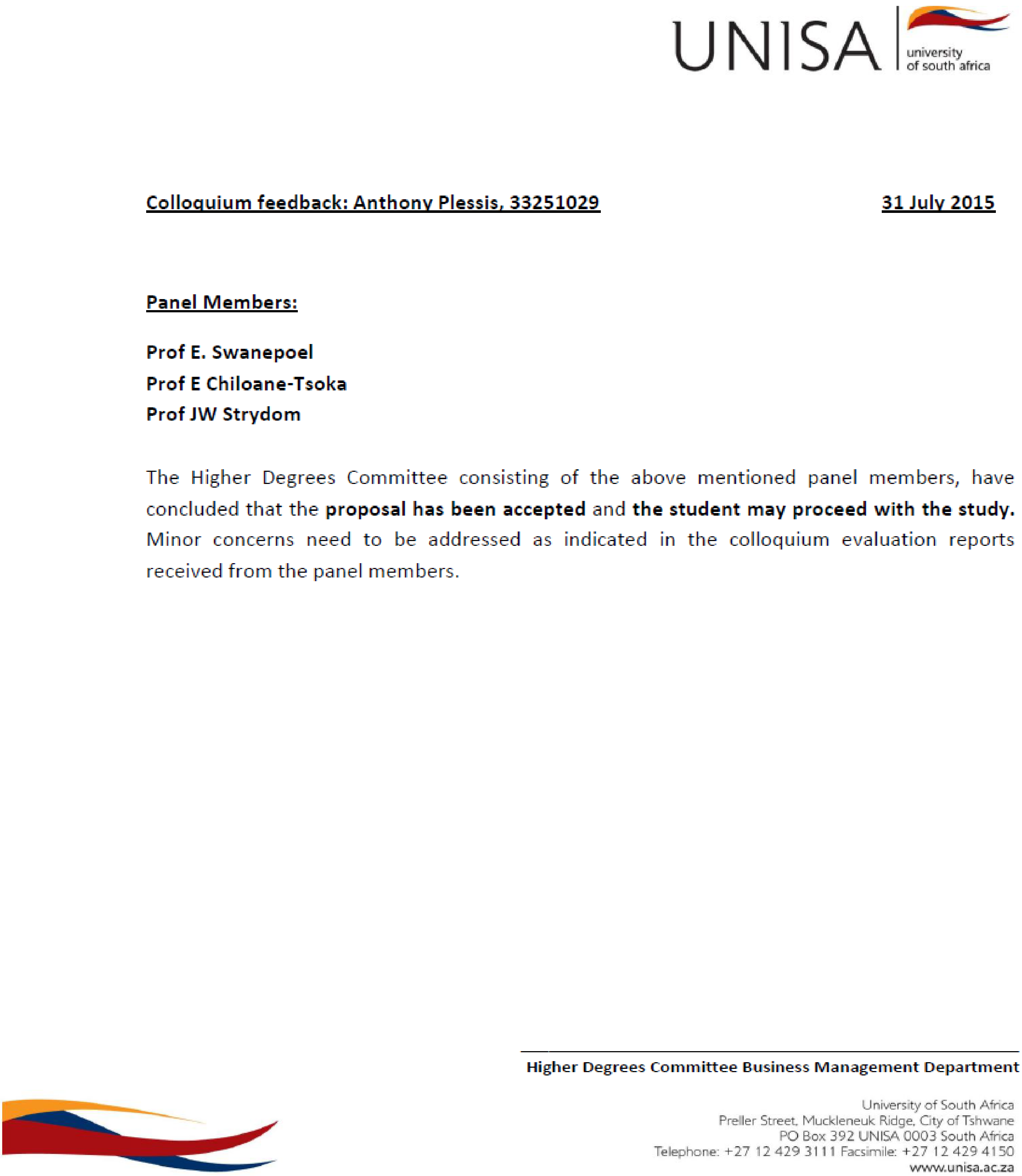
The researcher undertakes to keep any information provided herein confidential, not to let it out of our possession and to report on the findings from the perspective of the participating group and not from the perspective of an individual or company.

The outcome of this research will be shared with you as it will assist enterprises within the South African mining industry to mitigate and lessen information security breaches. It will also help mining enterprises to review their current policies and measure it against the recommendations from this study.

Yours sincerely

Anthony Graham Plessis
Researcher
mailto: anthony.plessis@angloamerican.com
083 300 2819 (m)
011 638 3234 (w)

APPENDIX C: COLLOQUIUM COMMITTEE CERTIFICATE



UNISA university of south africa

Colloquium feedback: Anthony Plessis, 33251029 **31 July 2015**

Panel Members:

Prof E. Swanepoel
Prof E Chiloane-Tsoka
Prof JW Strydom

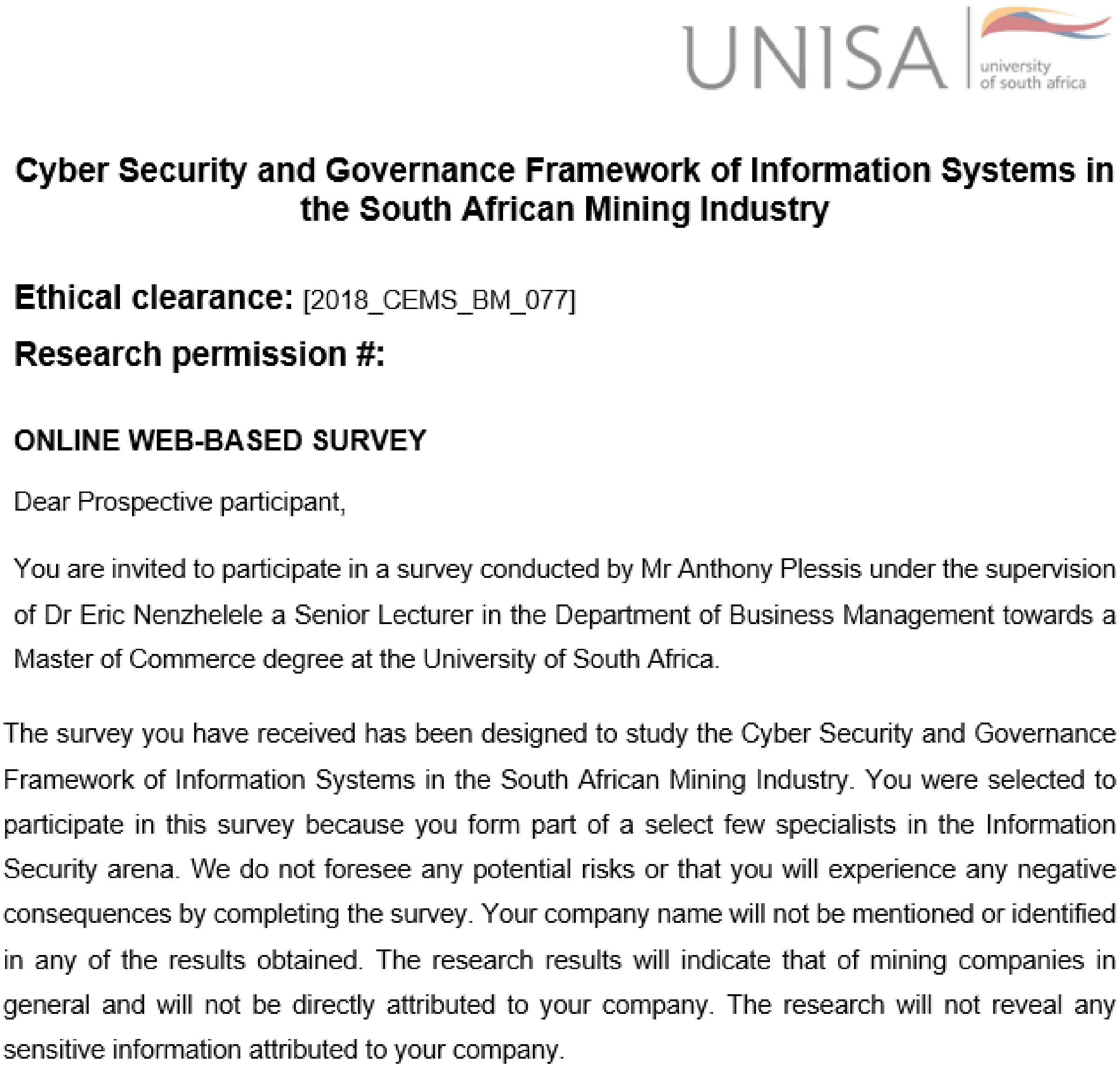
The Higher Degrees Committee consisting of the above mentioned panel members, have concluded that the **proposal has been accepted** and **the student may proceed with the study.** Minor concerns need to be addressed as indicated in the colloquium evaluation reports received from the panel members.

Higher Degrees Committee Business Management Department

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

APPENDIX D: INFORMED CONSENT

PARTICIPATION INFORMATION SHEET



UNISA university of south africa

Cyber Security and Governance Framework of Information Systems in the South African Mining Industry

Ethical clearance: [2018_CEMS_BM_077]

Research permission #:

ONLINE WEB-BASED SURVEY

Dear Prospective participant,

You are invited to participate in a survey conducted by Mr Anthony Plessis under the supervision of Dr Eric Nenzhelele a Senior Lecturer in the Department of Business Management towards a Master of Commerce degree at the University of South Africa.

The survey you have received has been designed to study the Cyber Security and Governance Framework of Information Systems in the South African Mining Industry. You were selected to participate in this survey because you form part of a select few specialists in the Information Security arena. We do not foresee any potential risks or that you will experience any negative consequences by completing the survey. Your company name will not be mentioned or identified in any of the results obtained. The research results will indicate that of mining companies in general and will not be directly attributed to your company. The research will not reveal any sensitive information attributed to your company.

It is anticipated that the information we gain from this survey will help us to assist enterprises within the South African mining industry to mitigate and prevent information security breaches. It will also help mining enterprises to review their current policies and measure it against the recommendations from this study. You are, however, under no obligation to complete the survey and you can withdraw from the study prior to submitting the survey. Any identifying information that is obtained regarding this survey will remain confidential and will only be disclosed with your permission or as required by law. If you choose to participate in this survey it will take no more than ten minutes of your time. We do not foresee that you will experience any negative consequences by completing the survey. The researcher undertakes to keep any information provided herein confidential, not to let it out of our possession and to report on the findings from the perspective of the participating group and not from the perspective of an individual or company.

The outcome of this research will be shared with you as it will assist enterprises within the South African mining industry to mitigate and prevent information security breaches. It will also help mining enterprises to review their current policies and measure it against the recommendations from this study.

The records will be kept for five years for audit purposes where after it will be permanently destroyed and electronic versions will be permanently deleted from the database in which it resides. You will not be reimbursed or receive any incentives for your participation in the survey.

The research was reviewed and approved by the Unisa Ethics Review Committee. The primary researcher, Mr Anthony Graham Plessis, can be contacted during office hours at 011 638 3234 (w), 083 300 2819 (m) or 33251029@mylife.unisa.ac.za.
The study leader, Dr Eric Nenzhelele can be contacted during office hours at 012 429 3756, Nenzhte@unisa.ac.za.

Should you have any questions regarding the ethical aspects of the study, you can contact the chairperson of the Ethics Research Committee, Professor Sharon Rudansky-Kloppers, (012) 429 4370 or rudans@unisa.ac.za.

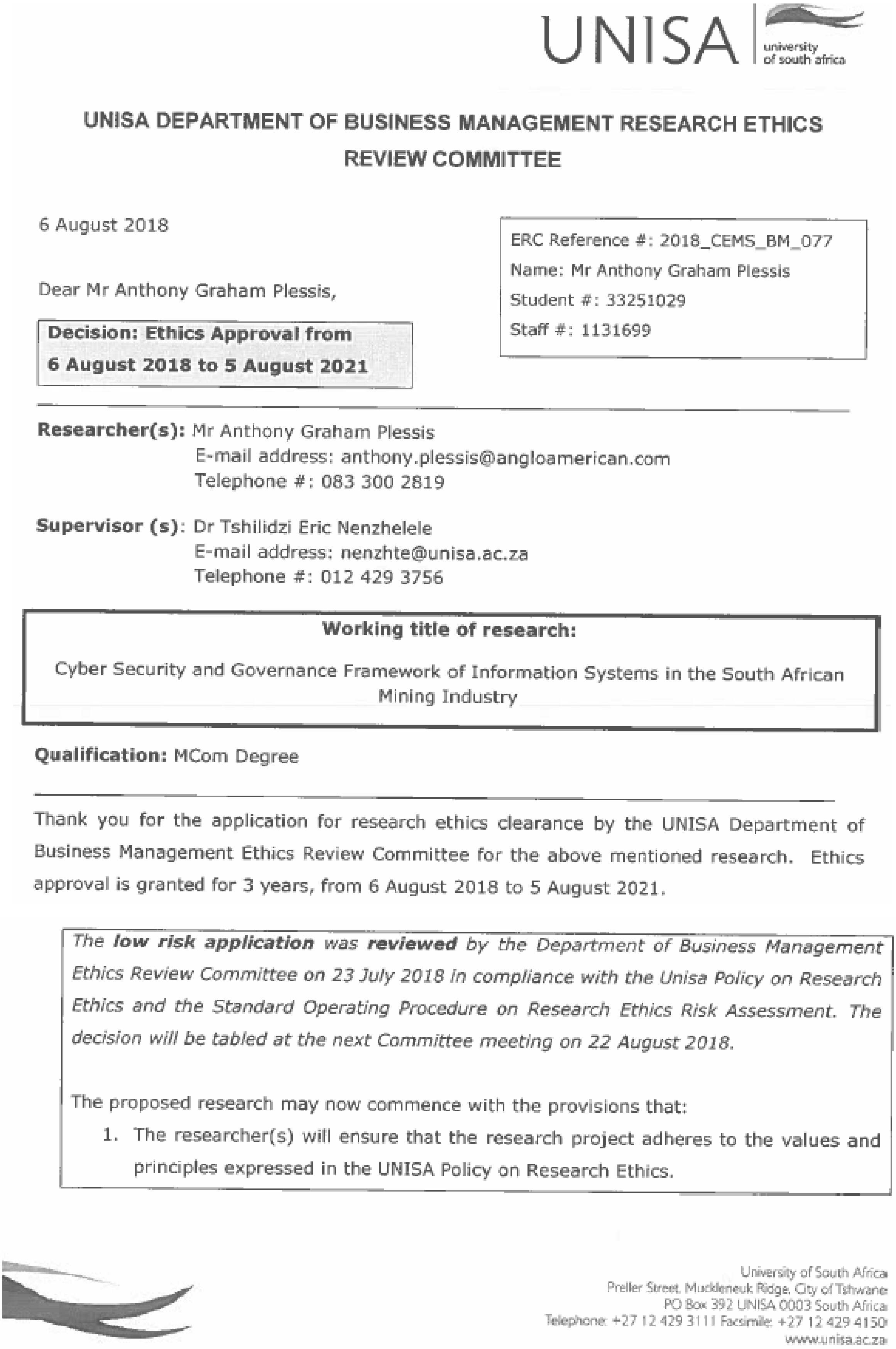
Alternatively, you can report any serious unethical behaviour at the University's Toll-Free Hotline 0800 86 96 93.

You are making a decision whether or not to participate by continuing to the next page. You are free to withdraw from the study at any time prior to clicking the send button.

Thank you for taking time to read this information sheet and for participating in this study.

Anthony Graham Plessis

APPENDIX E: ETHICAL CLEARANCE CERTIFICATE



UNISA university of south africa

UNISA DEPARTMENT OF BUSINESS MANAGEMENT RESEARCH ETHICS REVIEW COMMITTEE

6 August 2018

ERC Reference #: 2018_CEMS_BM_077
Name: Mr Anthony Graham Plessis
Student #: 33251029
Staff #: 1131699

Dear Mr Anthony Graham Plessis,

Decision: Ethics Approval from 6 August 2018 to 5 August 2021

Researcher(s): Mr Anthony Graham Plessis
E-mail address: anthony.plessis@angloamerican.com
Telephone #: 083 300 2819

Supervisor (s): Dr Tshilidzi Eric Nenzhelele
E-mail address: nenzhte@unisa.ac.za
Telephone #: 012 429 3756

Working title of research:

Cyber Security and Governance Framework of Information Systems in the South African Mining Industry

Qualification: MCom Degree

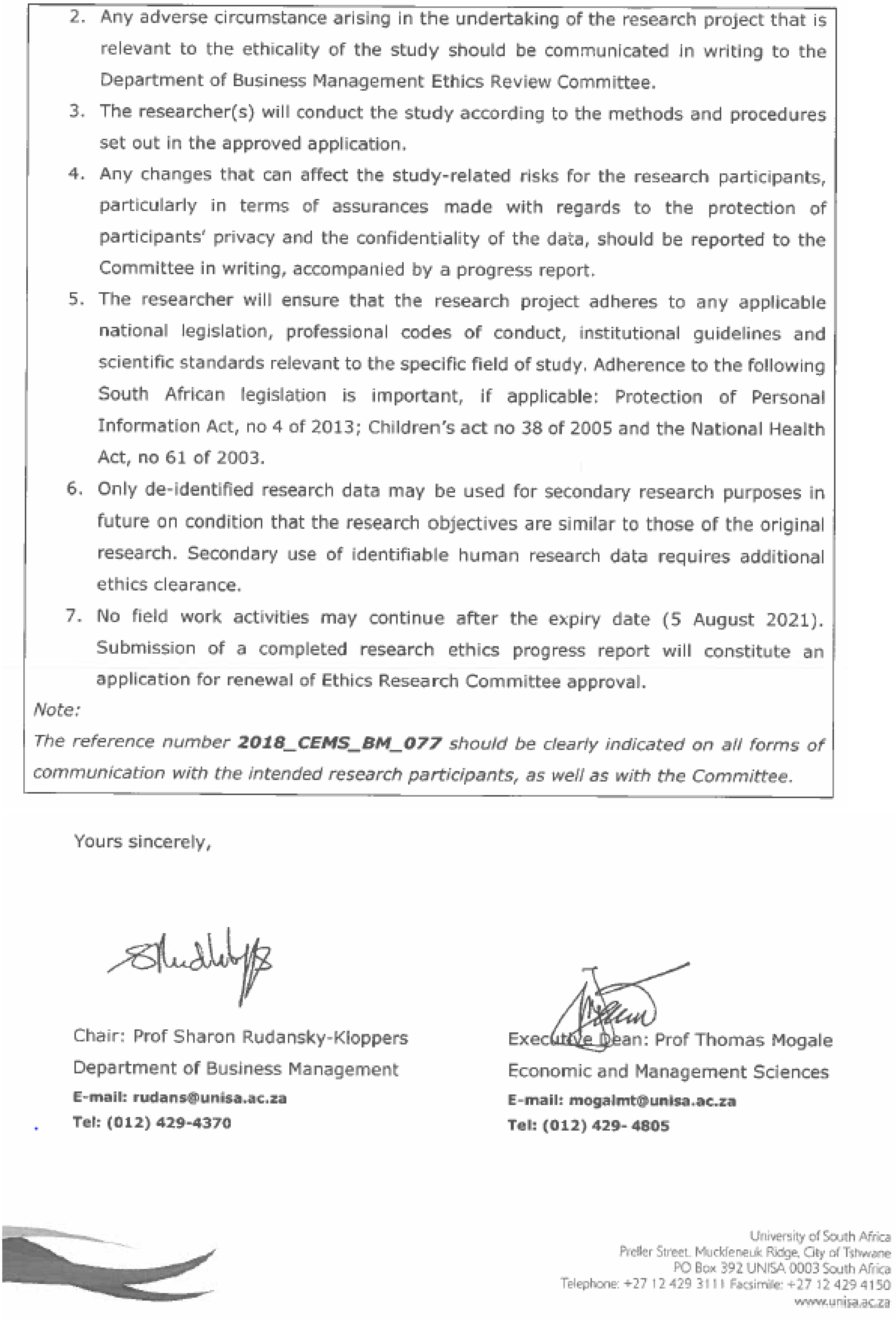
Thank you for the application for research ethics clearance by the UNISA Department of Business Management Ethics Review Committee for the above mentioned research. Ethics approval is granted for 3 years, from 6 August 2018 to 5 August 2021.

*The **low risk application** was **reviewed** by the Department of Business Management Ethics Review Committee on 23 July 2018 in compliance with the Unisa Policy on Research Ethics and the Standard Operating Procedure on Research Ethics Risk Assessment. The decision will be tabled at the next Committee meeting on 22 August 2018.*

The proposed research may now commence with the provisions that:

1. The researcher(s) will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za



2. Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study should be communicated in writing to the Department of Business Management Ethics Review Committee.
3. The researcher(s) will conduct the study according to the methods and procedures set out in the approved application.
4. Any changes that can affect the study-related risks for the research participants, particularly in terms of assurances made with regards to the protection of participants' privacy and the confidentiality of the data, should be reported to the Committee in writing, accompanied by a progress report.
5. The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the specific field of study. Adherence to the following South African legislation is important, if applicable: Protection of Personal Information Act, no 4 of 2013; Children's act no 38 of 2005 and the National Health Act, no 61 of 2003.
6. Only de-identified research data may be used for secondary research purposes in future on condition that the research objectives are similar to those of the original research. Secondary use of identifiable human research data requires additional ethics clearance.
7. No field work activities may continue after the expiry date (5 August 2021). Submission of a completed research ethics progress report will constitute an application for renewal of Ethics Research Committee approval.

Note:

*The reference number **2018_CEMS_BM_077** should be clearly indicated on all forms of communication with the intended research participants, as well as with the Committee.*

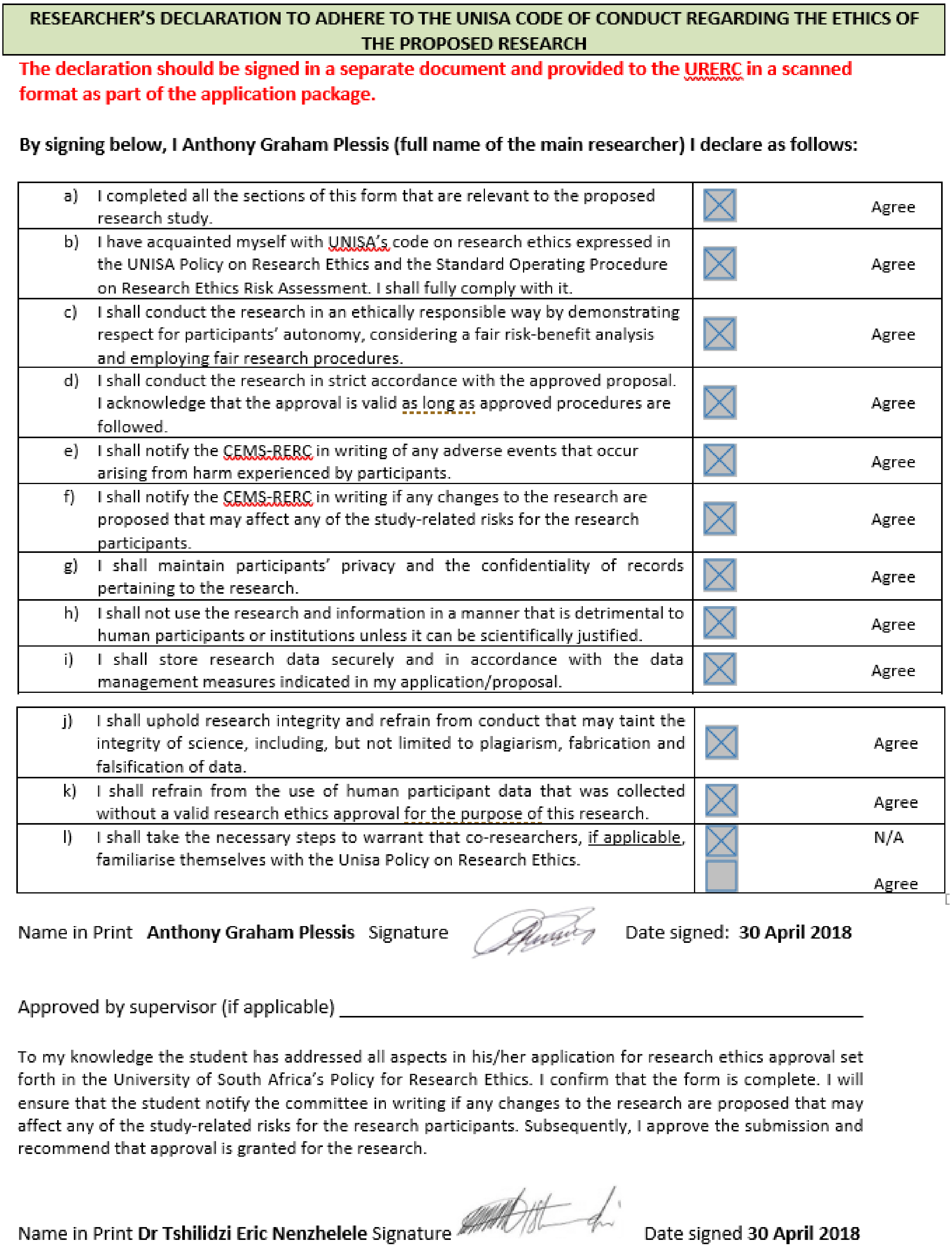
Yours sincerely,

Chair: Prof Sharon Rudansky-Kloppers
Department of Business Management
E-mail: rudans@unisa.ac.za
Tel: (012) 429-4370

Executive Dean: Prof Thomas Mogale
Economic and Management Sciences
E-mail: mogalmt@unisa.ac.za
Tel: (012) 429- 4805

APPENDIX F: ETHICAL CLEARANCE

RESEARCHERS' DECLARATION



RESEARCHER'S DECLARATION TO ADHERE TO THE UNISA CODE OF CONDUCT REGARDING THE ETHICS OF THE PROPOSED RESEARCH

The declaration should be signed in a separate document and provided to the URERC in a scanned format as part of the application package.

By signing below, I Anthony Graham Plessis (full name of the main researcher) I declare as follows:

a)	I completed all the sections of this form that are relevant to the proposed research study.	☒	Agree
b)	I have acquainted myself with UNISA's code on research ethics expressed in the UNISA Policy on Research Ethics and the Standard Operating Procedure on Research Ethics Risk Assessment. I shall fully comply with it.	☒	Agree
c)	I shall conduct the research in an ethically responsible way by demonstrating respect for participants' autonomy, considering a fair risk-benefit analysis and employing fair research procedures.	☒	Agree
d)	I shall conduct the research in strict accordance with the approved proposal. I acknowledge that the approval is valid as long as approved procedures are followed.	☒	Agree
e)	I shall notify the CEMS-RERC in writing of any adverse events that occur arising from harm experienced by participants.	☒	Agree
f)	I shall notify the CEMS-RERC in writing if any changes to the research are proposed that may affect any of the study-related risks for the research participants.	☒	Agree
g)	I shall maintain participants' privacy and the confidentiality of records pertaining to the research.	☒	Agree
h)	I shall not use the research and information in a manner that is detrimental to human participants or institutions unless it can be scientifically justified.	☒	Agree
i)	I shall store research data securely and in accordance with the data management measures indicated in my application/proposal.	☒	Agree
j)	I shall uphold research integrity and refrain from conduct that may taint the integrity of science, including, but not limited to plagiarism, fabrication and falsification of data.	☒	Agree
k)	I shall refrain from the use of human participant data that was collected without a valid research ethics approval for the purpose of this research.	☒	Agree
l)	I shall take the necessary steps to warrant that co-researchers, if applicable, familiarise themselves with the Unisa Policy on Research Ethics.	☒ □	N/A Agree

Name in Print **Anthony Graham Plessis** Signature Date signed: **30 April 2018**

Approved by supervisor (if applicable) ________________________________

To my knowledge the student has addressed all aspects in his/her application for research ethics approval set forth in the University of South Africa's Policy for Research Ethics. I confirm that the form is complete. I will ensure that the student notify the committee in writing if any changes to the research are proposed that may affect any of the study-related risks for the research participants. Subsequently, I approve the submission and recommend that approval is granted for the research.

Name in Print **Dr Tshilidzi Eric Nenzhelele** Signature Date signed **30 April 2018**

APPENDIX G: INFORMED CONSENT

PARTICIPATION INFORMATION SHEET

UNISA university of south africa

CONSENT TO PARTICIPATE IN THIS STUDY

I, __________________ (participant name), confirm that the person asking my consent to take part in this research has told me about the nature, procedure, potential benefits and anticipated inconvenience of participation.

I have read (or had explained to me) and understood the study as explained in the information sheet.

I have had sufficient opportunity to ask questions and am prepared to participate in the study.

I understand that my participation is voluntary and that I am free to withdraw at any time without penalty (if applicable).

I am aware that the findings of this study will be anonymously processed into a research report, journal publications and/or conference proceedings.

I agree to the recording of the web based survey via Survey Monkey.

Participant name & surname………………………………………….. (please print)

Participant signature…………………………………………….Date…………………

Researcher's name & surname **Anthony Graham Plessis** (please print)

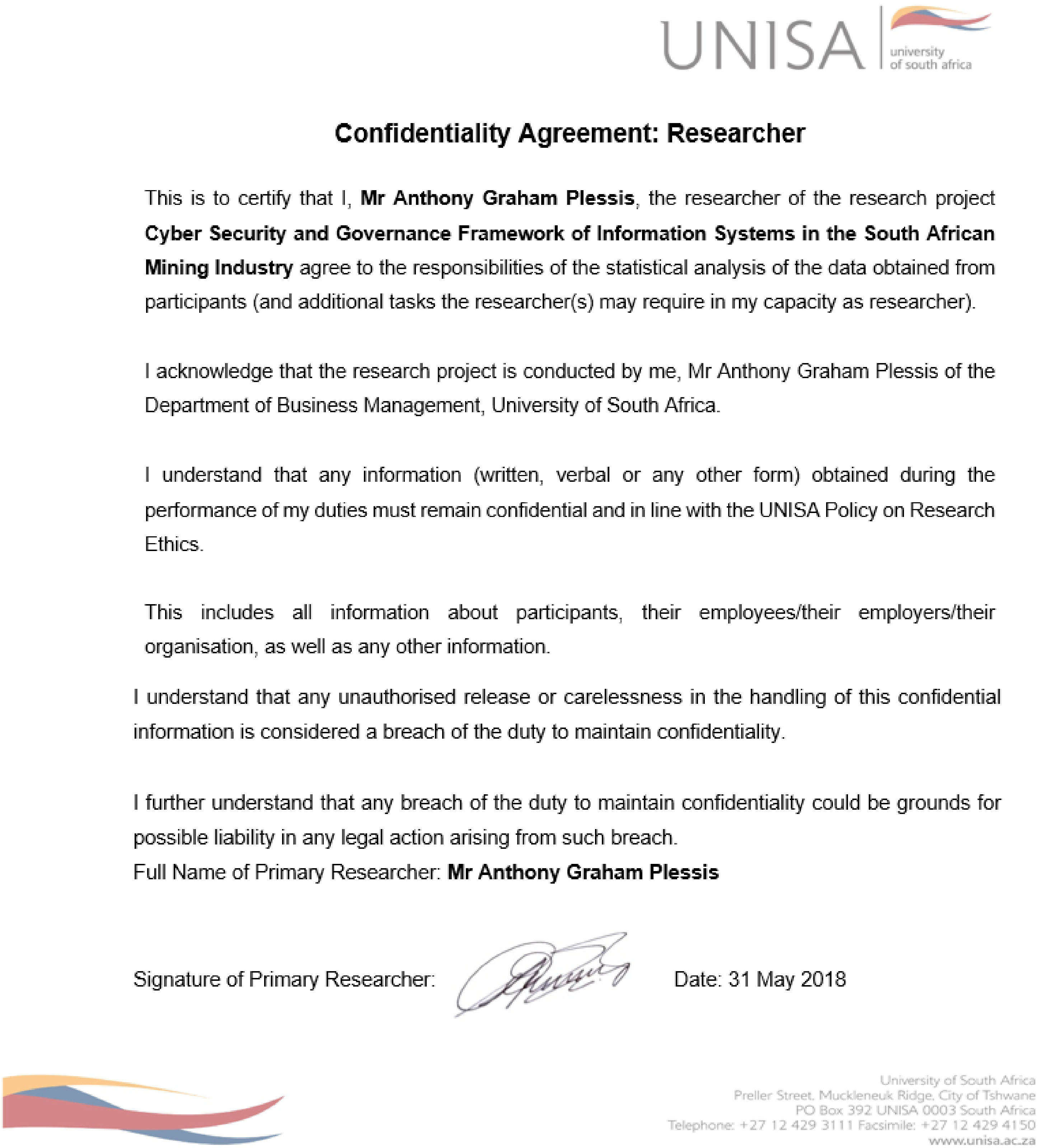
Researcher's signature Date 31 January 2018

Witness name & surname...(please print)

Witness's signature……………………………………….................Date…......................

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

APPENDIX H: CONFIDENTIALITY AGREEMENT



UNISA university of south africa

Confidentiality Agreement: Researcher

This is to certify that I, **Mr Anthony Graham Plessis**, the researcher of the research project **Cyber Security and Governance Framework of Information Systems in the South African Mining Industry** agree to the responsibilities of the statistical analysis of the data obtained from participants (and additional tasks the researcher(s) may require in my capacity as researcher).

I acknowledge that the research project is conducted by me, Mr Anthony Graham Plessis of the Department of Business Management, University of South Africa.

I understand that any information (written, verbal or any other form) obtained during the performance of my duties must remain confidential and in line with the UNISA Policy on Research Ethics.

This includes all information about participants, their employees/their employers/their organisation, as well as any other information.

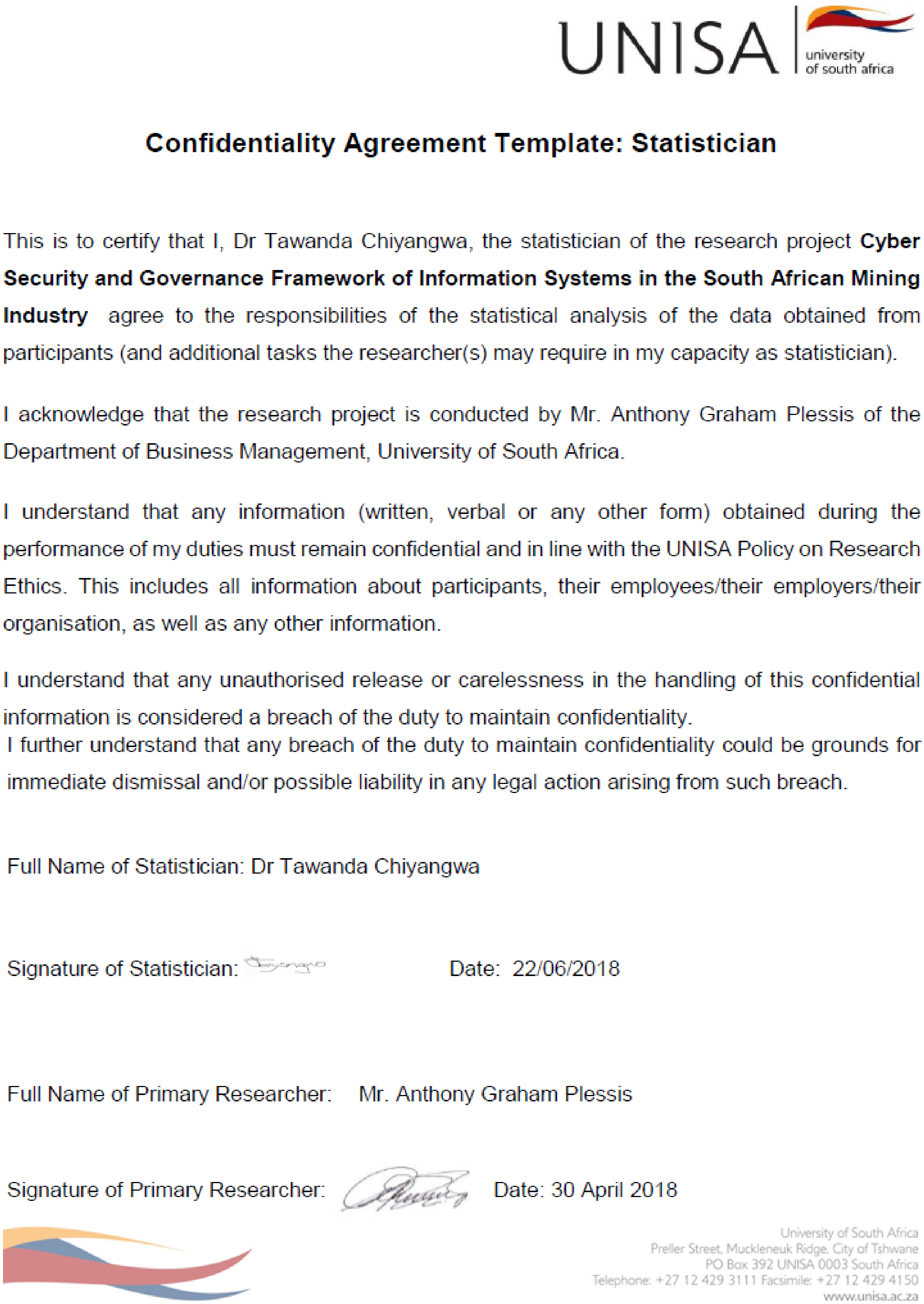
I understand that any unauthorised release or carelessness in the handling of this confidential information is considered a breach of the duty to maintain confidentiality.

I further understand that any breach of the duty to maintain confidentiality could be grounds for possible liability in any legal action arising from such breach.
Full Name of Primary Researcher: **Mr Anthony Graham Plessis**

Signature of Primary Researcher: Date: 31 May 2018

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

APPENDIX I: STATISTICIAN CONFIDENTIALITY AGREEMENT



UNISA university of south africa

Confidentiality Agreement Template: Statistician

This is to certify that I, Dr Tawanda Chiyangwa, the statistician of the research project **Cyber Security and Governance Framework of Information Systems in the South African Mining Industry** agree to the responsibilities of the statistical analysis of the data obtained from participants (and additional tasks the researcher(s) may require in my capacity as statistician).

I acknowledge that the research project is conducted by Mr. Anthony Graham Plessis of the Department of Business Management, University of South Africa.

I understand that any information (written, verbal or any other form) obtained during the performance of my duties must remain confidential and in line with the UNISA Policy on Research Ethics. This includes all information about participants, their employees/their employers/their organisation, as well as any other information.

I understand that any unauthorised release or carelessness in the handling of this confidential information is considered a breach of the duty to maintain confidentiality.

I further understand that any breach of the duty to maintain confidentiality could be grounds for immediate dismissal and/or possible liability in any legal action arising from such breach.

Full Name of Statistician: Dr Tawanda Chiyangwa

Signature of Statistician: Date: 22/06/2018

Full Name of Primary Researcher: Mr. Anthony Graham Plessis

Signature of Primary Researcher: Date: 30 April 2018

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

APPENDIX J: EIGEN VALUES

EXTRACTION FACTORS AND ROTATED FACTORS

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3.017	20.113	20.113	3.017	20.113	20.113	2.509	16.729	16.729
2	2.282	15.212	35.325	2.282	15.212	35.325	2.156	14.372	31.101
3	2.051	13.676	49.002	2.051	13.676	49.002	2.038	13.586	44.688
4	1.670	11.134	60.136	1.670	11.134	60.136	1.728	11.520	56.207
5	1.182	7.882	68.018	1.182	7.882	68.018	1.401	9.341	65.548
6	1.014	6.763	74.781	1.014	6.763	74.781	1.385	9.233	74.781
7	0.851	5.674	80.455						
8	0.814	5.429	85.884						
9	0.519	3.458	89.342						
10	0.486	3.241	92.583						
11	0.352	2.348	94.931						
12	0.281	1.874	96.805						
13	0.246	1.641	98.447						
14	0.170	1.133	99.580						
15	0.063	0.420	100.000						

Extraction Method: Principal Component Analysis.

Table 5.13 Total Variance explained, initial eigenvalues, extraction factors and rotated factors

APPENDIX K: ROTATED COMPONENT MATRIX

ITEM LOADING PER FACTOR

Rotated Component Matrix[a]

	Component					
	1	2	3	4	5	6
Q7				-0.693		
Q13		0.746				
Q14		0.874				
Q15	0.859					
Q16	0.871					
Q17	0.607					
Q18		0.622				
Q24				0.543		
Q25			0.821			
Q26				0.712		
Q29			0.734			
Q32					0.491	
Q40					-0.837	
Q41						0.905
Q42			0.743		0.419	

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in 14 iterations.

APPENDIX L: ITEM TOTAL STATISTICS

ITEM LOADING PER FACTOR

Item-Total Statistics				
	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Q7	24.71	28.946	0.122	0.606
Q13	25.13	27.316	0.314	0.567
Q14	24.77	27.714	0.199	0.592
Q15	25.71	28.880	0.534	0.563
Q16	25.29	26.880	0.382	0.555
Q17	25.65	28.237	0.406	0.562
Q18	24.94	26.329	0.333	0.561
Q24	25.84	30.006	0.195	0.589
Q25	25.32	30.692	0.061	0.607
Q26	24.29	29.346	0.065	0.621
Q29	24.77	24.981	0.497	0.526
Q32	25.52	28.258	0.217	0.586
Q41	24.23	29.914	0.026	0.629
Q42	25.26	28.598	0.432	0.563

APPENDIX M: DESCRIPTIVE STATISTICS

Item statistics			
	Mean	Std. Deviation	N
Q7	2.32	1.17	37
Q13	1.90	1.04	37
Q14	2.26	1.24	37
Q15	1.32	0.48	37
Q16	1.74	1.00	37
Q17	1.39	0.72	37
Q18	2.10	1.19	37
Q24	1.19	0.65	37
Q25	1.71	0.78	37
Q26	2.74	1.26	37
Q29	2.26	1.12	37
Q32	1.52	1.06	37
Q40	2.81	1.25	37
Q42	1.77	0.62	37

Table 5.2 ICT Governance practices