UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

# ASSESSING CYBER RESILIENCE OF PUBLIC SECTOR INFORMATION SYSTEMS: A SOUTH AFRICAN PERSPECTIVE

by

**Thenjiwe Glyndah Sithole**
**15267203**

Submitted in fulfilment of the requirements for the degree
**Master of Information Technology**
**in Information Systems**

in the

**FACULTY OF ENGINEERING, BUILT ENVIRONMENT AND INFORMATION TECHNOLOGY**

at the

**UNIVERSITY OF PRETORIA**

**Supervisor:** Dr NJ Croft

June 2019

# Abstract

The rapid increase of emerging technologies has become a backbone upon which organisations now increasingly rely on. It has prompted public sector organisations around the globe to embrace these technologies and digitise their information systems. To capitalise on these global technological advancements, public sector organisations in South Africa have been investing in electronic government (e-government) services to perform effectively, accelerate and improve efficiency in service delivery, promote transparency and accountability, and bolster information sharing and collaboration between government organisations. The e-government interaction includes governments, businesses, and citizens.

However, these technological advancements and digital transformation come with unintended ramifications and at a high cost - such as unprecedented cyber risks that can cause disruptions to critical systems, networks, and data. The far-reaching impact of these cyber risks could include financial loss, damage to information assets, failure of Information and Communications Technology systems, reputational damage, violation of privacy due to data breaches. Therefore, public sector organisations need to ensure the protection of the confidentiality, integrity, and availability of their critical information systems.

This research study sets out to assess the cyber resilience of the South African public sector organisations information systems, that is, the capability to anticipate, withstand, detect, respond to, recover from, and adapt to any disastrous cyber incidents with an ability to resume services at an acceptable level and time.

To achieve the objective, a qualitative method and interpretive approach to collect and analyse data was adopted. Empirical data was collected from the South African public sector organisations in the Gauteng Province through semi-structured, face-to-face interviews as a primary source and utilising a survey raw dataset as the secondary source. Furthermore, data triangulation was used to strengthen and validate the thematic findings. This was accomplished by comparing the thematic finding from the primary source with the statistical results from the secondary source.

Findings for this research study revealed that the South African public sector organisations are more vulnerable to cyber risks due to lack of basic cybersecurity controls requirements namely: a cybersecurity strategy, an adequate skilled workforce, an effective incident response plan, a cyber risk management strategy, a cybersecurity awareness programme as well as clearly defined cybersecurity roles and responsibilities for the executive management and senior management. Consequently, the impact of cyber-attacks on the South African public sector organisations can be potentially damaging and, in some instances, even catastrophic.

South African public sector organisations surveyed in the study were found not to have the capacity and capability to anticipate, withstand, detect, respond to, recover from, and adapt to any disastrous cyber incidents and be able to resume services at an acceptable level and time.

The South African public sector organisations need to implement the basic cybersecurity controls as the first step towards cyber resilient information systems. The South African public sector organisations need to be more pro-active; develop a cybersecurity strategy and a comprehensive cyber incident response plan; allocate sufficient budget for cybersecurity technologies, education, training, and development; and implement continuing compulsory cybersecurity awareness programmes.

**Keywords:** cyber resilience, public sector, information systems, cyber risks, cyber threats, cyber-attacks, cybersecurity and information security frameworks and standards.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

# Declaration Regarding Plagiarism

| | |
|---|---|
| I (full names & surname): | Thenjiwe Glyndah Sithole |
| Student number: | 15267203 |
| Degree/Qualification | Master of Information Technology (Information Systems) |

**Declare the following:**

1. I understand what plagiarism entails and am aware of the University's policy in this regard.

2. I declare that this dissertation is my own, original work. Where someone else's work was used (whether from a printed source, the Internet, or any other source) due acknowledgement was given and reference was made according to departmental requirements.

3. I did not copy and paste any information directly from an electronic source (e.g., a web page, electronic journal article or CD ROM) into this document.

4. I did not make use of another student's previous work and submitted it as my own.

5. I did not allow and will not allow anyone to copy my work with the intention of presenting it as his/her own work.

Signature

Date

## Acknowledgements

First, I would like to give thanks with a grateful heart to the Almighty God for giving me the strength and ability to complete this dissertation. My journey was not easy, but My God has always been there to carry me through.

I am grateful with a humble heart to my two wonderful and loving sons, Ayabonga and Siyabonga, for their unconditional support, understanding and patience throughout my research study.

I thank my mom and my two sisters for their support and words of encouragements.
My sincere gratitude to all the participants for their willingness to participate.
Last but not least, I thank my supervisor Dr Neil Croft for his support, guidance, and encouragement.

## Dedication

I dedicate this dissertation to my two wonderful sons,

**Ayabonga and Siyabonga**

# Terms and Abbreviations

| | |
|---|---|
| BRICS: | Brazil, Russia, India, China, and South Africa |
| CIA: | Confidentiality, Integrity and Availability |
| CIO: | Chief Information Officer |
| CISO: | Chief Information Security Officer |
| COBIT: | Control Objectives for Information and Related Technologies |
| CRO: | Chief Risk Officer |
| CRR: | Cyber Resilience Review |
| CSIR: | Council for Scientific and Industrial Research |
| CSIRT: | Computer Security Incident Response Team |
| DDOS: | Distributed Denial of Service |
| DHA: | Department of Home Affairs |
| DLP: | Data Loss Prevention |
| DoJ&CD: | Department of Justice and Constitutional Development |
| DoT: | Department of Transport |
| e-government: | Electronic Government Services |
| ICT: | Information and Communication Technology |
| IDS: | Intrusion Detection System |
| IPS: | Intrusion Prevention System |
| IRP: | Incident Response Plan |
| ISF: | Information Security Forum |
| ISMS: | Information Security Management System |
| ISO/IEC: | International Organisations for Standardisation / International Electrotechnical Commission |
| ISS: | Information Systems Security |
| ITU: | International Telecommunication Union |
| MISS: | Minimum of Information Security Standards |
| MOU: | Memorandum of Understanding |
| NCPF: | National Cybersecurity Policy Framework |
| NIST: | National Institute of Standards and Technology |
| PSOs: | Public Sector Organisations |

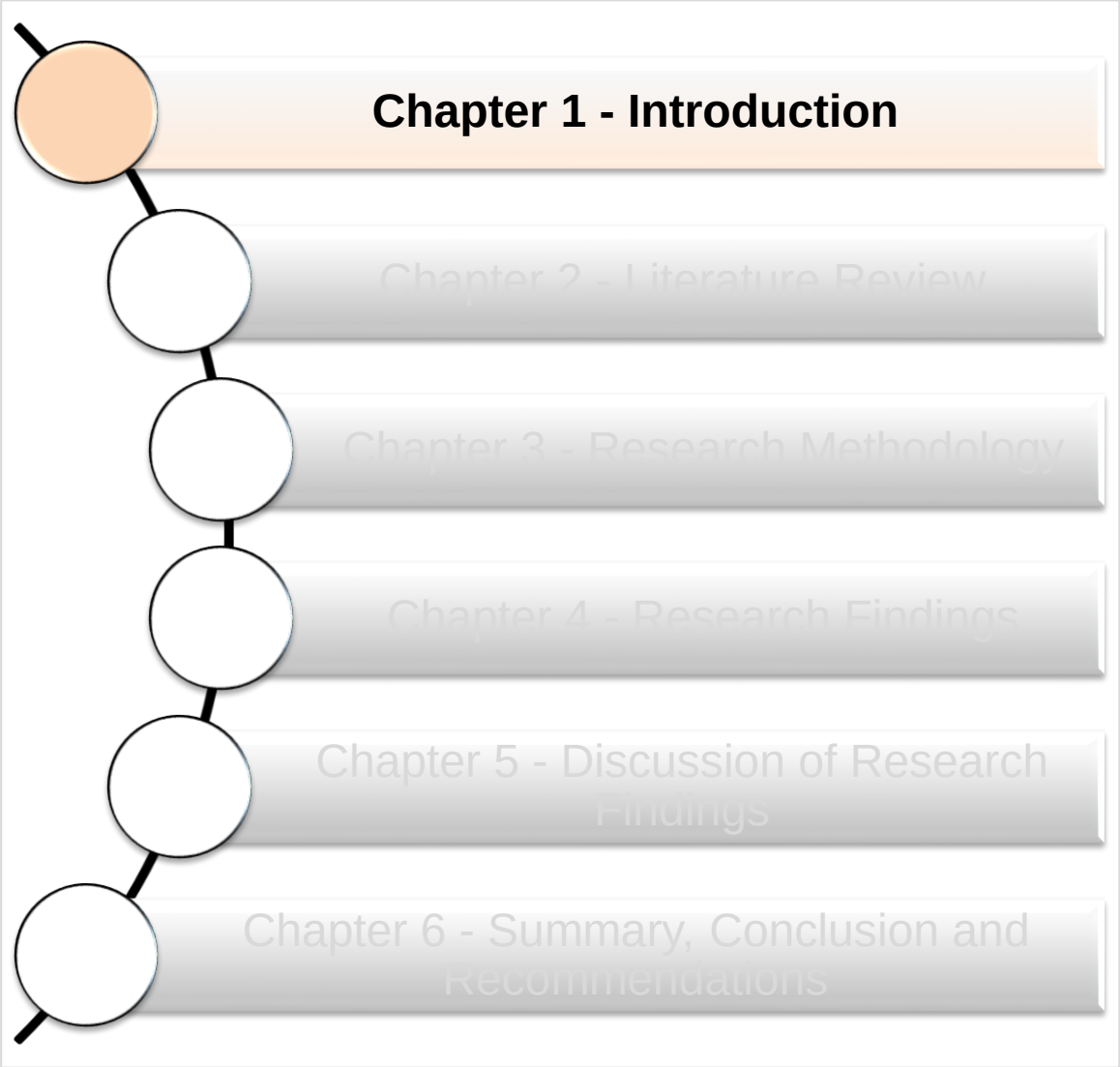
| | |
|---|---|
| PT: | Penetration Testing |
| SAPSOs: | South African Public Sector Organisations |
| VA: | Vulnerability Assessment |
| VAPT: | Vulnerability Assessment and Penetration Testing |
| VPN: | Virtual Private Network |

# Table of Contents

# List of Tables

# List of Figures

# 1. CHAPTER 1 – INTRODUCTION



## 1.1 Background Information

Public sector organisations () are increasingly dependent on rapidly evolving information systems. An information system is one of the organisation's most critical functions. This is so because information systems play an important role in the success of an organisation's business processes, its ability to deliver on its mandate and its managerial decision-making. For PSOs to achieve their strategic objectives and stay relevant, they need to have information systems that are technologically driven. This implies that PSOs' Information and Communication Technology (ICT) infrastructures need to be efficient, accelerate productivity, increase the organisational speed of response and reduce costs.

ICT is a powerful source for driving economic growth and societal development. In this regard, the rapidly-evolving ICTs have compelled PSOs around the globe to transform their traditional ways of doing business and redesign their business processes, business networks and business scope (Ward & Peppard, 2002). Consequently, PSOs are capitalising on the unprecedented opportunities brought about by the latest technologies to launch digital services, which are also known as electronic government services (e-government) and mobile services (m-services). According to an e-government survey done by the United Nations (UN), global trends in e-government advancements have been rapidly developing since 2001 (UN, 2018).

The global technological advancement has influenced the public sector in South Africa to invest in e-government services to accelerate and improve service delivery, promote transparency and accountability, and bolster information sharing and collaboration between government organisations (DTPS, 2017a). The South African government utilises e-services such as tax return e-filing of the South African Revenue Service (SARS) and the integrated electronic National Traffic Administration Information Systems (eNaTIS) utilised by the Department of Transport (DoT).

Smart Cities are becoming a critical necessity with some South African local governments such as Johannesburg and Cape Town aspiring to be Smart Cities (Musakwa & Mokoena, 2017). This aspiration is driven by the need to interconnect different customer services systems such as city development; corporate and legal; energy; infrastructure services;

health and social services; and water and sanitation, for monitoring, control, and automation (Mzekandaba, 2018; Software AG, 2014).

However, this technological advancement comes at a high cost in the form of heightened cyber risks flowing from information systems' increasing use of the internet or cyberspace. Organisations are becoming exposed to various types of cyber risks and information systems are becoming vulnerable to various and constantly-evolving cyber threats and cyber-attacks which could potentially cause enormous damages (Feng & Li, 2011; Mouna, Rabai, & Aissa, 2014). Cyber risks and their capacity to disrupt information systems are increasing at an unprecedented speed. In its 2018 Global Risks Report, the World Economic Forum ranked two cyber risks among the top five (5) global risks, namely: cyber-attacks (3rd position) and data fraud or theft (4th position) (WEF, 2018).

South Africa is of course not immune to these cyber risks. On the contrary, some cybersecurity survey reports rank South Africa in the 20 top countries most vulnerable to cyber risks. The following serve as some examples:

- The 2016 National Exposure Index ranked South Africa as the 9th most vulnerable country to cyber-attacks (Rapid7, 2016). The company subsequently ranked South Africa as the 16th most vulnerable country to cyber-attacks for 2018 National Exposure Index, reflecting a seven position improvement compared to 2016 (Rapid7, 2018).

- The 2017 Cyber Exposure Index rated South Africa as the 3rd most exposed country to cyber risk (Kinkayo, 2017).

- In a research study conducted by Ponemon Institute, South Africa is reported to have an astounding 43% likelihood of experiencing a major data breach at within the next two years (Ponemon Institute LLC, 2018) compared to the global probability of 27%.

Considering the above, it should be noted that PSOs store a lot of data and often use legacy systems which are vulnerable to sophisticated cyber threats and attacks. Therefore, the consequences of a data breach could be immense. As PSOs are increasingly utilising

technology and cyberspace to improve business processes and accelerate service delivery, they equally become more exposed and potentially vulnerable to cyber-attacks. Examples of recent cyber incidents impacting South African PSOs (SAPSOs) include the following:

- In 2017, an Islamic hacktivist group defaced the websites of the Buffalo City Municipality and Eastern Cape Education Department (Grove, 2018);

- During June 2017, the Department of Basic Education website was defaced by "Team System DZ" posting gruesome pictures along with a message to the government, American people and the rest of the world (IOL, 2017);

- The Master Deeds Office discovered in October 2017 that it had a data breach of sensitive personally identifiable information of more than 60 million individuals (Niselow, 2018);

- In 2018, the websites of the Presidency, the Department of Environmental Affairs, the Department of Home Affairs and the Cybersecurity Hub were shut down by a hacker group, "Black Team" (Breakfast, 2018; Pijoos & Grobler, 2018);

- ViewFine, a contractor for some municipalities' traffic departments in May 2018 discovered a data breach of personal records of more than 934 000 South Africans (Mohapi, 2018); and

- In September 2018, the Department of Labour indicated that they have experienced an unsuccessful Distributed Denial of Service (DDoS) attack on one of its external facing servers (Lloyd, 2018).

Vulnerabilities in SAPSOs may, among others, also be associated with the procurement of international ICT software and equipment through prescribed supply chain processes. Unverified and untested ICT software and/or equipment could have flaws, vulnerabilities and even 'backdoors' (either through improper secure design or purposefully), rendering these organisations more vulnerable to cyber threats and cyber-attacks. For instance, in 2004,

Cisco made a proposal for “lawful intercept” backdoor for routers that can be used by law enforcement agencies to log in to routers remotely. More backdoors were then discovered years later including five new backdoors within a period of five months in 2018 (Armasu, 2018). Investigation and time will eventually reveal, especially after Cisco’s proposal in 2004, whether these ‘backdoors’ were intentionally designed and incorporated within their products or whether it was just an error.

While the level of cyber risk is rapidly escalating, the South African government has realised that there are no physical boundaries in cyberspace and that SA, just as it is the case with all other countries, is susceptible to cybersecurity threats and cyber-attacks. Consequently, in March 2012 (as published in the Government Gazette in December 2015), the Cabinet approved a National Cybersecurity Policy Framework (NCPF) to address cybersecurity threats and securing cyberspace and cyber infrastructures. The NCPF is aimed at combating cyber warfare, cybercrime, cyber terrorism, and cyber espionage as well as at building confidence and trust in the secure use of ICT infrastructure. However, and is as far as could be surmised from the public discourse, the process of finalising the implementation of the NCPF, the development of a National Cybersecurity Strategy and an Implementation Plan are not gaining momentum – despite an exponential increase in cyber threats and cyber-attacks.

The South African Government has a critical responsibility in building a cyber resilient country as well as assisting organisations and the nation to be cyber resilient. In this regard, securing organisational information systems should not be dependent on the structures responsible for cybersecurity as articulated in the NCPF. The need to understand that there is no silver bullet for cybersecurity and every single organisation is responsible for its own cybersecurity. They need to be pro-active and consider an integrated approach to manage escalating and sophisticated cyber risks. Investing in traditional cybersecurity solutions alone is no longer enough. The effective mitigating of cyber risks requires a cyber risk management-based approach which asserts and progresses cyber resilience (WEF, 2017).

An organisation’s cyber resilience is critical because it pertains to an organisation’s preparedness for cyber incidents and distributes to everyone the organisational

responsibility for managing cyber risks and protect critical systems, network as well as data. Further to this, cyber resilience denotes that critical information systems can withstand cyber incidents and are able to respond and recover at an acceptable level (Björck, et al., 2015). For organisations to achieve an organisation-wide cyber resilience posture, they need to have a defence-in-depth approach. The reason for such an approach is that it is challenging to address all cyber risks to an organisation with just a traditional cybersecurity approach (Jaquire & von Solms, 2017). The resilience of information systems (IS) must be fundamental for any organisation for its successful recovery to resume operations as quickly as possible.

Cyber resilience relies comprehensively on identifying the organisation's critical assets (data, systems and networks); identifying cyber risks (identifying vulnerabilities, threats and understanding the possible impacts of cyber-attacks); cyber threat actors that the organisation might face; sound cyber governance; effective cybersecurity awareness, training and education programmes; adequate resources (budget, skilled workforce, technologies, policies, procedures, strategies and so on); data protection; considering cyber resilience of third-parties; effective partnerships and collaborations within and outside the organisation; and an adequate and effective cyber incident response plan, which is approved and regularly tested (ASIC, 2015; NIST, 2018).

Organisations also require an effective cybersecurity framework, which can be adopted from one of the cybersecurity standards, frameworks, and good practices such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, ISO/IEC Security Control Standards and COBIT, to name but a few.

## 1.2 Problem Statement

To help address the unintended consequences of cyber threats and cyber-attacks, information systems and infrastructures need to be secured to ensure the confidentiality, integrity and availability of critical systems, data, and networks. The NCPF does not mention the concept of cyber resilience and to date, there is neither a National Cybersecurity Strategy (together with an Implementation Plan) nor a cyber resilience framework in place

to provide a guideline for SAPSOs to implement information systems that are resilient to cyber threats and cyber-attacks. Furthermore, South Africa, like many other developing countries, is perceived as having insufficient capacity and capability to effectively counter these sophisticated cybersecurity threats and cyber-attacks, which are increasingly gaining world attention. In South Africa, there is still a gap in cybersecurity awareness, making more people and organisations vulnerable.

## 1.3 Objective of the Study

The objective of this study is to investigate South African public sector organisations capability to anticipate, withstand, detect, respond to, recover from, and adapt to any disastrous cyber incidents and be able to resume services at an acceptable level. To achieve the objective of the study, it is important to:

- Be acquainted with the cyber risks that the South African public sector organisations are exposed to;

- Appraise current cyber threats to, and the impact of cyber-attacks on, South African public sector organisations information systems; and

- Look into the measures that the South African public sector organisations can take to mitigate cyber risks.

## 1.4 Research Questions

To support the research objective, the following research questions were formulated:

- **Main research question** – How cyber resilient are the information systems of South African public sector organisations?

    - **Sub-question 1** – What are the cyber risks that the South African public sector organisations may face?

- **Sub-question 2** – What are the current cyber threats to, and the impact, of cyber-attacks on, the South African public sector information systems?

- **Sub-question 3** - What are the measures in place for the South African public sector organisations to mitigate cyber risks?

## 1.5 Assumptions

The study assumed that the South African government promotes the use of e-services and m-services to accelerate and improve service delivery and that cybersecurity initiatives are of importance to all SAPSOs since the approval of the NCPF. Therefore,

- All the SAPSOs invited to participate in the research study will grant the researcher permission to conduct the research study;

- all the government institutions responsible for cybersecurity as prescribed by the NCPF will willingly participate; and

- the study will have sufficient data for analysis given the importance of cybersecurity for government institutions.

## 1.6 Limitations

This section describes the factors or circumstances that narrow the scope of the research methodology thus affect the research. SAPSOs are a very large collective which includes about 47 national government departments, more than 200 provincial and local governments as well as more than 100 state-owned enterprises. Therefore, the study's scope was narrowed to SAPSOs located in the Gauteng province as the majority of the SAPSOs are in the Gauteng Province. The survey targeted at least two participants per organisation who are active in any one of the following fields: information technology, information technology security, information security, cybersecurity, and information risk management.

## 1.7 Significance/Benefits of the Study

To the researcher's knowledge, there is insufficient data available regarding the state of cybersecurity readiness of the SAPSOs. Further to that, there is a lack of investigations, publications or published academic research on cyber resilience and (South African) PSOs in general.

This study sought to conduct research to benefit the SAPSOs by identifying cyber risks and establishing a cyber risk management approach, to adopt an approach of building cyber resilient information systems and organisation through developing cyber resilient strategies, following cybersecurity good practices, as well as promoting an organisation-wide cyber resilient culture.

## 1.8 Dissertation Structure

This section gives a brief overview of the chapters of this research study.

**Chapter 1 Introduction**

This chapter provides introductory information about the research study, presents the problem statement and the objectives, and advances the research questions. This is followed by the postulation of assumptions, the limitation of the study, and the significance of the study. Finally, it outlines the chapters of the research study.

**Chapter 2 Literature Review**

**T**his chapter presents the literature in the context of addressing the research topic, problem statement, objective, and research questions. It relates to the following themes: information systems, cyber risks, information systems security, cyber resilience, and the approach towards cyber resilience.

**Chapter 3 Research Methodology**

This chapter discusses the research methodology applied in this study. This chapter also covers the following sections: research design, sampling, data collection, data analysis, triangulation, ethics, and the problems encountered during data collection.

**Chapter 4 Research Findings**

**T**his chapter presents in detail the findings of the data collected through semi-structured, face-to-face interviews as well as raw data from survey research as a secondary source. The findings are presented in six (6) themes.

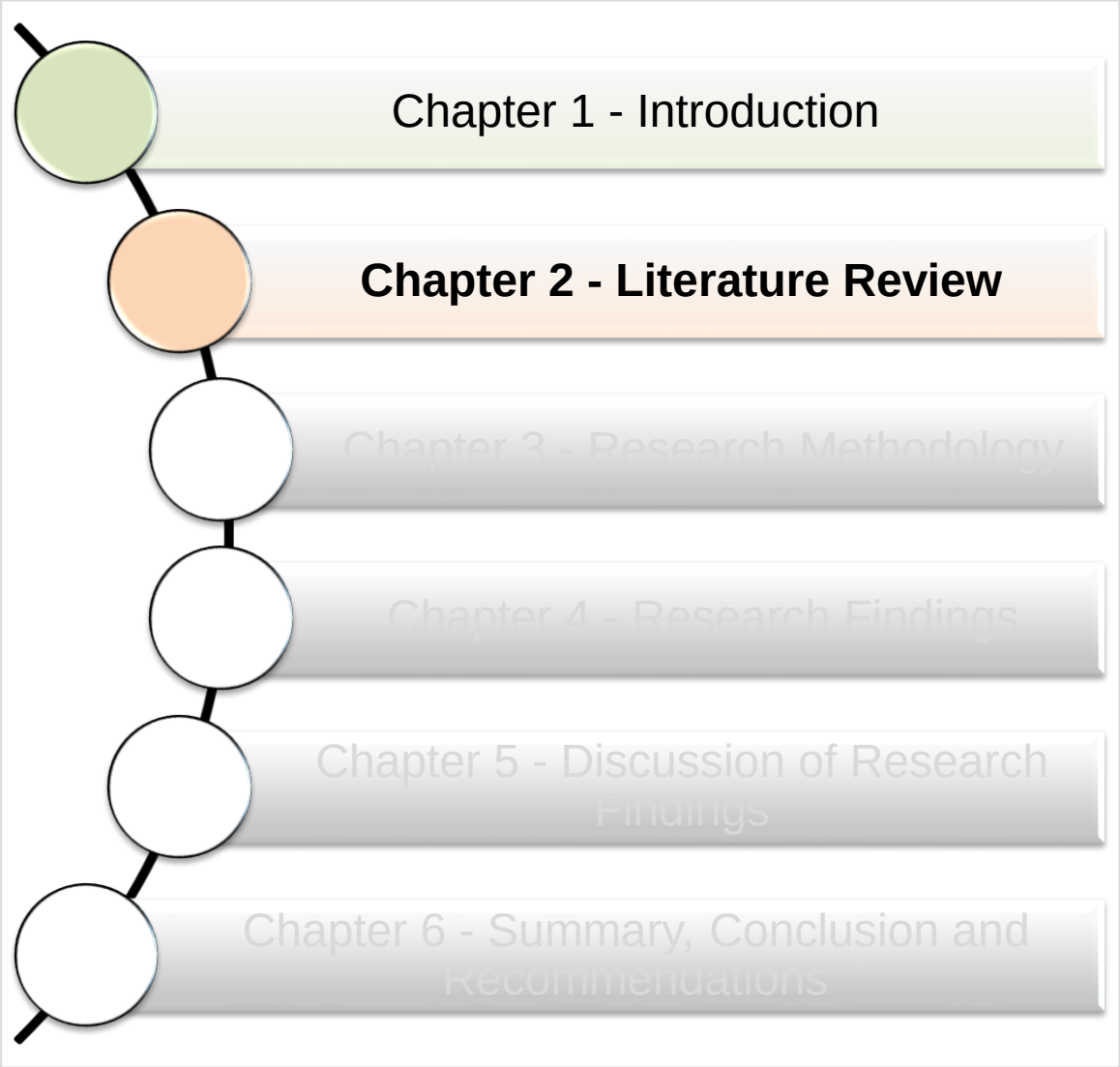
**Chapter 5 Discussion of Research Findings**

**T**his chapter discusses the research findings of the study. The discussions are presented according to the themes as indicated in Chapter 4.

**Chapter 6 Recommendation and Conclusion**

**T**his chapter responds to the research questions, provides recommendations for further research, and presents the conclusion.

# 2. CHAPTER 2 – LITERATURE REVIEW



## 2.1 Introduction

Today's public sector organisations (PSOs) are embracing digital transformation, making use of the internet and advanced technologies for economic growth, rapid service delivery, healthcare systems, and education amongst others. This digital transformation teems with advancing and unprecedented cyber risks that can cause disruption to critical systems, networks, and data. Therefore, organisations must ensure the protection of the confidentiality, integrity, and availability of their critical information systems.

While there is a vast amount of literature relating to cybersecurity, cyber threats and cyber-attacks, there is little published research that addresses, in a South African context: public sector information systems; public sector and information security; public sector and cybersecurity as well as public sector and cyber resilience.

The South African research relates mostly, to list a few, (i) cybersecurity (Mbelli & Dwolatzky, 2016; von Solms, 2015); (ii) cybersecurity awareness and education (Dlamini & Mapule, 2012; Korjan & von Solms, 2014; Phahlamohlaka, Jansen van Vuuren, & Coetzee, 2011); (iii) cybersecurity policy (Burmeister, Phahlamohlaka, & Al-Saggaf, 2014; Dagada & Eloff, 2013; Grobler, Jansen van Vuuren, & Leenen, 2012; Jansen van Vuuren, et al., 2013); (iv) cybersecurity governance (Sutherland, 2017; von Solms, 2016); and (v) cyber resilience and cyber threat intelligence (Dalton, Jansen van Vuuren & Westcott, 2017; Mutemwa, Mtsweni & Mkhonto., 2017; Peter, 2017).

This chapter presents a review of literature related to the research topic. It examines literature that relates to information systems, cyber risks, information systems security, cyber resilience, and frameworks, standards and good practices for information security and cybersecurity.

## 2.2 Information Systems

Information Systems are the methods by which organisations and personnel use ICT infrastructure to collect, process, store, analyse and disseminate data or information to

achieve organisational strategic objectives. The significance of "information systems" concedes to different definitions and its usage has been developing in diverse ways and with complexity over time. The different definitions, which are a decade apart, are as follows:

*"A system which assembles, stores, processes and delivers information relevant to an organisational (or to society) in such a way that the information is accessible and useful to those who wish to use it, including managers, staff, clients and citizens. An information system is a human activity (social) system which may or may not involve computer systems"* (Buckingham, et al., 1987, p. 18 cited by Avison & Myers, 1995).

*"Information systems are the means by which organisations and people, utilising information technologies, gather, process, store, use and disseminate information"* (UKAIS, 1997)

*"An information system can be defined technically as a set of interrelated components working together to collect, process, store and disseminate information to support decision making, coordination, control, analysis and visualisation in an organisation"* (Laudon & Laudon, 2007, p. 15).

Therefore, these definitions show that information systems are about the inseparable relationship between an organisation, technology, and business processes. The six (6) critical components of the information systems are hardware, software, networks, data, people, and procedures. In today's world the organisations, both in private and public sectors have become so reliant on emerging information systems, and the question arises as to what makes information systems so critical? The answer lies in understanding that information systems are so critical because they enable organisations to realise their strategic objectives such as to obtain reliable and valuable information for decision-making, boost performance, gain competitive advantage, improve customer relations, and have service continuity and availability (Lannon, 2013; Laudon & Laudon, 2007).

### 2.2.1 Public sector information systems

The significant benefits brought by the evolving technologically-driven information systems have also allowed the public sector to take advantage of Information and Communication

Technology (ICT) tools and applications to digitise and automate traditional government services. The advantages of using ICT include: to perform effectively, improve efficiency in service delivery, promote better accountability and transparency, empower their citizens (Hendriks, 2012; UNDESA, 2014;), as well as improve information sharing or delivery to all stakeholders. The intention for digitising and automating traditional government services is to offer access to government services anytime and anywhere over the open network (Jin-fu, 2009).

### 2.2.2 Electronic government

West (2004) and UNDESA (2014) refer to digitised and automated services through public sector information systems as electronic government services (e-government). The e-government services make use of wired-internet to gain access to government services through government websites (Trimi & Sheng, 2008). Therefore, e-government is defined as "Government's use of technology, particularly web-based Internet applications, to enhance the access to and delivery of government information and service to citizens, business partners, employees, other agencies and government organisations." (McClure, 2000, p. 3).

Previous surveys reveal that the use of e-government services by citizens, business, employees and government organisations and the provision of e-services by governments is maturing every year (UN, 2018; UNDESA, 2014; West, 2004). There are four distinct bi-directional e-government interactions (DTPS, 2017a):

- **government to business (G2B):** Interaction between government entities and businesses, including non-profit organisations,

- **government to citizens (G2C):** Interaction between government entities and its citizens,

- **government to employees (G2E):** Interaction between government and its employees,

- **government to government (G2G):** Interaction between government entities and within government units.

South Africa is among the top five African countries (Mauritius, Tunisia, South Africa, Morocco, and Seychelles) that have the e-government development index above global average of 0.4992 and its ranking position is up by 21 places, moving from 93 (2014) to 72 (2016) in the world (UNDESA, 2016). Some examples of e-government services in South Africa are illustrated in Table 2-1.

**Table 2-1:** Some examples of e-government services (created by Author)

| Interaction | Examples of e-government services |
|---|---|
| G2B | SARS: eFiling – submit a variety of tax returns<br>National Treasury – register to Central supplier to conduct business with SA government<br>CIPC – eservice for registration of private and non-profit companies and intellectual property rights<br>DoL:<br>uFiling – submit unemployment insurance fund (UIF) declarations, pay UIF contributions and update salary details,<br>compensation fund – register, submit earning, submit claims and pay electronically<br>SITA – e-Services website (www.eservice.gov.za) for various G2B, G2C and G2G services |
| G2C | SARS: eFiling – submit a variety of tax returns<br>SAPS: online enquiry for the police clearance certificate<br>Education:<br>DBE: e-Matric – for matric registration, re-mark of papers and re-issue of a matric certificate<br>DHET: central application Clearing House helps to find a place for tertiary studies<br>Gauteng online registration and admission<br>DoT: eNatis – booking of drivers licence learner test, driving licence test, card renewals and professional driving permits<br>DHA: eHomeAffairs – ID and passport application and verification<br>Municipalities: e-statements, e-payment<br>SITA – e-Services website (www.eservice.gov.za) for various G2B, G2C and G2G services |
| G2E | e-administration within departments<br>Government Employee Pension Funds (GEPF)<br>DPSA: eDisclosure: disclosure of financial interests |

| | |
|---|---|
| G2G | SARS: eFiling – submit a variety of tax returns<br>NSG: Online learning<br>e-Services website (www.eservice.gov.za) (SITA) |

### 2.2.3 Mobile government

The Increase use of mobile technologies has enabled governments to expand e-government services to mobile government services (m-government) (Mengistu, Zo, & Rho, 2009; Trimi & Sheng, 2008). M-government affords access to government services to a wider population through mobile technologies such as smartphones, tablets, laptops, and wireless communication networks, anytime and anywhere (Mengistu, et al., 2009; Ogunleye & Van Belle, 2014). M-government is not a replacement for e-government, but rather an extension or complementary to existing e-government services (Zefferer, 2011).

M-government is defined as “a strategy and its implementation involving the utilisation of all kinds of wireless and mobile technology, services, applications and devices for improving benefits to the parties involved in e-government including citizens, business and all government units.” (Kushchu & Kuscu, 2003).

In spite of the factor that global use of mobile technologies is increasing rapidly, several research studies indicate that the implementation of m-government and the research focusing on it is still nascent (Ahmad & Khalid, 2017; Alshammari, Cheung & Messom, 2018; Ogunleye & Van Belle, 2014). Like e-government, m-government has four distinct interactions:

- **m-government to business (mG2B):** Interaction between government entities and businesses, including non-profit companies,

- **m-government to citizens (mG2C):** Interaction between government entities and their citizens,

- **m-government to employees (mG2E):** Interaction between government and their employees,

- **m-government to government (mG2G):** Interaction between government entities and within government units.

According to ITU, m-government services and applications are mostly developed for the government to citizens interaction (OECD/ITU, 2011). This is no exception for South Africa as shown in Table 2-2:

**Table 2-2:** Some examples of m-government services (created by Author)

| Interaction | Examples of m-government services |
|---|---|
| mG2B | None known |
| mG2C | SARS:<br>mobile application for eFiling<br>SMS eFiling notification<br>SAPS: SMS notification for the police clearance certificate<br>Municipality: alerts notification<br>Education:<br>DBE: USSD and SMS for Matric results<br>Gauteng SMS notification registration progress and admission<br>DoT: SMS to check the status for booking of drivers licence learner test, driving licence test, card renewals and professional driving permits<br>DHA: SMS to track for ID and passport application and verification of marital status<br>DoH:<br>MomConnect – SMS to support maternal and Child health |
| mG2E | SMS notification for internal affairs<br>DoH:<br>NurseConnect – SMS relating to maternal health, child health and family planning for nurse or midwife in public health facilities |
| mG2G | None known |

In view of the above indications of different SAPSOs interactions G2B, G2C, G2E and G2G, SAPSOs have significant volumes of critical and sensitive data and information that they store and process such as citizens and employee personal information, customer data, financial information, state secrets on intelligence operations and military weapons, and so

on. Therefore, the introduction of e-government and m-government services contribute to issues of managing risks to information systems, security and privacy of critical data and critical information systems (Otjacques, Hitzelberger, &, Fernand, 2007).
This data or information has remarkable value and repercussions that can be so devastating in the event that they are lost, destroyed or land in the hands of unauthorised persons (Laudon & Laudon, 2007). Which can raise a question of what are the risks to public sector information systems and how secure are the South African public sector information systems? Mutula (2013) noted that citizens require a guarantee that the information they enter online is protected, secure and confidential.

## 2.3 Risk to Information Systems

Any organisation that is connected to the internet or dependent on third-party technology suppliers or store personally identifiable information is susceptible to cyber risks (Olsen, 2013). Cyber risks pertain to significant consequences such as financial loss, damage to information assets, failure of ICT systems, reputational damage and so on. As indicated in Chapter 1, cyber risks are ranked in the top five (5) of global risks by the World Economic Forum placing cyber-attacks and data fraud or theft in the 3rd and 4th positions respectively (WEF, 2018).

For organisations to effectively mitigate cyber risk, they need to make cyber risk part of enterprise risk management (Antonucci, 2017); they need to understand precisely what cyber risk signifies and be able to differentiate it from other traditional risks such as financial or operations risks. There are several useful definitions of ‘cyber risk’.

Eling & Schnell (2016, p. 483) define cyber risk as “any risk emerging from the use of IT that compromises the confidentiality, availability or integrity of data or services”. Cyber risks, as defined by RSA “are the potential loss or harm related to technical infrastructure or the use of technology within an organisation” (RSA, 2016). Refsdal, Solhaug & StØlen, (2015, p. 33) define cyber risk as “a risk that is caused by a cyber threat”.

In view of these cyber risk definitions, this research defines cyber risk as a potentially damaging consequence caused by cyber threats that compromise the confidentiality, integrity, and availability of technological information systems.

Kaspersky (2018) lists the following possible cyber risks to public sector information systems:

- Data Manipulation
- Cyber espionage
- Restricted availability of online services
- Identity theft
- Hacktivism acts
- Unauthorised transactions
- Critical data theft or corruption
- Extortion

Apart from the cyber risks listed above, there are four main enterprise risks that could have serious implications to an organisation as a result of a successful cyber incident event (Blackman, 2014; Metzler, 2018)

- **Business operational risk:** possible direct or indirect loss resulting from the failure of critical business systems, processes, procedures, and people or external events.

- **Reputational risk:** potential damage or loss resulting from a negative impact on an organisation's brand and reputation

- **Legal and compliance risk:** potential damage or loss resulting from legal actions taken when an organisation fails to comply with regulatory requirements or contravening the law.

- **Financial Risk:** loss of investments and finance from litigations, repairing and remediating affected critical systems and losing clients or customers.

Risk is always associated with a threat, vulnerability (of an asset) and the potential adverse impact (Death 2017; Gibson, 2011; Talabis & Martin, 2012). This implies that without either a cyber threat or a vulnerability there will be no or little risk, see Table 2-3 for examples of common cyber risks. The terms pivotal to risks can be delineated as follows (Ciampa, 2017):

- **A threat** is any action or situation that has the potential to cause harm to or undermine the security of the organisation's information systems.
- **A vulnerability** is a flaw or weakness in information systems and information systems security controls that could be exploited by a threat actor.

- **An asset** is something of value whose failure or compromise may result in potential damage or loss to an organisation.

- **Adverse impact** is the harm resulting from the compromise of the confidentiality, integrity and availability of information or information systems.

**Table 2-3:** Examples of Information Systems Risks **(Old Dominion University, 2013)**

| Vulnerability | Threat | Risk of Compromise |
|---|---|---|
| Patches to correct flaws in application or operating system software not installed. | Computer crime, malicious use, system compromise, unauthorised access | Confidentiality and integrity of corporate data. |
| Poor Systems Administration Practices | Computer crime, malicious use, system compromise, unauthorised access | Confidentiality and integrity of corporate data. |
| Poor Password Practices | Computer crime, malicious use, system compromise, unauthorised access | Confidentiality and integrity of corporate data. |
| Lack of sufficient Operational Policies | Computer crime, malicious use, system compromise, unauthorised access | Confidentiality and integrity of corporate data. |
| Single Point of Failure | System Unavailable | Inability to access the system. |

The cyber threat landscape and cyber-attacks are dramatically escalating at a very fast pace. Cyber threats and cyber-attacks have become more diverse because the cyber threat actors are working diligently to explore new and known vulnerabilities as well as create new attack vectors or modify the old attack vectors. Cyber threat landscape reports reveal the world as being faced with new and sophisticated cyber threats and cyber-attacks every quarter or year (Check Point Research, 2018; SonicWall, 2018; Symantec, 2018). Information security companies like Symantec[1], Trend Micro[2], Hackermageddon[3] and Check Point[4] on their websites provide the latest reports and statistics on cyber threats and cyber-attacks, including the details, of the latest malware.

### 2.3.1 Cyber threats

The World Economic Forum (WEF) defines cyber threats as any potential cyber event that may breach the security of information systems and cause loss or damage by exploiting a vulnerability (WEF, 2012). Cyber threats can lead to a compromise of the confidentiality and integrity of data and can render the systems and networks inefficient and unavailable. According to Lehto (2013) and Jouini; Rabai & Aissa (2014), previous research has proposed many different ways in which cyber threats can be classified for information systems. Cyber threat classification is imperative because, for the most part, it enables understanding, identification, and profiling of features, traits, and source of the cyber threats to counter and secure information systems (Alhabeeb, et al., 2010).

Cyber threats can be classified according to the following: source, cyber threat actor, intention, motivation, impact, threat frequency and type of threat (Alhabeeb, et al., 2010; Gerić & Hutinski, 2007; Jouini, et al., 2014). For organisations to prepare for the unavoidable cyber threats, they need to consider and understand cyber threats that they are likely to face. Cyber threats can differ from one organisation to another, depending on the nature of the business, the source, and/or the threat actors' motives. A simple threat classification model such as Figure 2-1 can be used.

[1] http://www.symantec.com/security_response/
[2] http://www.trendmicro.com/us/security-intelligence/current-threat-activity/index.html
[3] http://hackmageddon.com/2015/06/08/may-2015-cyber-attacks-statistics/
[4] https://www.threat-cloud.com/ThreatPortal/#/map

**Cybersecurity threat classification criteria**

- Cyber threat source: about where the threat originates.
  - ♦ Internal source includes all employees (current and former), contractors and business associates.
  - ♦ External source includes state or non-state.
- Cyber threat intent: about whether the cause of the threat was premeditated or was without premeditation.
  - ♦ Unintentional / Accidental.
  - ♦ Intentional.
- Cyber threat motive: the goal that the source or actor wants to achieve
  - ♦ Malicious.
  - ♦ Non-malicious.

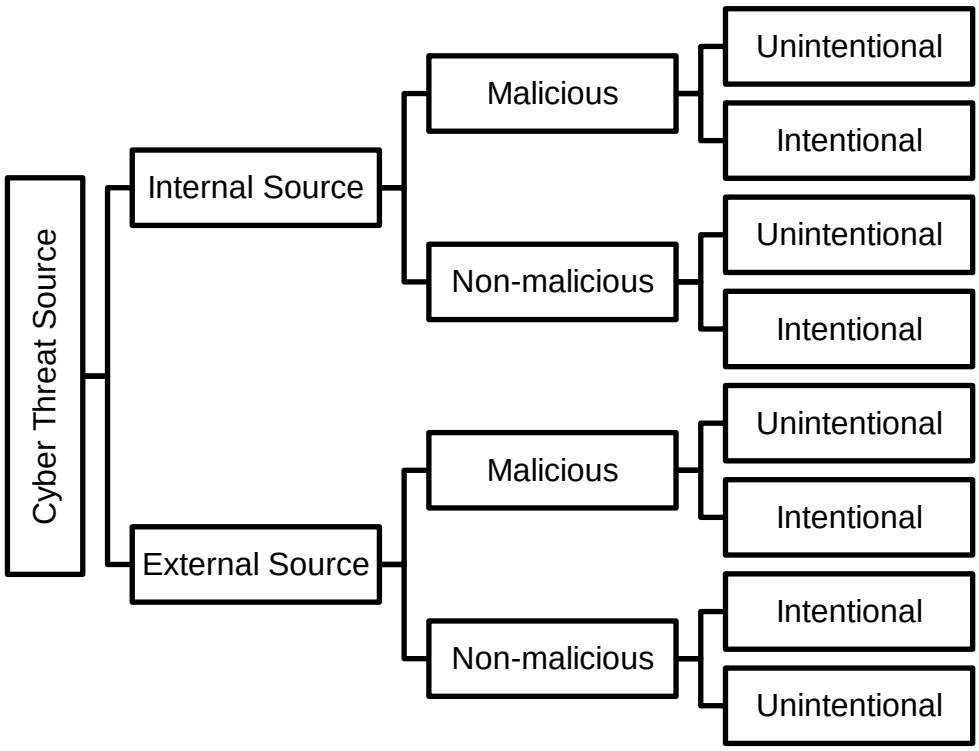



**Figure 2-1:** Cyber threats classification model **(Jouini, et al., 2014)**

There are various kinds of cyber threats, and nation-states consider different types of cyber threats in their cybersecurity strategies. In South Africa, the NCPF identifies and defines the following cyber threats to national security:

- Cybercrime: illegal acts, the commission of which involves the use of information and communication technologies.

- Cyber espionage: act or practice of obtaining secrets without the permission of the holder of the information (a person, sensitive, proprietary or of classified nature) from individuals, competitor, rivals, groups, Governments, and enemies for personal, economic, political, or military advantage.

- Cyber warfare: actions by a nation/state to penetrate another nation's computer and networks for the purpose of causing damage or disruption

- Cyber terrorism: use of internet-based attacks in terrorist activities by individuals and groups, including acts of deliberate large-scale disruptions of computer networks, especially computers attached to the internet, by means of tools such as computer viruses.

However, except for the four (4) above-mentioned broader cyber threats, PSOs are likely to face other types of cyber threats, such as:

**Malware**

Malware, short for malicious software, is a software programme written for malicious intent that surreptitiously enters the computer system (Ciampa, 2017). Malware includes viruses, rootkits, worms, Trojans, scareware, spyware, ransomware and so on. Malware is becoming sophisticated and increasing at a fast pace. According to the ENISA 2017 Threat Landscape Report, some antivirus vendors detected more than 700 million samples of malware just for the first quarter of 2017 (ENISA, 2018).

ENISA further states that there is a rise in mobile malware sophistication. Research from antivirus vendors and information risk or related firms indicates that one of the fastest growing malware and security threat to date is ransomware (Alien Vault 2017; Symantec 2018). McAfee recorded in their 2018 quarter 2 threats report about a 34% increase on new malware and a 27% increase on new mobile malware (McAfee, 2018b).

**Ransomware**

Ransomware encrypts a victim's system or data and demands from the victim for ransom to regain access to their data or system (Mims, 2017). Attackers use emails, web applications and websites as a threat vector for ransomware. According to the global investigation on data breaches by Verizon (2017), in 2016, the PSOs were the second highest victims of ransomware attacks and 96 % of public sector data was compromised by multiple ransomware attacks. In their 2018 Cyber Threat Report, SonicWall (2018) claims that in 2017, there was a "101.2% increase in new ransomware variants". The well-known ransomware for 2017 is WannaCry, NotPetya, Petya and Bad Rabbit. South Africa was targeted by ransomware between 2016 – 2017 (SOPHOS, 2018).

**Data Breaches**

A data breach is a successful security violation by which sensitive, confidential, or protected data is deliberately or accidentally accessed by or disclosed to an unauthorised person or service or entity (Ciampa, 2017). Data breach compromises information such as credit card information, personal information, intellectual property, trade secrets, health information, user account information and so on. The consequences of data breaches include identity theft, financial losses, and reputational damages (Cheng, et al., 2017). Although a data breach is counted as a cyber threat, in essence, it is not a data breach but a mutual term for launched cyber threats (ENISA, 2018).

During 2017 and 2018, South Africa experienced its two (2) biggest data breaches – both linked to public sector, namely (i) exposure of 60 million citizens' sensitive personal identifiable information (Moyo, 2017) and (ii) breach of personal records of more than 934 000 individuals for online traffic fine payment (Mohapi, 2018).

## Hacktivism

Hacktivism is an alliance that combines hacking skills and activism. It is an action inspired by ideology driven by or to address political change, social change or other agenda through cyber threats and cyber-attacks (Ciampa, 2017). Hacktivism carries civil protests in the cyberspace (Denning, 2001). This action can be conducted either by a group or individuals known as hacktivists. The cyber-attack techniques that are normally used for hacktivism are data leaks, DDOS attacks and defacement of websites (Pompon, 2017). The impacts of hacktivism are tainted organisational reputation, disruption of organisational activities, and loss of confidence from customers.

Some SAPSOs that were targeted through hacktivism are: SABC (ENCA, 2016); Armscor (van Zyl, 2016); Government Communication and Information System (GCIS) (Vermeulen, 2016); the Presidency (Watson, 2017) and the Department of Basic Education (IOL, 2017); in 2018 the Presidency, the Department of Environmental Affairs, the Department of Home Affairs and the Cybersecurity Hub were shut down by a hacker group known as “Black Team” (Breakfast, 2018; Pijoos & Grobler, 2018).

## Phishing

Phishing is one of the most commonly used cyber-attacks which primarily relies on human weaknesses. Phishing is a critical attack vector used by cyber-attackers (ENISA, 2018) to obtain sensitive personal or private information to be used for fraudulent activities. It normally occurs through a fake email sent by an attacker, which appears to be correspondence from a legitimate entity such as a known person or bank. The intention is to trick users to click a link that will direct them to an imposter website which will require users to fill in personal information.

Ciampa (2017) explains that there is some form of variation in phishing attacks, such as spear phishing – which targets specific individuals and emails are personalised for the recipient; whaling – which targets wealthy individuals or executives; and vishing – which is the voice version of phishing, the attacker uses a phone to obtain sensitive personal information; smishing – the SMS version of phishing – victims receive messages from

attackers. According to several recent cyber threats' reports, phishing modus operandi is continuously increasing in sophistication and quantity (Oest, et al., 2018; PhishLabs, 2018; Vergelis, et al., 2018)

In its 2018 Phishing Trends and Intelligence Report, PhishLabs (2018) claimed that South Africa hosts about over and around 110% of phishing sites. In 2018, PhishMe reported that phishing scams are on the rise in South Africa (PhishMe, 2018). SAPSOs are not immune to phishing, in 2017, the office of the Deputy President issued a warning against phishing scams using "email" from the Deputy President. There were also alerts purporting to be from other organisations such as the South African Revenue Services (SARS)

**Insider Threat**

A security threat to the organisation's information systems does not always come from outside of the organisation. The threat can emanate from people within the organisation who have authorised access to the organisation's sensitive data or information such as employees (current or former), business associates and contractors. Insider threat refers to a threat that can be caused by employees using their authorised access to harm the security of information systems, either intentionally or accidentally (ENISA, 2018).

Research done by Cybersecurity Insiders (2017) indicates that 90% of organisations are vulnerable to insiders. About 72% of PSOs globally had security compromised in 2016 and the main cause attributed to human error (over 50%) (Netwrix, 2017). In 2015 Aljazeera obtained copies of hundreds of leaked classified documents involving State Security Agency (SSA) and several foreign intelligence services allegedly from an intelligence agent who gave his brother-in-law access to his computer, who thus copied the files (Maphumulo, 2015).

**Cybercrime**

The advancement of ICT has brought a fast-growing crime which is a major threat to national economies - cybercrime. Cybercrime is any criminal activity committed using ICT infrastructure. Cybersecurity Ventures (2018) claim that in the next two decades the

humankind will face their greatest challenge, which is the biggest threat to every person and organisation in the world. Cybercrime cost to the global economy has jumped from the range between $345 billion and $445 billion (R4 trillion and R4.16 trillion) in 2014 to the range between $445 billion and $600 billion (R4.26 trillion and R6.96 trillion)[5] (McAfee, 2018a).

South Africa is affected by cybercrime as well with it being ranked as the fourth most reported economic crime according to the 2017 Midyear Cybersecurity Report (Cisco, 2017). According to the South African Parliament, during 2015/2016 there was a cybercrime attempt to steal +/-R3 billion from Eskom financial infrastructure (South African Parliament, 2017).

**Cyber Espionage**

(Traditional) espionage is a practice of illegally collecting intelligence to obtain confidential or sensitive information, such as military secrets, state secrets, trade secrets, and intellectual property to gain an advantage over the adversary or competitor (Hua, et al., 2015). This practice, when conducted with the means of computer systems and/or in cyberspace, is called cyber espionage. Cyber espionage can be sponsored by nation states or non-nation states (e.g. corporate). Although it has been known that cyber espionage is directed to nation states and non-nation states (corporate or industrial), individuals seem to be targets of a major cyber-espionage campaign (Fadilpasic 2017; SMEX 2018). Rubenstein (2014) claims that the three major players in cyber espionage are the United States of America (USA), Russia and China. Cyber espionage attacks rose from 9.2 % in 2016 to 14.5 % in 2017 (Passeri, 2018).

Research on data breaches by Verizon indicates that cyber espionage is one of the major threats to the public sector, and it is responsible for 41 % of data breaches in the public sector. Its further states that over 90% of data breaches to the public sector were attributed to nation states (Verizon, 2017). van Niekerk (2017) raised an interesting argument that BRICS (Brazil, Russia, India, China, and South Africa) has two of the three cyber espionage superpowers, that is, Russia and China. Therefore, South Africa should be fully cognisant

[5] Currency rate 1 USD = 11.5998 ZAR from www.oanda.com 24/02/2018.

of the potential cyber espionage actions from the two countries for their economic advancement. It is perceived China has been conducting economic cyber espionage actions to industries that are strategic to their Five-Year Plan for Economic and Social Development (Accenture, 2017).

### 2.3.2 Cyber threat actors

As the internet connection increases and cyber-attacks intensifying, the cyber-attack world is growing with different actors who are becoming more advanced and sophisticated (ENISA, 2018). The actors have different skills levels, from amateurs with no skills to cyber spies with advanced skills and well-structured support (Ciampa, 2017). The cyber-attack actors may use the same tools and cyber-attack vectors but differ depending on the target and motive. Similar to the cyber threat classification, it is critical to recognise who the major cyber threat actors are and what are their objectives are (Ablon, 2018). The four major cyber threat actors are:

**Insiders** (see also the explanation as in cyber threat)

Insiders can use their authorised access to harm the security of information systems, either intentionally or accidentally (ENISA, 2018). Most insider attacks come from negligent insiders because of, for example, carelessness, non-compliance, and compromised credentials (Cybersecurity Insiders, 2017). The insiders can cause serious impacts to the organisation such as disruption of organisational activities or operations; disclosure of the organisation's sensitive information; tainted reputation to the organisation and loss of confidence by customers or stakeholders.

**Hacktivists**

Hacktivists are not motivated by money but motivated by political, economic, and socio-cultural agenda. Their objective is to expose information about wrongdoings or retaliate for a specific prior event (Ciampa, 2017). They have moderate skills and their preferred methods of attacks are a defacement of websites to make a statement and DDoS attacks to deny access to services (Denning, 2001). Hacktivists want their motivation to attract

attention since they direct their attacks with an unequivocal aim of press coverage, conveying their message and humiliating their targets (Donaldson, et al., 2015). The well-known hacktivist group is Anonymous and its affiliates.

**Cyber criminals**

Cyber criminals are motivated by money, they attack for profit, that is, to steal money or data and sell it (ENISA, 2018). Cyber criminals are a network of very motivated, organised, equipped and operate at an advanced skills level using different methods depending on the target (Ciampa 2017; Merkow & Breithaupt, 2014).

**Nation-States**

This group of cyber-attackers is state sponsored. Nation-states cyber actors are extremely skilled, strategic, and coordinated (Ciampa, 2017). They are well funded and have sufficient and sophisticated resources. Their main focus is to engage in cyber espionage, although they can focus on others as well such as sabotage or propaganda (Death, 2017). To achieve their objective, nation-state cyber actors are patient and persistent; they will quietly hunt their target regardless of what extent it takes; and their targets can be foreign governments, foreign business, and their own citizens (Ciampa, 2017).

### 2.3.3 Cyber-attacks

Cyber-attack is a deliberate action by an individual or group or organisation or government, being driven by a certain motivation, to damage, destroy, compromise the information systems by employing various malicious methods through cyberspace. NIST SP 800-53 defines a cyber-attack as “an attack, via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.” (NIST, 2013, pp. B-6).

No one is immune from cyber-attacks; they strike organisations every day. In many instances it is impossible to immediately know that a cyber-attack has occurred in an organisation, even if it is known, the primary objective and true purpose of the actors even

if claim responsibility may not be known (Shakarian, et al., 2013). The escalating of the sophisticated cyber-attacks these days is very disturbing and by the look of things, they are going to be part of our everyday lives.

Cyber-attacks are classified using the same model used for cyber threat classification. There are various techniques used for cyber-attacks and some of the commonly used cyber-attack methods are listed in Table 2-4.

**Table 2-4:** Some of the commonly used cyber-attack methods (Kaur, et al., 2015; Farbat, et al., 2001)

| Method | Description |
|---|---|
| Targeted | A targeted cyber-attack that targets a specific organisation because of a specific motive or interest in that organisation. This attack is more damaging because attacks are customised just for that organisation. |
| Distributed Denial-of-service (DDOS) | Attacks used to force organisations' systems or network to be out of service by bombarding the target systems or network with a big volume of data containing malware. It is usually launched using a Botnet. |
| Botnet | Network of computers infected with malware and is remotely controlled by the originator to launch an attack (DDOS). Computers are private, from different locations, and owners might not be aware. |
| Phishing and spear phishing | Cyber criminals mostly use phishing, to get sensitive information such as banking details and password. It uses fake websites, emails and instant messaging that look authentic and it attacks randomly.<br>Spear phishing is a targeted phishing aimed at a specific person or a specific group. |
| Advanced persistent threats | A targeted attack, which is stealth and takes place continuously and persistently for a specific target to gain access to very valuable information. It is used for cyber espionage. |
| Malware/spam | Malicious software is developed for the intent of executing malicious actions to the computer or network, such as destroying information, disrupt or modify or infect other systems. Virus, worm, Trojan horse, and spyware. Spam is an attack by sending voluminous unsolicited emails for the aim of introducing a malware. |
| Hacking | Gaining unauthorised access to a computer or network. |

| Method | Description |
|---|---|
| SQL injection | An attack by injecting a malicious SQL query into the SQL database application. |
| Ransomware | Malware used to prevent a user from accessing their computer until they pay to regain access to their computer. It encrypts the data or computer system. |
| Defacement | Is mostly carried out by altering the content of the target's website driven by a certain motive, and a message will relay the motive. |

South Africa is not immune to cyber-attacks. According to the 2013 Norton global cybercrime report[6], about 84% of South African adults have been victims of cybercrime, which rate South Africa to be 2nd globally. The economic impact caused by cybercrime in South Africa equals 0.14% of the national Gross Domestic Product (GDP), about R5.8 billion a year[7]. During the ITWeb Security Summit[8], Vernon Frey (2015), a chief technology security officer at Vodacom, in his presentation stated that South Africa is the most attacked country in Africa by the distributed denial-of-service (DDOS). These DDOS attacks increased by about 150% between November 2013 and April 2015. There have been attacks in South Africa, but most of them are either not reported or under-reported because there is no legislation that is enforcing organisations to disclose cyber-attacks or data security breaches.

## 2.4 Information Systems Security

Public sector information systems carry a big amount of information or data, not only about its employees but it includes citizens, businesses, and other government organisations, therefore, the PSOs become targets of cyber threats and cyber-attacks.

Furthermore, a large part of the PSOs network is connected to the internet to provide e-government and m-government services making it more vulnerable because it is practically

[6] http://za.norton.com/cybercrimereport
[7] http://www.htxt.co.za/2014/11/11/cybercrime-costs-south-africa-about-r5-8-billion-a-year/
[8] 10th annual security summit was held in Midrand, South Africa, 26-27 May 2015 and The author attended the security summit.

exposed to anyone. The critical information and data that is stored and processed by PSO information systems include citizens and employee personal information, financial information, medical records, individual and company taxes, state secrets on intelligence operations and military weapons and so on. This increase the concern of security, privacy and integrity of critical information, data, systems, and networks.

Some cyber-attack reports reveal that PSOs are beginning to be amongst the prime targets for cyber-attacks (Brown, 2018; Dimension Data, 2017). SAPSOs such as the Department of Home Affairs, Department of Social Development, Municipalities, and the South African Revenue Services (SARS) have personal information of nearly every South African and if that information lands in the hands of cyber threat actors such as cyber criminals it may have a devastating effect.

Considering the sensitive nature of personal information and other critical data in PSOs information systems, it is critical that PSOs ensure the security and resiliency of their information systems. Consequently, failure to secure the information systems will be at a great cost. The design consideration for PSOs to secure information systems is to put information security, cybersecurity, and cyber resilience at the core of the information systems (Caballero, 2017).

Information Systems Security (ISS) involves the application of the set of policies, processes, and procedures to ensure the protection of confidential, integrity and availability of information systems from unauthorised access, use, modification, disruption, disclosure, and repudiation (Smith & Jamieson, 2005). ISS has become an increasing priority for organisations. The success of technologically interconnected PSOs information systems and ISS concerns addressing the issues of cybersecurity as well.

### 2.4.1 Information and cybersecurity

Information security as defined by ISO/IEC 27000 “ensures the confidentiality, availability and integrity of information.” ISO/IEC 27000 further states that “information security involves the application and management of appropriate controls that involves consideration of a

wide range of threats, with the aim of ensuring sustained business success and continuity and minimising consequences of information security incidents." (ISO/IEC, 2018).
von Solms & von Solms (2017, p. 5) define Cybersecurity as "that part of Information Security which specifically focuses on protecting the Confidentiality, Integrity and Availability (CIA) of digital information assets against threats, which may arise from such assets being compromised (via) using the internet".

Therefore, both information security and cybersecurity are concerned with the confidentiality, integrity, and availability (CIA) of information. These three are referred to as the CIA triad (Figure 2-2). The CIA triad is defined as follows (Whitman & Mattord, 2014):

- **Confidentiality** concerns information and data privacy. It ensures that sensitive information and critical data is not accessed, used, or disclosed by unauthorised persons or entities.

- **Integrity** concerns the accuracy and consistency of systems, networks, and data. It ensures that systems, networks, and data have not been modified or deleted, either deliberately or accidentally.

- **Availability** ensures that networks, systems, and data are accessible and usable by authorised users.

According to Cherdantseva & Hilton (2013), some researches claim that the CIA triad as a comprehensive set of security principles is inadequate and that it does not give protection against emerging security threats in the collaborative de-parametrised situations. Cherdantseva & Hilton (2013) therefore based on their detailed analysis of Information Assurance and Security (IAS) literature proposed the IAS-octave as an expansion of the CIA triad to includes accountability, auditability, authenticity/trustworthiness, non-repudiation, and privacy. They are defined as:

- **Accountability** is a security measure that ensures people or systems are accountable, and they take the liability of their actions.

- **Auditability** is a security measure that assures that information systems are continuously monitored and assessed and any actions can be traceable.

- **Authenticity / Trustworthiness** are a security measure that verifies the credentials of, for example, a user, software applications or programs, hardware and then establish trust as soon as there is authorisation.

- **Non-repudiation** is a security measure which uses security mechanisms like digital signature or cryptography to ensure that a party does not deny the legitimacy of their actions or operations regarding information or data.

- **Privacy** is a security measure that ensures the privacy of personal information and is limited to only those who use it.

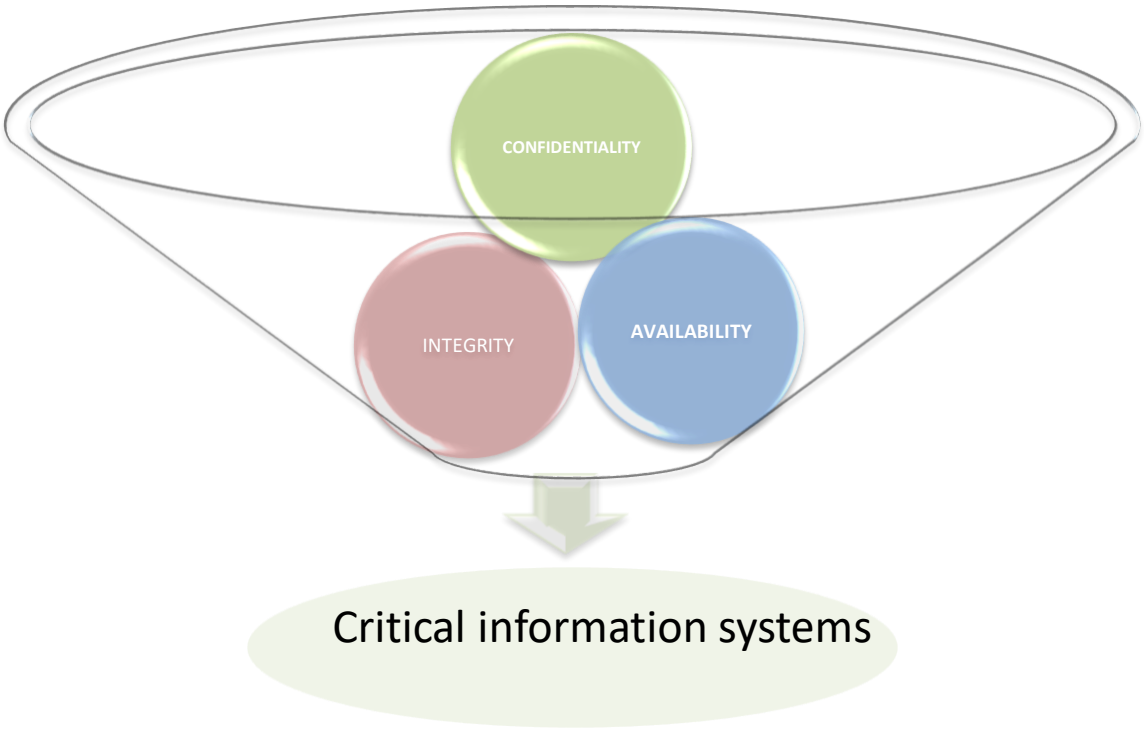



**Figure 2-2:** The core fundamentals of information and cybersecurity security (created by Author)

For information security and cybersecurity to be successful and to ensure the resilience of information systems, an efficient information security management system (ISMS) and defined critical success factors (CSFs) are required. Rockart (1979) defines CSFs as “the limited number of areas in which results, if they are satisfactory, will ensure successful competitive performance for the organisation.”.

CSFs support the achievement of the organisational objectives; therefore, the executive management must give continuous and worth consideration to them (Rockart, 1979). There are several research studies that have identified the CSFs in the successful implementation of ISS in the public sector (Jin-fu, 2009; Shareef, 2016; Smith & Jamieson, 2005; Torres, et al., 2006; Tu & Yuan, 2014). The CSFs differ given the differences in the organisations, however, they have similar CSFs that is thought to be critical for public sector information systems security.

- Organisational support
  - Active top management support
  - A commitment of sufficient funding

- Organisational awareness
  - Staff awareness and training
  - Security culture

- Security controls and development / Information security infrastructure
  - Risk management
  - Security policies implementation
  - Compliance with standards
  - Protection of information assets

- Statutory / legislative requirements
  - Security and privacy legislation

### 2.4.2 Information security management system

According to the international standard ISO/IEC, ISMS "preserves the confidentiality, integrity and availability of information by applying a risk management process." (ISO/IEC, 2013, p. v). Furthermore, ISMS is regarded as "a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organisation's information security to achieve business objectives." (ISO/IEC, 2018, p. 11). The goal of the ISMS is to ensure business continuity and managing risks to information systems by proactively limiting the impact of a security breach to minimal (Susanto & Almunawar, 2018)

The implementation of a successful ISMS presently is governed by the availability of standards. These standards are developed to assist organisations to ensure that security is maintained at a satisfactory level, resources are utilised correctly and the best practices for security are adopted. "By adopting an authoritative guideline, organisations can demonstrate their commitment to secure business practices; organisations may then apply for certification, accreditation, or a security-maturity classification attesting to their compliance to a set of rules and practices" (Siponen & Willison, 2009). Some of the standards that can be adopted are ISO/IEC 27001, ISO/IEC 27002, COBIT, ITIL, and so on.

**ISO/IEC 27001**

The ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organisation (ISO/IEC 27001, 2014). Its focus is to safeguard the confidentiality, integrity and availability of the information in an organisation based on a risk management process (ISO/IEC27001, 2014; Kosutic, 2014). ISO/IEC provides a four-stage continuous improvement process that is used to check and preserve the effectiveness and efficiency of ISMS (Susanto & Almunawar, 2018). This process is referred to as Plan-Do-Check-Act (PDCA) model as illustrated in Figure 2.3:

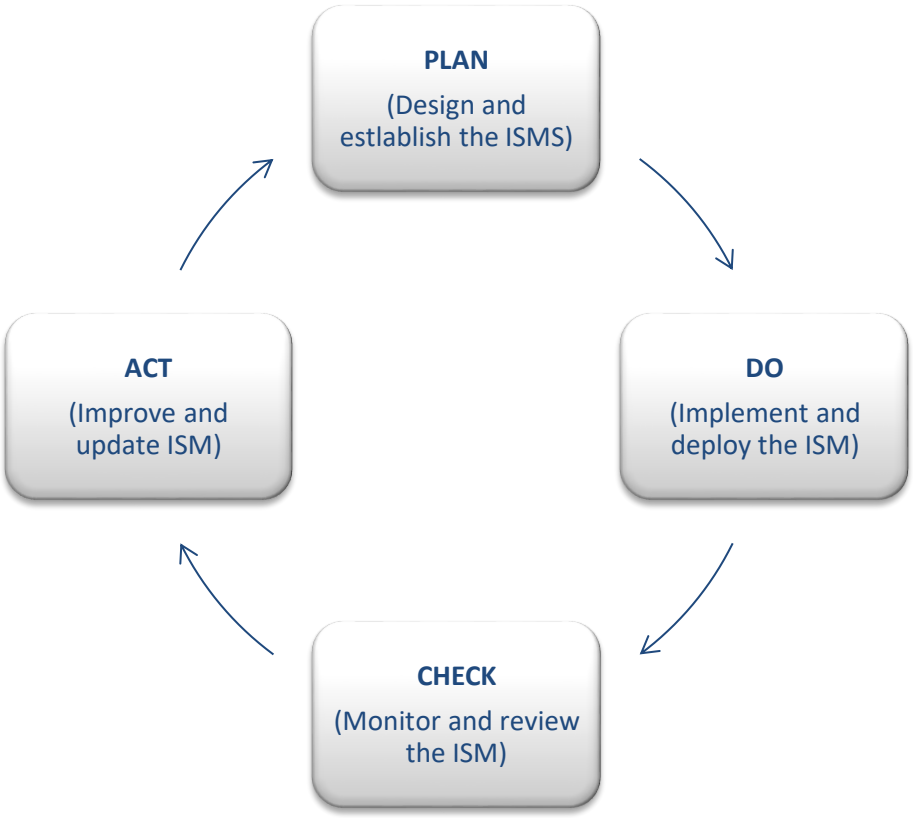



**Figure 2-3:** ISO/IEC 27001 process for ISMS efficiency and effectiveness **(ISO/IEC, 2013)**

ISO/IEC 27002 provides guidelines for best practise and guidance for the selection, implementation and management of control objectives based on ISO/IEC 27001 in the process of implementing an effective information security management system (Pandey, et al., 2013). The control objectives specified in ISO/IEC 27001 are:

- Information security policies,
- Organisation of information security,
- Asset management
- Human resources security
- Physical and environmental security,
- Communications and operations management
- Information systems, acquisition, development and maintenance
- Access control,

- information security incident management,
- Business continuity management,
- Compliance.

**COBIT**

Control Objectives for Information and Related Technology (COBIT) is an IT management and IT governance framework developed by the Information Systems Audit and Control Association (ISACA). COBIT is an internationally recognised framework for enterprise IT that aligns and corresponds with other highly recognised standards and frameworks such as ITIL, PRINCE2, TOGAF, PMBOK and ISO (ISACA, 2012). COBIT also act as a tool for regulatory compliance because it gives an option for organisations to have frameworks in place for risk monitoring, mitigation and control, for example, South Africa has a Corporate Governance of ICT (GCICT) policy framework based on the principles of King III, ISO/IEC 38500 and COBIT (ITWeb, 2013). The COBIT framework, like ISO/IEC 27000 family of standards, is applicable to any organisation regardless of sector and size. The latest version is COBIT 5.

*"COBIT 5 provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise IT, helps enterprises create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resources use and it enables IT to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT-related interests of internal and external stakeholders"* (ISACA, 2012, p. 13).

Some research findings state that COBIT 5 is the only framework that provides management and governance of enterprise IT and integrates high-level thinking in enterprise governance and management techniques (Khanyile & Abdullah, 2012; Mukherjee, 2013). COBIT 5 assists businesses and IT experts with globally adopted principles, practices, analytical tools and models to enhance trust in, and value from, their enterprises' information systems (Bernard, 2012; Mukherjee, 2013). The COBIT framework is based on five basic principles

inclusive of guidance on a holistic approach of seven enablers for effective governance and management of enterprise IT (ISACA, 2012).

***A. Principles***

- Meeting stakeholders needs
- Covering the Enterprise End-to-End
- Applying a Single, Integrated Framework
- Enabling a Holistic Approach
- Separating Governance from Management

***B. Enablers based on Principle 4***

- Principles, Policies and Frameworks
- Processes
- Organisational Structure
- Culture, Ethics and Behaviour
- Information Services, Infrastructure and Applications
- People, Skills and Competencies

**ITIL**

Arraj (2013) defines the Information Technology Infrastructure Library (ITIL) as a framework of best practices and guidelines that provides a holistic process and practical approach to the identification, planning, delivery and support structures for the effective management and control of IT services. ITIL is the most popular, globally accepted framework approach to IT Service Management (Al Mourad & Hussain, 2014). ITIL can be applicable to just about any type of IT environment. The latest version of ITIL is ITIL 2011 (also known as ITIL V3), which adopts a life cycle of five core volumes (Ali & Soomro, 2014).

**A. Five core volumes of ITIL V3**

- Service Strategy
- Service Design
- Service Transition

- Service Operational
- Continual Service Improvement

Volume 2 of ITIL V3, the ITIL Service Design, provides information security management process, which is based on the ISO/IEC 27002, the Information security management systems – Code of practice for security control, as well as other ISO 2700x family of standards (Larrocha, et al., 2010). ITIL also aligns and corresponds with other internationally recognised frameworks and standards, such as COBIT, ISO/IEC 20000 and ISO/IEC 27001 (Kneller, 2010).

Effective information security, cybersecurity, ISMS and achieving business objectives is not only about or dependent on security technologies alone but should be established from all these pillars: people, processes, and technology. (Dutton, 2017; Edwards, 2017; Norman & Yasin, 2013). This is a build-up to an integrated approach that will enable resilient information systems. An organisation can have the best security technologies, however, without looking at the other ISMS pillars and CSFs that influence the successful implementation of ISMS, the security of information systems will not be effective.

### 2.4.3 Information security risk management

An effective and efficient ISMS and the identification of organisational needs concerning requirements for information security requires a systematic approach to information security risk management (ISRM). ISO/IEC 27005:2018 defines ISRM as a “continual process that should establish the external and internal context, assess the risks and treat the risk using a risk treatment plan to implement the recommendations and decisions.” (ISO/IEC, 2018, p. 2). The ISRM process consists of context establishment, risk assessment, risk treatment, risk acceptance, risk communication and consultation and risk monitoring and review (ISO/IEC, 2018) as illustrated in Figure 2-4.

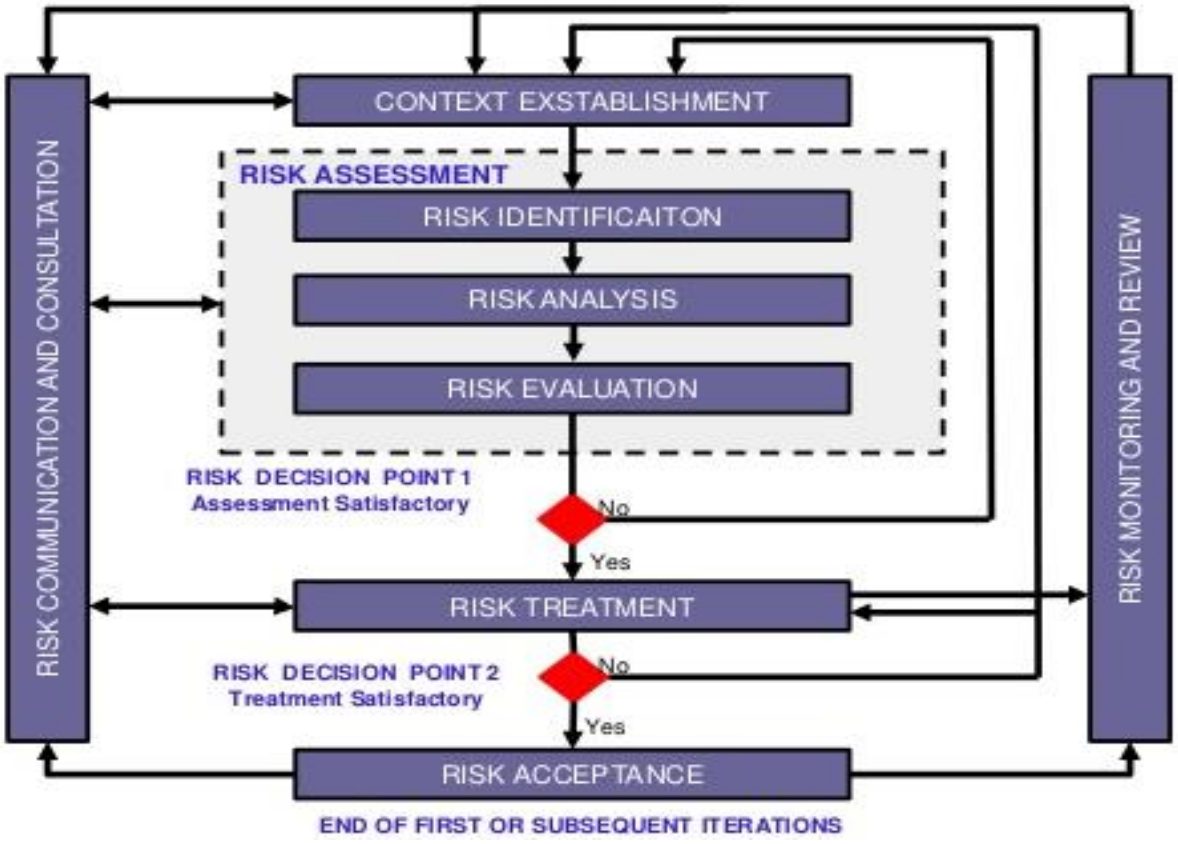



**Figure 2-4:** Illustration of an information security risk management process **(ISO/IEC, 2018)**

### 2.4.4 Business continuity plan and disaster recovery plan

Business continuity plan (BCP) and disaster recovery plan (DRP) are plans intended for the protection of mission-critical information systems from the impacts of major distractions and limiting the risks of disruptions to business activities. Business continuity implies that an organisation's critical information systems will continue with operations during and after extremely difficult conditions. Disaster recovery simply implies the recovery of information systems after disasters. Business continuity is more about organisational operations and it is strategic, whereas disaster recovery is more on technology and it is a component of the business continuity (Kosutic, 2010).

According to ISO 22301, BCP is defined as "documented procedures that guide organisations to respond, recover, resume and restore to a pre-defined level of operation following a disruption." (ISO 22301, 2012).

According to (Martin, 2002), DRP is “designed to ensure the continuation of vital business processes in an event that a disaster occurs.” This process will resume and restore all mission-critical process within a required timeframe.

### 2.4.5 Cyber resilience

Cyber risks are becoming more frequent, sophisticated, and diverse. Cyber mitigation approach is about introducing specific measures to either reduce, to an acceptable level the likelihood of re-emerging, impact and exposure or eliminate cybersecurity risks. Cyber risk mitigation is not about using technology only, but it should be a risk-based approach that involves cybersecurity strategy as well as security and risk management standards to improve cybersecurity and resilience.

There is no silver bullet in securing information systems in this technologically interconnected world. Nations and organisations need to have a better solution to address cyber risks that they face every day. Therefore, the cybersecurity concept alone is no longer sufficient to deal with these sophisticated, diverse, and rapidly intensifying cyber risks. Security must advance outside the limitations of cybersecurity in the direction of a proactive approach - cyber resilience approach.

The two concepts are different but they complement each other. Cyber resilience should not be considered as being a duplicate to or isolated from information security and cybersecurity.

#### What is cyber resilience?

The term resilience is used with reference to a different perspective from various disciplines such as ecology, engineering, social sciences, psychology, health, and beyond (Ruth & Goessling-Reisemann, 2019). This term can be defined differently and applied in different research context and topics across all these fields, however, the concept of resilience is closely related with the ability to respond well to difficult circumstances and recover from them to a normal state.

O'Neill (2016, p. 451) defines resilience as "the ability of systems and organisations to maintain an acceptable level of service in spite of crises or adverse operating conditions and to recover quickly in the event that service falls below acceptable standards".

The notion of resilience to information systems does not change that much. Resilience within the information systems context, considering the interrelated components (technology, people, and processes), is related to both social (organisation, people) and technical or technological systems to respond and recover from difficult circumstances. Resilience is an emerging topic in information systems research, but there is limited knowledge around the conceptualisation and application of resilience in relation to information systems (Heeks & Ospina, 2019; Koslowski, 2014; Müller, et al., 2013).

Information systems resilience is defined as "the ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs." (NIST, 2013).

Resilience has been embraced by many organisations in private and public sectors, such as the World Economic Forum, Symantec, European Commission and MITRE Corporations, as a guiding principle for cybersecurity, recognising the interrelationships among information systems, people, and processes (Roege, et al., 2016)

To unpack the concept of 'cyber resilience', a relook is firstly required of 'cybersecurity', 'information security' and 'ISMS' as discussed in section 2.4.1. Cybersecurity is concerned with the protection of confidentiality, integrity, and availability of information in cyberspace from cyber threats and cyber-attacks. Cybersecurity is about protection and prevention – it is reactive.

**Cyber resilience** is the ability of information systems and the organisation to anticipate, withstand, prepare for, respond to, recover from, adapt to, and evolve to improve capabilities in the face of, adverse conditions, cyber-attacks, cyber incidents, or compromise on cyber resources (Bodeau & Graubart, 2017; Clark-Ginsberg, 2017).

Information security is fundamental to the cyber resilient approach because it is an underpinning factor to resilient information systems. Information security is also concerned about business continuity and minimising consequences. Therefore,

**Cyber resilience** = information security + cybersecurity + cyber risk management + business continuity + incident response.

Cyber resilience does not only protect and prevent cyber-attacks. It assesses and mitigate cyber risks, responds to the attacks as well as restores operations to a stable condition at an acceptable time after an adverse cyber incident. Similar to ISMS, the success of cyber resilience relies on people, processes, and technology (Symantec, 2014). Finally, cyber resilience is also concerned about the protection of confidentiality, integrity and availability of information and information systems.

**Why is cyber resilience important?**

*"Cyber resilience is important for mission-essential systems…is that attribute of a system that assures it continues to perform its mission-essential functions even when under cyber-attacks."* (US Department of Homeland Security, 2018, p. 6).

Cyber resilience is more of a defence in-depth, risk management-based approach. It is concerned with the management of cyber risks and cybersecurity using an approach that incorporates people, information, technology, and facilities (Symantec, 2014). Cyber resilience is a concept that provides various principles and practices associated with cybersecurity, information security, business continuity, disaster recovery and cyber incident response (Giudice, 2016). One of the focuses for cyber resilience is that it provides organisations with an ability to be ready of the 'unknown unknowns' in cyberspace (de Crespigny, 2012).

As per the definition, cyber resilience will ensure that critical systems, networks, and data are restored during and after an adverse attack. Cyber resilience is a risk management approach that can minimise the impacts of cyber-attacks. Zhu, et al., (2016) proposed cyber resilience metrics to estimate the resilience time of the systems:

- **Identification time –** the time that a system takes to identify an incident.

- **Protection time –** the time that a system can withstand an incident without performance degradation.

- **Degradation time –** the time that a system takes to reach its maximal performance disruption due to an incident.

- **Performance degradation –** the maximal system performance disruption due to an incident.

- **Recovery time –** the time that a system needs to recover and return to normal operations after an incident.

**Why cyber resilience and not cybersecurity?**

*"A key point that differentiates cyber resilience from cybersecurity is that cyber resilience continues to function even after the adversary has penetrated the security perimeter of a network and has compromised cyber assets."* (US Department of Homeland Security, 2018).

Cybersecurity provides single layer protection, that is, it focuses on security alone. On the contrary, cyber resilience is broad, it provides multi-dimensional protection. Cybersecurity is concerned with protecting IT systems from cyber threats and cyber-attacks, while cyber resilience takes a risk management-based approach: prepare/identify, protect, detect, respond and recover, and minimise risks (threats and vulnerabilities) to ensure business continuity and delivery (Björck, et al., 2015).

von Solms & von Solms (2018, p. 4) define cybersecurity as a "preservation of the confidentiality, integrity and availability of information in cyberspace". Allen, et al. (2012) state that cyber resilience, during and after disruption, must achieve confidentiality, integrity, availability, and privacy but depend on the type of asset (people, information, technology, and facilities).

**How does an organisation become cyber resilient?**

*"A cyber-resilient company is one that can prevent, detect, contain, and recover, minimising exposure to an attack and its impact on business, against countless threats to data, applications and IT infrastructure, and especially against devices, where the organisation's most valuable assets reside, since reaching them also implies attacking the integrity of identities and users."* (The European Cybersecurity Hub, 2018)

Organisations striving to attain and maintain resilience must acknowledge that information systems protection, cybersecurity and information security approaches alone no longer suffice. Organisations need to transform their information security and cybersecurity posture from a reactive, defensive mode to a pro-active, robust, and resilient mode (Symantec, 2018). Any organisation that uses ICT systems and is connected to the internet will need to have the capability to resist and recover from the impacts of cyber incidents. Organisations need to start thinking about cyber risks and consider integrating cyber risk management to their enterprise risk management (The European Cybersecurity Hub, 2018; WEF, 2012; WEF, 2015).

Organisations need to have the following adequate and approved documents in place: cybersecurity strategy, business continuity plan, disaster recovery plan and cyber incidence response plan (WEF, 2017). Furthermore, the top executive needs to drive and be responsible for the cyber resilience agenda, align the cyber resilience strategy to the organisation's strategy (WEF, 2015). "No organisation is an island", therefore, a cyber resilient organisation leverages on a partnership for information and cyber threat intelligence sharing. Organisations can adopt as well as align their cybersecurity to internationally recognised cyber frameworks or standards or good practices (Brown 2013; Donaldson, et al. 2015)

Goche & Gouveia (2014) pointed out that there are three key changes required from an organisation:

- **Perspective** – towards identifying critical assets and the security measures required by the critical assets instead of looking at security measures first.

- **Budget** – prioritised for best security methods for the protection of critical assets.

- **Expectations** of cyber risks or cyber-attacks and reduce the impacts through cyber resilience instead of focusing on cybersecurity alone.

There are some key elements required to lay a solid cyber resilience foundation for organisations to be and remain cyber resilient, that is, (i) promoting a cyber-secure culture by ensuring that all employees, business partners and contractors understand that cybersecurity and cyber resilience is a shared responsibility; and (ii) employees need to understand the cyber risks and their roles and responsibilities to reduce the risk (Rance, 2014). Cyber resilience is risk management based and there is information sharing and partnerships.

**Who is responsible for cyber resilience?**

*"Cyber resilience is about more than just IT risks, it deals with business risks that could impact the survival of the whole organisation. This means that decisions about cyber resilience need to be made by executive management and the board of directors."* (Rance, 2014).

The existence and reputation of an organisation reside with the Board of Directors (the Board) or Executive Management (the Executive), therefore, cyber resilience and cyber risk management is fundamentally their responsibility (WEF, 2017). As cyber risk can have a devastating impact on the organisation's day-to-day operations, therefore, the cyber risks mitigation must form part of the strategic or enterprise risks. The key to successful mitigation of cyber risk is to rely not on cybersecurity alone but on cyber resilience and subsequently, the key to successful cyber resilience depends on the governance and leadership of the board or executive (North & Pascoe, 2016). The Board and Executive's "buy-in" is essential for the success of cybersecurity and cyber resilience.

To effectively manage cyber risks and cyber resilience, the Board or Executive must understand their roles and responsibilities and that cyber resilience must be driven from the top. Furthermore, cybersecurity roles and responsibilities need to be identified, clearly

defined, and aligned to the cybersecurity strategy as well as ensuring employees are aware of their roles and responsibilities for cyber resilience (Giudice 2016; NIST 2017). Some examples of the Board or Executive roles and responsibilities as pointed out by North & Pascoe (2016), WEF (2017) and Rance (2014) are listed below:

- Promote well established organisation-wide cybersecurity and cyber resilience culture.
- Ensure that cybersecurity strategy is aligned with the organisation's strategy, moreover, cyber risk and cyber resilience is incorporated into the organisation's strategy.
- Take ownership of cyber risk and cyber risk management strategy.
- Provide adequate resources for cyber resilience such as a budget, capable cyber workforce and so on.
- Delegate senior manager(s) with the expertise to lead on cyber resilience planning, cyber risk management, as well as to advise the board or the executive on the organisation's capability to manage and implement cyber resilience.
- Ensure that good communication and data breach notification strategy is in place.

## 2.5 Approach Towards Cyber Resilience

The complex nature of the rapidly escalating and sophisticated cyber threat landscape makes it challenging to have a "one-size-fits-all" solution or a silver bullet to suitably address cyber risks to technological-driven information systems.

As discussed in section 2.4.1 and 2.4.2, there are three pillars for successful ISMS and cyber resilience: people, processes, and technology. Furthermore, cyber resilience, as per the definition, has the following key attributes: anticipate, withstand, prepare, respond,

recover, adapt, and evolve. Lastly, cyber resilience is a risk management-based approach, it is intended to assess and mitigate cyber risks.

Therefore, moving towards a cyber resilience approach should start with looking at encompassing the three pillars, the cyber resilience attributes, and risk management process. This section looks at the fundamental steps an organisation needs to take towards a cyber resilience approach. Further, the section looks at some of the guidelines or attributes or best practices that have been recommended for cybersecurity and can be used as a base for the development of a cybersecurity /resilience strategy.

### 2.5.1 Fundamental steps (Harvardx, 2018)

**A. Identify critical information systems assets**

- Critical systems
  - ♦ business critical
  - ♦ mission-critical

- Critical networks
  - ♦ business and administration networks
  - ♦ operational and service delivery networks
  - ♦ communications networks: wired, wireless; and virtual private network (VPN)

- Critical data
  - ♦ personal identifiable information
  - ♦ financial data
  - ♦ state secrets
  - ♦ contract data
  - ♦ login credentials

**B. Identify possible cyber risks to the organisation (as discussed in Section 2.3)**

- cyber risks
- cyber threats

- cyber actors
- vulnerabilities

### C. Mitigating cyber risks

- Analyse identified cyber risks, cyber threats, and cyber-attacks from multiple cyber threat intelligence sources to assist in understanding the incident, verify the incident and make informed decisions. In future handling of the cyber-attacks and on how to prioritise a cyber incident based on the functional impact, information impact, as well as resources and time required to recover from an incident as illustrated in Tables 2-4, 2-5 and 2-6 respectively.

**Table 2-5:** Functional impact

| Classification level | Category | Description |
|---|---|---|
| 0 | None | No disruption to services |
| 1 | Low | Minor disruption to critical services |
| 2 | Medium | Major disruption to critical services |
| 3 | High | Severe disruption to critical services |

**Table 2-6:** Information Impact

| Category | Description |
|---|---|
| None | No information breached |
| Privacy Breach | Sensitive and personally identifiable information breached |
| Proprietary Breach | Proprietary information accessed |
| Integrity Loss | Sensitive information modified |

**Table 2-7:** Recoverability

| Category | Description |
|---|---|
| Standard | expected recovery time with available resources |
| Extended | Unpredictable recovery time with additional resources required |
| Unrecoverable | Impossible to recover |

- Implement effective physical security controls.
- Implement a perimeter network.
- Implement effective network and data protection techniques:
  - ♦ Intrusion detection and prevention system (IDPS): to monitor the IT systems to detect and alerts of any breaches to the network and then prevent the detected threats from breaching the network.
  - ♦ Security information and event management: for detection, collection and analysing of events data and logs. It generates a report and alert based on analysed log data.
  - ♦ Logs: logs from operating systems, application, network data flow and network devices are used to detect, monitor or generate alerts of anomalies against set baselines.
  - ♦ Data and file integrity checking software: used to detect any alterations made to the system and application files during a cyber incident.
  - ♦ Next-generation firewalls: deep-packet inspection, identifying and blocking sophisticated cyber incidents.
  - ♦ Antivirus and antispam software: antivirus identifies malware, generates alerts and prevent them from infecting the system. Antispam detect and block spam messages from entering the mailbox.

- ♦ Vulnerability scanners: for detecting any weakness on the systems to prevent exploitation.

- ♦ physical and logical access control: to limit unauthorised access to critical facilities such as server rooms, and limit authorised access to networks, applications and data through logical access control.

- ♦ Encryption: to protect data at rest, in use and in motion as well as email encryption.

- Regulatory and legal compliance: to comply with laws and regulations to protect data or information integrity and data privacy.

- Consider cybersecurity posture and cyber resilience of third-party service providers.
  - ♦ Have a cyber risk mitigation plan for third-party service providers.

- Have an effective, regularly tested and reviewed incident response plan and communication strategy.

- Build cyber expertise and promote organisation-wide cyber resilience culture.

### 2.5.2 Cybersecurity frameworks

There are a number of best practices, standards and guidelines for effective cybersecurity and cyber resilience implementation. These are industry standards that are internationally recognised and they can be applied to any organisation irrespective of size, industry, or sector. Organisations can use the combination of the standards to achieve maximum security and satisfy compliance and organisation requirements (Moraetes, 2018). Some of the essential vendor-neutral and technology-neutral international standards and frameworks that are most commonly adopted (Watson 2018; Telos 2017) and an organisation can choose to include the following (non-exhaustive list):

- ISO/IEC 27001 – Information Security Management System – Requirements.
- ISO/IEC 27002 – Code of Practice for Information Security Management System.
- ISO/IEC 27005 – Information Security Risk Management.
- ISO/IEC 27035 – Information Security Incident Management.
- ISO/IEC 27031 – ICT Readiness for Business Continuity.
- ISO/IEC 22301 – Business Continuity Management System.
- NIST Cybersecurity Framework.
- NIST Framework for Improving Critical Infrastructure Cybersecurity.
- NIST SP 800-160, Volume 2, Systems Security Engineering: Cyber Resilience Considerations for the Engineering of Trustworthy Secure Systems.
- ISF Standard of Good practices for Information Security.
- PAS 555 – Cybersecurity Risk Governance and Management Specification.
- COBIT 5.
- US-CERT Cyber Resilience Review.

There are quite a number of suggested best practices or controls or principles and tools for cyber resilience. However, cyber resilience begins with having an effective cybersecurity strategy in place.

### 2.5.3 Cybersecurity strategy

The first line of defence and an essential place to start measuring cybersecurity performance is for an organisation to devise a cybersecurity strategy that is aligned with the organisation's strategy (Antonucci, 2017). The cybersecurity strategy can be developed based on or referring to a single framework or combinations of frameworks (indicated in section 2.5.1 and examples to be discussed in section 2.5.3). The cybersecurity strategy must entail a clearly articulated vision, strategic goals, objectives, an action plan with set milestones and metrics to measure the progress:

- **Vision –** description of what the organisation would aspire to achieve when implementing the cybersecurity strategy. For example, “A cyber-secure and cyber resilient organisation”

- **Strategic Goals –** key actions for the organisation must achieve to mitigate the cyber risks. For example, “Build cyber expertise and promote an organisation-wide cyber-secure and cyber resilient culture”.

- **Objectives –** objectives are set to achieve strategic goals. Each strategic goal must have a set of objectives.

- **Action plan and set milestones –** an action plan is formulated from each objective that will allocate, for each task, roles, and responsibilities to a specific person. Milestones are set to determine the start and end date of actions for each task.

- **Metrics –** used to analyse or measure the progress and achievement of each goal and objectives.

**NIST Cybersecurity Framework**

One of the commonly recognised frameworks is the NIST (National Institute of Standards and Technology) cybersecurity framework. This framework provides a reference model of continuous cyber risk management that creates an effective cybersecurity programme and improves the resilience of information systems and critical infrastructures. The NIST Cybersecurity Framework has five core functions: identify, protect, detect, respond, and recover. These core functions with their categories and sub-categories are based on existing standards, guidelines, and practices (NIST, 2018), see Figure 2-4.


**Figure 2-5:** Five continuous core functions to effective cybersecurity

**Identify –** this core function is about developing an understanding of how to manage cybersecurity risks to systems, assets, data, and capabilities. The outcome for this function focuses on the following categories: asset management, business environment, governance, risk assessment, and risk management.

**Protect –** this core function is with regard to developing and implementing appropriate security systems to protect the environment against risks; to ensure delivery of critical infrastructure services as well as support the ability to limit or contain the impact of a potential cybersecurity event. The outcomes for this function focus on the following categories: identity management and access control; data security; information protection processes and procedures; protective technology; and awareness and training.

**Detect –** this core function is concerned with the detection of any information security compromise and network anomalies. Moreover, it is about the development and implementation of appropriate activities to identify the occurrence of a cybersecurity event. Implementation involves activities such as conducting continuous proactive and real-time monitoring. The outcomes for this function focus on the following categories: anomalies and events; security continuous monitoring and detection processes.

**Respond** – this core function is about the development and implementation of appropriate activities to act regarding a detected cybersecurity incident. The outcomes for this function focus on the following categories: response planning; communications; analysis, mitigation, and improvements. This function can provide an ability to respond quickly and automatically to potential attacks and thereby limiting the impact.

**Recover** – this core function is about the development and implementation of appropriate activities to maintain plans for resilient and to timely recover any capabilities or critical services that were destructed or damaged due to a cyber-attack to normal operations. This function follows a risk management process. The outcomes for this function focus on recovery planning, improvements, and commutations.

The framework also provides four implementation tiers that organisations can use to assess their current state in terms of cyber risks and processes in place to mitigate cyber risks. The tiers will assist the organisation to characterise its practices over four (4) progression ranges, that is, Tier1 – Partial; Tier 2 – Risk Informed; Tier 3 – Repeatable and Tier 4 – Adaptive. Each tier considers the following (i) risk management process, (ii) integrated risk management program, and (iii) external participation.

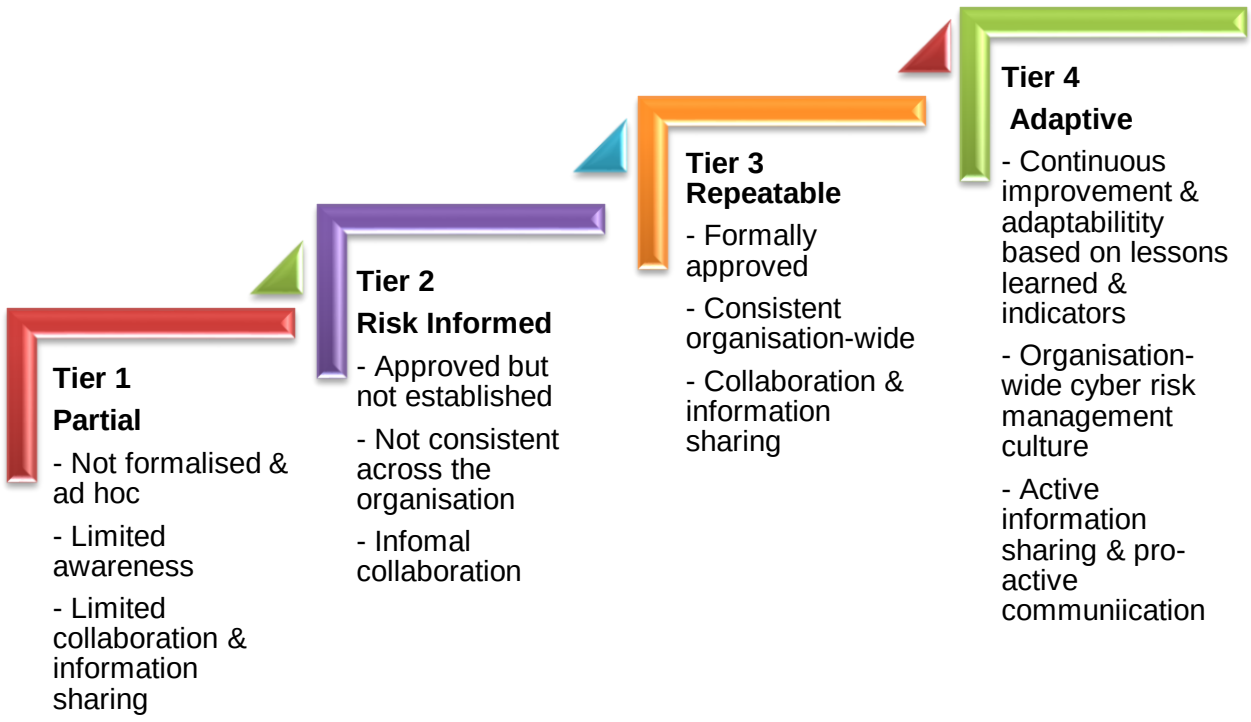



**Figure 2-6:** NIST Cybersecurity Framework Implementation Tiers (source: NITS, 2018).

### Cyber Resilience Review

The Cyber Resilience Review (CRR) is a tool developed by the US Department of Homeland Security (DHS). The CRR described as a "voluntary, non-technical assessment to evaluate an organisation's operational resilience and cybersecurity practices" (US_CERT, 2017). CRR aligns closely with the NIST cybersecurity framework. CRR evaluate cyber resilience through 10 domains:

- **Asset management –** about creating an inventory and the management plan of critical assets.

- **Controls management –** involves identification, implementation, assessing and managing physical and technological controls that support critical services.

- **Configuration and change management –** aim at the continuous processes that control and approve changes to ensure the integrity of critical assets.

- **Vulnerability management –** involves identification, assessment and management of vulnerabilities and sources of vulnerabilities.

- **Incident management –** establishes processes to identify, analyse, detect, respond, and recover. it also involves improving the processes from post-incident lessons learned.

- **Service continuity management –** to ensure that critical services continue to operate during a disruptive event. Service continuity plans are tested and reviewed.

- **Risk management –** process to identify, assess and mitigate risks to critical assets.

- **External dependency management –** establishes appropriate measures to identify and manage risks due to external dependencies (third-party providers).

- **Training and awareness –** focus on developing the required expertise of the cyber workforce to deal with risks. Also promotes cyber awareness activities for critical assets.

- **Situation awareness** – involves identifying, analysing, and communicating accurate and up-to-date threat information of immediate operational stability and security.

**ITU**

The International Telecommunication Union (ITU) advanced a cybersecurity strategy guide that sets parameters for designing a cybersecurity strategy. The guide indicates some pillars that a strategy should promote (ITU, 2011):

**Legal measures:** strengthening of the capacity to legislative measures to regulate cyberspace. The collaboration of government executive, judiciary, law enforcement, the private sector, stakeholder as well as international cooperation.

**Technical and procedural measures:** development of processes to ensure secure systems, apply governance and risk management. It is also for the creation of an internationally acceptable accreditation structure and standards for software applications and hardware systems to address vulnerabilities in software and hardware products as well as develop tools to identify, prevent, detect, respond, and recover from cyber-attacks, e.g. perimeter security, patching, network security strategy with secure communication, defence-in-depth, intrusion detection and prevention systems, computer forensics, and so on.

**Organisational Structures:** development of coordinated institutional structure and strategies to identify, prevent, detect, and respond to cyber-attacks against critical infrastructures, e.g. cybersecurity centre, cybersecurity research and development (R&D), Cybersecurity incident response team (both private and sector specific).

**Capacity building:** developing awareness programmes to boost cyber awareness to citizens, developing training and educational programmes for cybersecurity workforce enhancement. Developing R&D for technology innovations.

**International (organisation) cooperation:** cooperation and coordination for all nations (sectors) and international organisations in fighting against cyber-attacks.

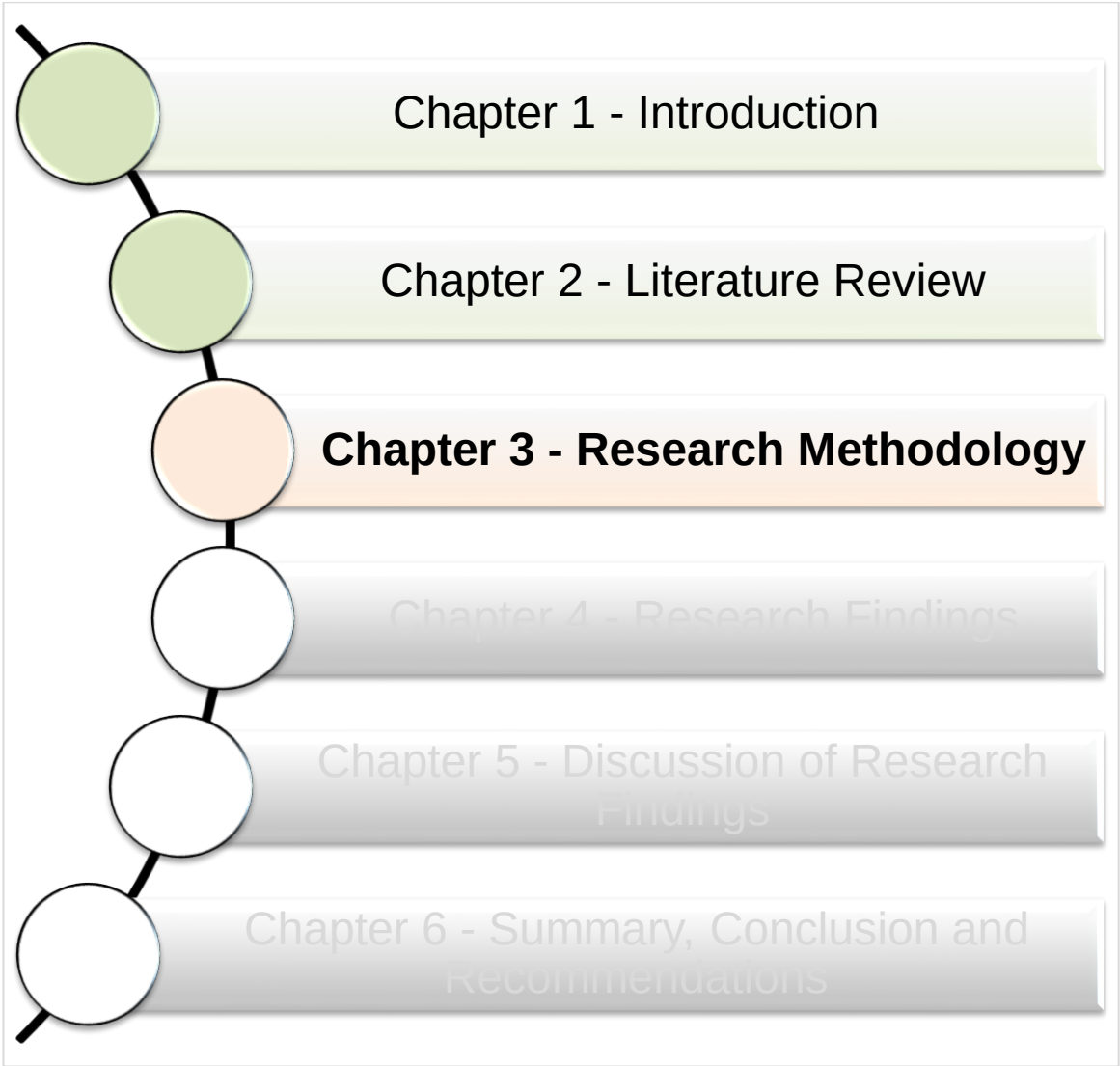
## 2.6 CONCLUSION

Research shows that information and cybersecurity alone are no longer efficient to protect information systems from sophisticated cyber threats and cyber-attacks that are increasing at a rapid speed. The key is for organisations to have cyber resilience at the core of mitigating cyber risks. Cyber resilience provides for measures to anticipate, identify cyber risks, and protect the critical assets (data, technology, people, and facilities) against the risks; detect and respond to possible cyber incidents; recover to a normal or acceptable

operation after a cyber incident as well as adapt or evolve the cybersecurity and cyber resilience programmes based on lessons learned. Although cyber resilience is a responsibility of every person in the organisation, a successful and effective cyber resilience above all requires commitment from the Board of Directors or Executive Management.

There is a rapidly growing body of research on cyber risks (threats and vulnerabilities) and cyber-attacks, which indicates that no organisation is completely cyber-secure. Consequently, prior research substantiates the supposition that organisations need to start prioritising cyber resilience, have comprehensive cybersecurity strategies, which are inclusive of cyber resilience. The cybersecurity strategy needs to be aligned to the business strategy as well as adopt standards, frameworks or guidelines that can assist in implementing cyber resilience. Although the literature review has found substantial research on cyber resilience, there is little research that focuses on public sector information systems and cyber resilience – specifically in relation to the South African public sector information systems.

# 3. CHAPTER 3 – RESEARCH METHODOLOGY



## 3.1 Introduction

This chapter outlines the research methodology that was applied to address the purpose and research questions of this study. The aim of the study is to assess the resilience of public sector information systems against cyber threats and attacks specifically in South Africa.

The next section explains the research design and the sampling approach. The chapter then proceeds with describing: the methods used for data collection, the approach to the analysis of data, the steps taken for ethical consideration and the challenges encountered during the study. The chapter ends with a conclusion.

## 3.2 Research Design

For the purpose of this study, as well as considering the limited published research regarding South African public-sector information systems, resilience, and cybersecurity. The researcher adopted a research method that she considered to be more appropriate to the research topic and to address the research questions. The researcher is of the view that the selected research method will provide a starting point in understanding the challenges faced by the government as well as to allow the researcher to get insight into the problem through people who have relevant experience in this field of cybersecurity or information security. The researcher adopted a qualitative method and an interpretive research approach as an underlying assumption (Myers, 2013).

### 3.2.1 Qualitative research

The qualitative research method is designed to assist researchers to understand the significance and perspectives of the people they study, understand how these perspectives are formed by, or shape, their (people) physical, social and cultural context as well as understand particular processes that are associated in keeping or changing these phenomena and connections (Maxwell, 2012). Myers (2013) describes qualitative research as a method that is intended to assist a researcher understand people's opinions and actions

as well as their social and cultural setting within which they live. Qualitative researchers argue that a qualitative research study is the best option in understanding people's motivations, reasons, actions, and the context for their beliefs in an in-depth method (Myers, 2013).

According to (Creswell, 2003), the main objective for conducting qualitative research is that it is an exploratory study because of the limited literature available about the topic or the population being studied and therefore the researcher seeks to engage with participants and build an understanding based on their thoughts. Qualitative research provides a researcher with an opportunity to see and comprehend the context within which decisions and actions occur, and this context is best understood by engaging with participants (Myers, 2013).

The researcher considers the qualitative research to be appropriate for this research study as the researcher seeks to gain an understanding of the status of the cyber resilience of the South African public sector information systems. According to Resilens (2016, p. 35), "Qualitative research, like all methods, has both its strengths and limitations, but offers a significant way to engage with organisational resilience, providing a space to explore issues that cannot be quantifiably measured." Issues such as governance and leadership involvement in cyber resilience, organisational cybersecurity or cyber resilience culture, training, mindfulness play a critical role in shaping the organisation to have resilient information systems.

### 3.2.2 Interpretive approach

In some researches, interpretive research is often used synonymously with qualitative research, even though the two concepts are not the same (Bhattacherjee, 2012; Myers & Avison, 2002).

Interpretive research is about the understanding of the essence of a phenomenon through accessing the meanings that participants assign to them (Myers & Avison, 2002; Orlikowski & Baroudi, 1991). It is also contextual, exploratory, and descriptive in its nature (Myers, 2013). It is context oriented in the sense that the data is only significant in a particular context (Klopper, 2008) and it is also the contextual condition that shapes the study (Flick, 2009).

Interpretive approach is “aimed at producing an understanding of the context of the information systems, and the process whereby the information systems influences and is influenced by its contexts.” (Walsham, 2009, pp. 4-5). Interpretivists believe that knowledge of reality is only possible through social constructions such as language, shared meanings, consciousness, documents, tools, and other related information systems artefacts (Goede & de Villiers, 2003)

The interpretive approach can assist the researcher to understand the thinking and actions of people in relation to the social and organisational context and it possesses the potential to construct profound understanding about information systems phenomena including the management and development of information systems (Klein & Myers, 1999). Information systems research is concerned about the ongoing interrelations among the organisation, people, process, and technology, and according to Trauth (2001), to recognise the need for qualitative research approach is to embrace a perspective that an information system is a socio-technical system and that an interpretive approach can be applied.

*“Socio-technical systems, both social and technological systems are complex, and their interactions require considerable attention not just to the working of each in isolation, but on the way in which they are connected and shape each other over time. Creating resilient socio-technical systems is an iterative process by which not only technologies, and interventions evolve, but also learning takes place by individuals and institutions.”* (Ruth & Goessling-Reisemann, 2019, p. 8).

Resilience is an emerging topic in information systems discipline that has not found a common definition or conceptualisation of resilience in information systems has been limited (Heeks, 2019; Sarkar, et al., 2016). This research study is investigating a complex, dynamic socio-technical phenomenon which has not been (sufficiently) addressed in the South African perspective.

The researcher is of the opinion that the interpretive approach is best suited to interpret and gain in-depth understanding of the situation relating to the cyber risks to, and cyber resilience of public sector information systems in South Africa, and the views of participants on the role and

responsibilities of individuals and the organisation in ensuring resilient information systems (Walsham, 2006 ).

To investigate the resilience of an organisation's information systems, the researcher needed to rely on the participants' views (understanding and interpretations) of the topic or aim of the research study based on their knowledge and experience. The interpretive approach allows the researcher to explore the basic elements which impact the ways in which organisations and people understand, identify, respond, and adapt to disruptive events. (Goede & de Villiers, 2003). Moreover, to deeply comprehend the complex social reality in view of the inherent influences and constraints of information systems (Twum-Darko, 2007), it is the researcher's considered view that the social context surrounding information systems and resilience cannot be ignored.

Interpretivism provides a framework for researchers to study and understand people's beliefs, values, meaning-making, experiences, attitudes, and self-studying (Cohen, Manion, & Morrison, 2007). Interpretive paradigm is seen by Heeks & Ospina (2019) as appropriate when resilience exists in socio-technical systems because of their open and complex nature and the involvement of people. The interpretive approach favours a qualitative method which allows in-depth investigation with a small population.

## 3.3 Sampling

This section outlines in detail the sampling technique used, the selection of a suitable population of participants and the size of the sample.

### 3.3.1 Sampling technique

Studies of this nature have applied various sampling techniques such as a non-probability, purposive sampling technique as a primary technique and snowball sampling technique as a secondary technique. A non-probability sampling does not permit random selection of the target population; however, it is significant for studying specific groups of people and/or

situations as well as probing certain important and attainable artefact for comprehensive analysis (Rubin, et al., 2010).

Purposive sampling technique is a non-probability procedure in which the target population is selected on the premise of their fit with the purposes of the study and that they satisfy a particular criterion of being considered or not considered participating in the study (Daniel, 2012). Snowball sampling technique is used when the qualities required from a target population is scarce and difficult to find (Dudovskiy, 2016).

The researcher applied the non-probability, purposive sampling technique due to the limited number of people that have knowledge and experience in this study. It is particularly appropriate in the South African public sector in addressing the purpose of this study and looking at the public sector information systems and its resilience. It was also appropriate in that the researcher required participants whose functions are primarily in information security, cybersecurity, ICT risk and/or related fields. A snowballing technique was used as a secondary technique in cases where the primary participant was not available, thus replacement was requested for an individual with similar knowledge and experience. It was used also during the interviews when the participant perceived that another person was appropriate to give more information relevant to this study.

### 3.3.2 Target population

The target population is defined as the total number of people, groups, elements, or systems that the study focuses on and to whom or which the research findings are to be applied (Boslaugh, 2008). The objective of the study was to look at public sector information systems, therefore, to ensure well representation, different government organisations were targeted as study population: national departments, local departments, parastatals, and municipalities.

The researcher targeted thirty-five (35) government organisations, with at least two (2) participants per organisation to explore the understanding of cybersecurity resilience by SAPSOs and obtain a wide range of opinions as well as to achieve the objective of the research study. Therefore, the total number of participants targeted was 70 provided that all

35 organisations agreed to participate. Subsequently, request for participation letters (Annexure A) attached with information for participation (Annexure B) and informed consent form (Annexure C) was sent to the accounting officers of each of the 35 organisations. Only 8 organisations granted the researcher permission to conduct interviews and 1 (one) organisation provided its raw data collected from a national cybersecurity readiness survey of which 11 of the respondents are government organisation. The target population was limited to the Gauteng Province. Gauteng is the economic hub of South Africa with most national government organisations and can serve as a good sample.

### 3.3.3 Sample

A sample is the set of participants or elements preferred from the target population for the purpose of the study (Guest, Namey, & Mitchell, 2013). The research study looks at assessing cyber resilience in information systems, therefore the selection of sample focused on participants with knowledge and experience in any of the fields, depending on what each entity calls it: IT security, ICT security, Cybersecurity, IT Risk Management and Governance or ICT Risk Management and Governance. The preference was to have the following participants per organisation: (i) one participant from senior management (for example, Chief Information Officer (CIO), Chief Information Security Officer (CISO), Chief Risk Officer (CRO) or ICT Manager) as they have authority, they have to account and they participate in decision-making relating to securing information systems; and (ii) practitioner in the field of ICT, information security, cybersecurity and/or information risk management.

### 3.3.4 Sample size

The sample size is the total number of participants or elements in the study (Salkind, 2010). Choosing a sample size is very critical and can be challenging particularly with some topics that are perceived to be “sensitive”. It is also noteworthy to choose or decide on the sample size that achieves the objectives of the study. However, in so doing, one should, as stated by Daniel (2012, p. 237) “carefully assess all of the relevant factors, but should not waste time and money by selecting a sample size too large, or fail to satisfy the objectives on one’s study because the sample size is too small”. There is quite a number of arguments regarding the correct size when one decides on sample size for qualitative research. In this study, the

researcher looked at what is the adequate or minimum number of participants to achieve the research purpose.

Dworkin (2012) argues that what is proposed as a minimum sample size is inconsistent. Dworkin (2012) further confers that an acceptable number for participants is anywhere from 5 to 20 as a recommended guidance and suggested by an exceedingly considerable number of articles, book chapters and books There are a range of parameters that affect the sample size, depending on the research being conducted, that is, context and logical model objectives, population, availability of resources, research design and ethical consideration (Boddy, 2016; Daniel, 2012).

Malterud & Siersma (2016) argue that “study aim, sample specificity, use of established theory, quality of dialogue and analysis strategy” influence the sample size. Some researchers argue that the primary guiding principle for the sample size should be saturation (Mason, 2010; Boddy, 2016; Guest, et al., 2013). Fusch & Ness (2015) described that data saturation is reached when there is sufficient data to repeat the research study when the capacity to obtain extra new information has been accomplished and when it is no longer possible for additional coding.

The intended sample size for this research was thirty-five (35) participants, out of the envisaged 70 participants as stated in Section 3.4.2. However, sample size can be significantly affected by different parameters, and this research study was no exception. This research study did not achieve the targeted sample size as a result of the sensitive nature of the research topic. The research topic was regarded as sensitive by various organisations, which therefore led to numerous non-responses to and declining the researcher’s request. Some of the contacted target population had a concern that information about their IT systems, policies, processes, and procedures for ICT security will be compromising.

The sample size at the end was eleven (11) for interviews. The researcher can assert the sample size as sufficient since data saturation was reached. From the eleven (11) semi-structured interviews saturation was reached in interview number seven. However, the

researcher conducted all the remaining interviews in full with the expectation to solicit new information and to fulfil sample size requirement.

## 3.4 Data Collection

This section describes in detail how data was collected with reference to data collection techniques, sources, access to participants and material. There are different data collection techniques for qualitative research and interpretive approach, however, most consider interviews to be the preferred techniques (Myers, 2013; Walsham, 2006).

### 3.4.1 Collection techniques

The researcher used two modes for collecting data, primary source, and secondary source. Primary source denotes unpublished data specifically collected by the researcher from the people or organisations, through interviews, surveys, unpublished documents such as reports, and so on (Myers, 2013). The researcher chose interviews as a primary source because it renders tangible information. The advantage of interviews is that they permit the researcher to collect in-depth information from different people in different positions and situations (Myers, 2013) and make follow-ups where answers are not clear or participants misunderstood the question(s) as well as to observe their reaction in relation to the questions.

A secondary source is pre-existing data originally collected for another primary source and reused for another research study (Hox & Boeije, 2005), such as published surveys, journal articles, and so on. The secondary source was used to complement the primary source by enriching the limited research and data available regarding the research topic.

#### Primary data

The best suitable type of interview method used was a semi-structured, face-to-face interview because it can stimulate opinions and elaborations from participants as well as allow the researcher to make follow-up questions for clarity. These types of data collection techniques also enable the researcher to collect credible information to address the purpose

of the study. The researcher gave participants some freedom to express their views through 'open-ended probing' questions and answers allowed along the way, while simultaneously containing the interview with some critical set of questions (Myers, 2013).

Interview questions (Annexure D) were developed to respond to the main research question and three research sub-questions. The questions were premised on the five (5) core functions that address cybersecurity and cyber resilience, namely: Governance and Leadership, Identify, Protect, Detect, and Respond and Recover. The total number of interview questions were 47.

Scheduling of interviews was mainly dependent on the availability of the participants. The researcher exercised flexibility by rescheduling or requesting a suitable replacement where cancellations or unavailability of the primary participant occurred. Out of sixteen (16) scheduled interviews, five (5) interviews did not materialise. All interviews took place at the offices of the participants. At the beginning of each interview, the researcher gave a brief explanation about the research study, read participation information (Annexure B) and requested the participants to sign a consent form (Annexure C).

The researcher recorded all interviews with a digital recording device, except for one (1) participant who requested not to be recorded. However, all the participants' responses were documented. The recordings, after all the interviews, were moved to the researcher's laptop which has encryption capability and backed up in an external encrypted storage device. All participants were asked the same interview questions in the same order to elicit and correlate data in a consistent set of data as well as avoid bias. All interviews took between 60 and 90 minutes.

**Secondary data**

The researcher obtained secondary data in the form of an unrefined survey report and survey raw dataset collected through survey questionnaire by a third-party. The latter was a joint project between two (2) organisations which are part of the cybersecurity community with the parties being a national government department and a research institute. The

objective of the survey was to determine cybersecurity readiness baseline across various sectors in South Africa, which included SAPSOs located in the Gauteng Province.

The secondary data survey's questionnaire used similar sets of questions used for the interviews by the researcher, which were based on the five (5) core functions of cyber resilience. The third-party collected the data between January 2017 and September 2017 and there were 83 respondents across South Africa, mostly security managers who work in the cybersecurity or related field. Eleven (11) of the 83 respondents were from the public sector in the Gauteng Province. Out of the eleven respondents, one (1) survey questionnaire was incomplete, therefore making a total of ten (10) respondents. The third-party conducted an online survey using a tool called Four Eyes.

### 3.4.2 Pre-testing

The researcher first drafted the interview questions and the questionnaire and then pre-tested with two "out of target population" participants with expertise in the study field. The purpose of pre-testing was to simulate the real interviews and the two participants made assessments and recommendations to ensure the questions were objective and that they did not violate ethical issues.

## 3.5 Data Analysis

This section describes the processes used to analyse raw data collected from different sources, that is, (i) interviews as a primary source and (ii) survey as a secondary source to answer the research questions. Data analysis is a critical part of the research because it allows the researcher to – from the huge amount of data collected – reduce, convert, and interpret to make sense out of the data (Myers, 2013). The researcher noted that data analysis is an ongoing process, therefore emerging data along the way was considered.

### 3.5.1 Primary source: semi-structured interviews

Interviews were transcribed, and depending on the time of the interview, transcription took about 5 to 7 hours per interview. This is because the researcher had to listen carefully to the participants' responses to capture them accurately. Re-transcription was also conducted to verify the accuracy of the first transcripts and took about 1 to 2 hours per interview. The researcher used a trial version of MAXQDA12 to transcribe the recorded interviews. Analyses of the transcribed data followed three phases: data reduction, data reorganisation and data interpretation (Roulston, 2014).

### 3.5.2 Secondary source: a survey

The survey's raw dataset that was received by the researcher from the third-party was in the form of a comma-separated values (CSV) format. The researcher used Microsoft Excel function "Text to Columns" to arrange the comma delimited data into columns. The columns were according to the survey questions. Subsequently, the researcher extracted data for the SAPSOs in the Gauteng Province. The researcher then separated the data into ten (10) documents, using Microsoft Word to analyse for each participant.

### 3.5.3 Coding

The researcher started by reducing transcribed data using the qualitative data analysis method of coding to establish what is important to address the research topic and questions (Ravitch & Carl, 2015). In coding, a code can be a word or symbol that is applied to characterise or condense a sentence, paragraph, or colour code entire text such as an interview. When using coding, the big collected data is labelled and then organised into certain categories or themes (Myers, 2013). The fundamental tasks associated with coding are (Ryan & Bernard, 2000):

- **Sampling** – initial reading through data and the selection of text to be analysed.

- **Identifying themes** – split the text into sections and then deriving themes from them, or maybe from the literature as well.

- **Building codebooks** – arranging a hierarchical list of sections with code and define them.

- **Marking texts** – allocating code into units of texts.

- **Constructing models** – identifying how the themes, concepts, beliefs, and behaviours are linked to each other.

- **Testing models** – assessing the model developed in bullet point 5 on a different or broader scale of data.

The data set comprised 2 primary documents: 11 interview transcripts and a survey transcript (raw data set). The researcher started by creating a list of pre-set of codes, deriving them from research questions, literature, and interviews in preparation for the actual coding. This process recorded 256 codes. The researcher went through the codes to determine duplicates and redundancies to eliminate them as well as overlaps to cluster them together. The process reduced the codes to 69.

The next step was for the researcher to reorganise the data and codes into themes.
The researcher during data transcription and rereading through literature identified twenty-five (25) themes, and these themes were revised during identification of codes and condensed into six (6) major themes, which correlate with the cyber resilient core functions used in this study. The researcher sorted the codes according to prospective themes, and during this process, codes were reduced to a total of thirty-seven (37).

This final code and theme process were done using Microsoft Word and Microsoft Excel. The researcher used a qualitative data analysis (QDA) software, Atlas.ti function auto-coding, to search for keywords from the final codes on all the documents. The codes were colour coded according to themes. This coding process created quotations and codebook.

## 3.6 Triangulation

The concept of triangulation is regularly discussed in qualitative research when there are concerns about issues of quality (Flick, 2007). Flick (2007) further states that triangulation is "sometimes discussed when qualitative research is combined with quantitative approaches in order to give its results more grounding". Triangulation, as described by Olsen (2004) is the process of combining data and methods so that various perspectives and points of views provide further information to explain the topic.

Clark & Ivankova (2016) state that triangulation is a logic used for mixed methods that allow the researcher to draw valid inferences based on comparing findings from qualitative and quantitative methods for convergence and divergence. Olsen (2004) argue that triangulation is not aimed simply at validation, but it is aimed at broadening and strengthening understanding of the research.

The concept of triangulation can be applied in four (4) forms according to Noaks & Wincup (2011), and the forms are defined below in Table 3-1.

**Table 3-1:** Forms of triangulation. **(Noaks & Wincup, 2011)**

| Form of triangulation | Definition |
|---|---|
| Methodology triangulation | Involves combining different methods to collect data |
| Data triangulation | Involves collection and using evidence from a different type of data sources on the same topic |
| Investigator triangulation | Involves the collection of data by more than one researcher |
| Theory triangulation | Approaching data with multiple perspective and hypothesis in mind |

Due to the nature of this study as well as limited research regarding South African public sector and cyber resilience, the researcher adopted two (2) forms of triangulation, that is, data triangulation and methodology triangulation. This was done to strengthen and get more understanding of the study, increase confidence, and confirm the validity of the thematic

findings; and to overcome limitations from the primary source. The triangulation was to compare the thematic findings acquired from the qualitative semi-structured interviews, the primary source and the statistical results acquired from the quantitative surveys, the secondary source to strengthen the research findings.

## 3.7 Ethics

Adherence to ethical requirements is very important because it does not only protect the participants, but it also protects the researcher as well as the reputation of the university. In this regard, the researcher submitted to the Ethics Committee of the Faculty of Engineering, Built Environment & IT all the documents that were used for this study to confirm that they comply with the ethical standards and for the committee to grant approval (Annexure E) before collecting research data. This was done to address any ethical concerns that may be encountered throughout data collection. The said documents were as follows:

- Ethics application form,
- Research proposal,
- Researcher declaration letter,
- Research Informed consent form template
- Interview questions,
- Permission letter (with organisational letterhead) from each participating organisation and
- Participation information.

Furthermore, and since other public organisations regarding the study as sensitive, the research as subjected to security screening and the completion of non-disclosure forms.

Prior to each interview, the researcher orientated participants by explaining the purpose of the study, ethical considerations, participation information, and informed consent form. The researcher clearly explained to each of the participants that their names and that of the organisation will remain anonymous and confidential because they will be identified by

codes. The researcher also informed the participants that they have a right to withdraw from the interview at any time and that the interview will be audio recorded only with their permission. A consent form (stating privacy, confidentiality, anonymity as well as the use of audio taping) and an agreement was signed by both parties and a witness prior to each interview. Each participant was given a copy of the informed consent form.

During the preparation for the interviews, personal information was collected because the researcher was provided with the names and contact details of the participants to schedule the interviews. The participants, in interview memos – both hard copy and softcopy, are referred using alphabet for an organisation and number for a participant, for example, A1, A2, B1, and so on. However, all the identities, participants, organisations, contact persons from the organisation remain anonymous, confidential, exclusively stored on an encrypted hard drive of a password protected laptop and are thus strictly in the control of the researcher.

## 3.8 Problems Encountered During the Study

The study initially envisaged conducting between 24-28 interviews with 14 government organisations. The aim was to interview two participants per organisation, that is, one senior management such as CIO, GITO or IT Manager and one IT Security, Cybersecurity, or information risk practitioner. Subsequently, requests to participate letters attached with information for participation and informed consent form were sent to the accounting officers of each organisation. Most organisations were reluctant to participate and did not grant the researcher permission to conduct the study. Several attempts to persuade them did not yield positive results.

Permissions were granted after a prolonged persistence of follow-ups by the researcher through emails and telephone calls, and only four (4) organisations, that is two (2) national departments and two (2) state-owned enterprises, granted the researcher permission to conduct the research study.

The researcher then sent 21 additional invitations (to other government organisation that were not invited before), but only 4 municipalities granted the researcher permission to conduct the research study. This is also after a long persistence through emails and telephone calls. The researcher continued to make follow-ups with the organisations that did not grant permission. Some organisations did not respond at all, and some stated that "the research is sensitive". This is an example of the nature of the response from one of the organisations. "Due to the general confidential nature of the COMPANY's information, I am not inclined to permit the research using internal information."

The overall invitations sent were to 35 organisations. If all 35 organisations granted the researcher permission, therefore the total could have been 70 participants. It took about 3 to 15 months to at least secure permissions from the 8 organisations. The delay highlighted the sensitive nature of this study. The researcher, after receiving permission to conduct interviews from the Faculty Ethics Committee, immediately sent requests for interview appointments to the 8 organisations, that is, requesting two (2) participants, one (1) at a senior level and one (1) practitioner.

However, the researcher experienced challenges again even after interview dates and times were agreed to. These include, unavailability of participants, (i) on two occasions participants cancelled on the day of the interview and (ii) on three occasions, participants were not available on the day and time of the interview. The participants could not find suitable dates or replacements. In some cases, participants did not respond to follow-ups. These challenges resulted in a sample size considerably smaller than originally envisaged, that is, the number was reduced from 16 to 11 participants.

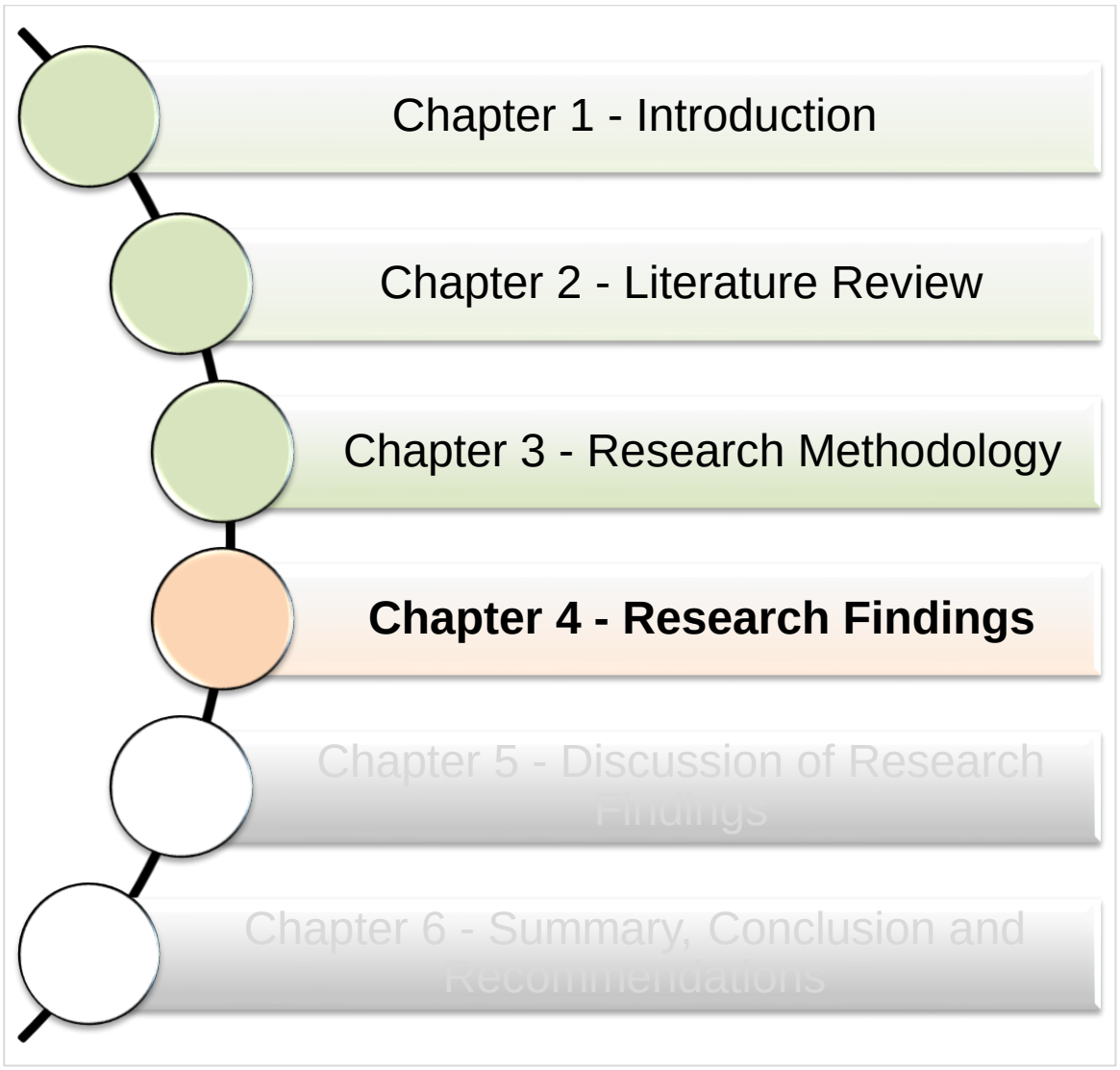
## 3.9 Conclusion

This chapter discussed the research methodology that the researcher, taking into consideration the limitations brought by the study. The researcher adopted an interpretive qualitative research approach. The research design method was also informed by the limitations and non-probability methods with which purposive technique was used for data

collection. The researcher used semi-structured interviews as primary data sources and survey report as a secondary data source.

Coding technique was used for data analysis, utilising of a software data analysis. Two forms of triangulation were adopted, comparing the qualitative primary source and the quantitative secondary source for the validation, and strengthening of research findings as well as broadening and strengthening the understanding of the research topic. The chapter showed the researcher as fully adhering to ethical academic requirements. Limitations and challenges experienced during the research study were also highlighted.

# 4. CHAPTER 4 – RESEARCH FINDINGS



## 4.1 Introduction

This chapter presents in detail the findings of the research study that was conducted in the SAPSOs in the Gauteng Province. The data was collected by means of semi-structured, face-to-face interviews as a primary collection instrument and a survey raw data collected using online questionnaires as a secondary source instrument. The interview questions were designed to respond to the research topic and four research questions which, were based on the following core functions that address cyber resilience and effective cybersecurity:

- **Governance and Leadership –** roles and responsibilities of the executive management to set a tone to establish a resilient organisation.

- **Identify** – identifying cybersecurity risks immediately to systems, data, and capabilities.

- **Protect** – protecting the environment against the risks and/or threats by developing appropriate security systems.

- **Detect** – detecting any information security compromise and network anomalies as well as conducting continuous proactive and real-time monitoring.

- **Respond** – responding quickly and automatically to attacks as well as conducting analysis, planning, mitigation, and improvements.

- **Recover** – recovering after a cyber-attack to ensure the integrity of data, maintaining cyber resilience, and recovering capacity and capability.

Furthermore, the interview questions helped the researcher to focus on the research objectives described in Chapter 1:

- To investigate the cyber resilience of the information systems of the South African public sector organisations.

- To investigate the cyber risks that South African public sector organisations may face.

- To investigate the current cyber threats and the impact of cyber-attacks in the South African public sector information systems.

- To propose measures for the South African public sector organisations to mitigate cyber risks.

The research findings are structured into two parts, Part A deals with interviews as the primary data source and Part B deals with the survey raw data as the secondary data source. Both parts A and B are structured according to the themes as coded in Chapter 3.

## 4.2 Demographic Information

### 4.2.1 Primary data

The primary data is from eleven interviews conducted from eight organisations in the Gauteng Province. The participants were mostly in managerial or supervisory positions in Information and Communications Technology (ICT), ICT Risk, and Corporate Risk Management (CRM) divisions with responsibility functions in ICT security or risk management.

The requirements for participants to participate in the interviews was to have knowledge and background in Information Security, ICT Security, Cybersecurity and Risk Management. Reference to participants was done using an alphabet to denote an organisation and a number to denote a participant, as shown in Table 4-1 below.
The reason for not declaring the names of organisations is because the research topic was considered to be sensitive, therefore the research study was conducted as an anonymous study. An agreement between the researcher and the participating organisations was that information regarding the participants was to be kept confidential.

**Table 4-1:** Demographic information for primary data

| Entity | Number of departments | Participants |
|---|---|---|
| National department | 2<br>(D and E) | D1<br>D2<br>E1 |
| State Owned Enterprise | 2<br>(A and G) | A1<br>G1<br>G2 |
| Municipality (metro/local) | 4<br>(B, C, F and H) | B1<br>C1<br>C2<br>F1<br>H1 |

### 4.2.2 Secondary data

The secondary data, in the form of a survey raw data, was received from a third-party organisation. The survey involved most sectors in South Africa, and this study was focusing only on the public sector organisations in the Gauteng Province (GP). Survey responses of the public sector organisations in GP were extracted from the survey raw data and resulted in 11 organisations. According to the survey raw data, respondents worked within the cybersecurity field, most of them were IT or cybersecurity managers, and they were required to have basic knowledge and background in cybersecurity to answer the survey questionnaire. The organisations, as listed in Table 4-2, were as follows:

**Table 4-2:** Demographic information for the secondary source

| Entity | Number |
|---|---|
| National departments | 2 |
| State-Owned Enterprises/parastatals | 9 |

# PART A: FINDINGS: INTERVIEWS

## 4.3 Governance and Leadership

Cyber resilience requires good governance and strong leadership by executive management to implement all the core functions. The objectives of including this core function in the interview were to assess (i) the organisation's status with regard to the establishment and approval of the cybersecurity strategy; (ii) if the executive management understands the roles and responsibilities required in achieving cyber resilience; (iii) the extent to which the executive or board is aware of cyber risks that their organisation may face; (iv) the degree to which cybersecurity roles within the organisation's cybersecurity strategy has been aligned to the organisational strategy; (v) whether the organisation has considered evaluating its cybersecurity strategy against international standards and guidelines such as the NIST Cybersecurity Framework; and (vi) a possible partnership across all sectors.

### 4.3.1 Cybersecurity strategy

To defend against the rapidly evolving cyber threats and cyber-attacks, the executive management needs to ensure that they have a solid foundation for cybersecurity and cyber resilience. This foundation begins with the drafting and approval of a comprehensive cybersecurity strategy that addresses specifically their information systems. The cybersecurity strategy must not only be drafted, but it is critical that it is approved as well as aligned to the business strategy. The participants were asked if their organisations have an approved cybersecurity strategy.

Majority of the participants indicated that their organisations do not have a cybersecurity strategy in place and instead they utilise other IT or security-related documents such as policies, frameworks, and procedures. Comments stated below:

*"No specific strategy as yet in place but there are policies and procedures in place that their organisation uses."* (A1).

*"The policies are in line with IT governance and not so much about IT security. From a strategic perspective, goals are not in place for cyber. The only approved policy is a security policy."* (B1).

C1 and C2 said they have an ICT strategy or framework, which has expired and needed to be reviewed.

*"There is no cybersecurity strategy, but we had an IT strategy that expired last year." (C1).*

*"No, we don't have a cybersecurity strategy, but we are in the process of developing it with CSIR. We had ICT Framework that needs to be reviewed."* (C2).

D1 indicated that they have a cybersecurity strategy in place but, D2 disagreed with D1's assertion.

*"Yes, we have an ICT security policy. We don't have a separate cybersecurity policy. There was an initiative to do the cybersecurity strategy but it is assumed is there since the policy cannot be there without the strategy"* (D1).

E1 mentioned that they use a combination of approved IT strategy, ICT security policy, threat and vulnerability management and procedures; G1 indicated that:

*"No, we don't have a cybersecurity strategy, but we have engaged with CSIR to guide us, and we are in the process of starting it. In the meantime, we have in place IT Strategy, Information Security policy, IT policy, Acceptable use policy and other security-related policies."* (G1)

Two participants, F1 and H1, stated that they have a cybersecurity strategy but, they do not specifically call it cybersecurity strategy. Comments stated below:

*"No, we don't have a cybersecurity strategy, but we have an approved Security strategy that includes ICT infrastructure (i.e. networks and systems infrastructure, IT Security Policy)"* (F1).

*"We have a strategy, but we don't call it cybersecurity strategy, we call it information security strategy and it includes cyber-related controls"* (H1).

There was a follow-up question to the participants as to what *are the future plans in having an approved cybersecurity strategy?* Participants A1, C1 and G1 indicated that they have engaged with the South African research institutes, Council for Scientific and Industrial Research (CSIR) to guide them (C1 and G1) and A1 indicated that they have a Memorandum of Understanding (MOU) with CSIR.

*"…* and that the MOU *will dictate also or support us so that we can tap at the expertise of the CSIR research group and we are currently engaging with them so that we can at the end have a holistic view and strategy that will now inform policies and procedures even further."* (A1).

According to D2, their organisation had the initiative to carry out the cybersecurity strategy but he was uncertain if the strategy was completed or not. B1 stated

*"At this point in time the strategy to extend security concerned has lapsed and there are no plans in place for drafting a cybersecurity strategy."* (B1)

Furthermore, the participants were asked whether their organisations have aligned cybersecurity roles against the business strategy, regardless of the status of the cybersecurity strategy. Most of the participants said that the roles are aligned to their business strategy, however, not as cybersecurity roles but as defined according to their respective policies, strategies, frameworks, or other related security documents they used.

The participants believed that they did not have to wait for the cybersecurity strategy to be drafted or finalised to determine the roles to protect their organisations but preferably make

use of the available tools and best practices that are already in place (A1, D1, D2, E1, F1, G1, G2, H1). One of the participants engaging with CSIR mentioned that the cybersecurity strategy will be aligned with the business strategy. The comments are illustrated below:

*"Yes, it is aligned because we need to protect the business systems such as financial systems."* (A1).

*"The IT strategic plan is aligned to the business strategy. We will also align the cybersecurity strategy to the business plan."* (G1).

"Yes, it is aligned to the Business Strategy and a framework that implements the business" (H1).

The remainder of the participants stated that there is no alignment of their respective policies, strategies, frameworks, or other related security documents to the business strategy mainly because there was no business strategy (B1, C1, C2) and moreover, they take no account of their ICT Security strategy since it has expired and has not been reviewed (C1, C2).

*"No, don't, even if there is an enterprise architecture. Therefore, if there is no enterprise architecture, then there won't be security architecture. The approved security policy in place is the only policy that exists and not aligned to business strategy."* (B1).

*"Since there is no Cybersecurity or OT strategy in place then, it is not."* (C1)

### 4.3.2 Executive management

Executive management should be concerned about the cyber resilience of their organisations and their information systems. The executive management needs to be knowledgeable of the cyber risks facing the organisation. In this regard, an effective cyber resilience requires the executive management's commitment, understanding of the roles they need to play and their responsibility to oversee development and implementation of a cybersecurity strategy and cyber resilience framework/programme.

On the question of the executive management understanding their roles and responsibilities, several participants stated that the executive management understands their roles and responsibilities regarding cybersecurity matters and it has been validated through their continued support of the structures responsible for ICT security or cybersecurity. They indicated that the executive management has defined roles in executive management level relating to either of the following: cybersecurity, ICT security, information security or IT risk. Their roles differ for each organisation, with some organisation having defined roles, including Chief Information Officer (CIO), Chief Information Security Officer (CISO) and Chief Risk Officer (CRO). This is illustrated by the interview responses below:

"*Yes, and their understanding has been validated. I am sure they do because we follow the King 3 / King 4. This whole initiative for Cyber approach actually came from the CEO with support from the board. So, it is really driven from top-down and I think that is why we have such a fruitful approach to the cybersecurity concept based on the buy-in from the top."* (A1).

*"Yes, and their understanding has been validated because were reported directly to them and issues relating to ICT security or cybersecurity is part of the report to them."* (D2).

*"Yes, and their understanding has been validated because they are driving it and supporting IT to consult external experienced organisation."* (H1).

Some participants indicated that although the executive management is informed about matters relating to cybersecurity; understanding of the roles and responsibilities is assumed because the participants do not see the support from the executive management. A comment from participants below:

"*No, I do believe they understand that cyber exists. This is a new EXCO. There is no full backing, and they don't understand the importance of cybersecurity, e.g. antivirus is at borderline/weak, gone to tender last year and funds hasn't been made available and tender not approved*." *(B1).*

*"They have been informed about cyber risks because it's one of the top risks and understanding is assumed."* (C2).

*"Not specifically, there is still a challenge when it comes to cybersecurity. They have been informed and understanding is assumed as partially. The Information Security Strategy includes some of the roles and responsibilities of the accounting officer, ISO, etc." (*H1).

Few participants believed the executive management or the board do not understand their roles and responsibilities.

*"No, because it is a new administration and we haven't had a chance to engage with them. This will be addressed during a strategic meeting soon."* (C1).

*"No, they don't understand."* (D2).

On the question of whether the executive management is aware of the cyber risks. Several participants mentioned that the executive management is aware of the cyber risks because cyber risks challenges are reported to the executive management. Comments from participants are indicated below:

*"Yes, there is an executive audit and risk committee to which the CIO reports to on a monthly bases and that goes to the board as well."* (A1).

*"They are aware of the cyber risk and when it comes to reporting we have a risk register separate from the report, and cyber risks are part of it. It is presented to EXCO." (D2).*

*"They have been informed about cyber risks because It's one of the top risks." (C2).*

Some participants were not sure if the executive management or the Board are aware of the cyber risks and some of their responses are as follows:

*"Not specifically and awareness is assumed because they are more financial, corporate and legal side. Yes, they are aware of the issues that are currently experienced on the network, e.g. Ransomware attack was disclosed to them."* (B1).

"*Not specifically cyber risks but IT risk and awareness is assumed*." (E1).

### 4.3.3 Assessing against NIST Cybersecurity Framework and other international standards

Effective cyber resilience requires organisations to be assessed against international standards, frameworks, methodologies, and other best practices such as the NIST Cybersecurity Framework because they can assist in improving cyber risks management and cyber resilience. The NIST Cybersecurity Framework is based on risk management, it is measurable and it enables organisations to assess and manage cyber resilience by assisting them to: determine current cybersecurity capabilities, set goals for a target level of cyber resilience and establish a plan to improve and maintain cybersecurity and cyber resilience (ASIC, 2015).

Participants were asked if they have considered assessing their organisations against the NIST Cybersecurity Framework or any standards or methodologies that can be used to assist the organisation to improve their cyber risk management. The participants indicated that they are assessing their organisations against at least one (1) international standard. Some of the participants indicated that they are assessing not specifically against the NIST Cybersecurity Framework alone, but against a combination of frameworks or standards or methodologies such as NIST, ISO27000 family, COBIT, ITIL, Sharewood Applied Business Security Architecture (SABSA) as well as the South African Minimum of Information Security Standards (MISS). Below are some of the comments by the participants:

*"Yes, but not really against one specific framework such as NIST but against a combination of frameworks and standards and methodologies, such as COBIT, ISO27001 and NIST".* (C1*).*

*"Yes, but not really against one specific framework such as NIST but against a combination of frameworks and standards and methodologies, such as our framework is based on 3 key international standards: SABSA (Sharewood Applied Business Security Architecture) framework*, ISO 27000 family, NIST framework." (H1)

Several of the participants indicated that they are assessing their organisation against only one specific standard, the ISO27001. The participants' comments are illustrated below:

*"Yes, only against an ISO27001. The assessment is provided by external service providers."* (E1).

*"The Information Security policy is aligned only against a specific standard (ISO27001)."* (G1).

*"Yes, we are aligned, and we have adopted ISO27001."* (D1)

## 4.4 Identify

This core function pertains to the development of an organisational understanding to manage cybersecurity risks to systems, assets, data, and capabilities (NIST, 2017). The interview questions for this function focused on the following categories: asset management; risk assessment; and risk management.

### 4.4.1 Asset management

Asset management is fundamental to risk management. It provides direction to the establishment and management of the inventory of essential assets (information, technology, people, and facilities) that supports critical services (Del Giudice & Wilkinson, 2016). This category aimed at investigating processes to identify the organisations' critical functions and information or business assets and that the delivery of those critical functions

and assets are supported by IT. It also investigated the assessment of the sensitivity and integrity of the data required for the delivery of critical functions.

The participants were asked if they have processes in place to identify critical functions and processes; information or business assets that are essential. In addition, the researcher asked if there was support from IT structures. Most participants mentioned that there is a process in place to identify essential assets for critical functions or services. However, it is not the responsibility of the participants' functions, but the process is the responsibility of other business functions within the organisation like IT risk or Business continuity management.

Furthermore, some participants indicated that it is also a responsibility of the specific function or division to inform IT or other structures responsible to identify critical assets and services. The participants indicated that, although they are not responsible for identifying the critical assets, they are supporting the critical business functions and processes. The participants' reference to essential assets related to information and technology and not people and facilities. One participant was not sure if there was such a process or procedure in the organisation. Comments from the participants are presented below:

*"…the process we have we say to business if you have a system you think is critical, it should be disaster recovery, and then we can say this is a critical business function, it is not for us to tell business what is critical or not, they have to tell IT. STAFF: there are no people taken as critical…. IT provides all support but once it has been identified that this is a critical system, obviously we [are] part [of] necessary security measures."* (C1).

*"Business continuity management looks at the critical applications of the organisation and identify all those critical applications. … From IT side, we'll look at the recovery and back-up of all critical applications … Yes, we are supporting that, because what we do have a service catalogue and all critical functions are listed and this is annually verified." (D2).*

*"Yes, this activity has been undertaken by enterprise risk but it is not considered a routine, repeatable process … we do support the enterprise risk management, part of the IT steering committee and audit committee and this is annually verified" (H1).*

The participants were asked if they assess data sensitivity and integrity. Some participants mentioned that they do not assess the sensitivity and integrity of data because they do not have a data classification system. Several participants said they do assess the sensitivity and integrity of data, however, most of them failed to elaborate on their data classification process. As *per* the researcher's observation, the participants were not convincing that they assess data integrity and sensitivity. Most of the precipitants indicated that data classification should be the responsibility of the owner of that data and not IT.

*"No assessment, we don't have a data classification scheme, it is something that is subjective." (C2).*

*"This is very difficult because we have different departments that handle different data. Verification of that data and whether that information is classified is done by the department owning that specific data, and not the IT Security division." (B1).*

### 4.4.2 Risk assessment

Risk assessment refers to processes that identify cybersecurity risks to an organisation's essential assets, critical services and functions, and external services providers that could have a negative impact on the delivery of critical services (NIST, 2017). This category investigated what cyber risks (threats and vulnerabilities) the organisations are exposed to; whether hardware and software vulnerabilities are identified, documented, and remediated; if the organisations have considered the cyber resilience of vital third-party providers or clients; and if threat information informs protection activities.

Regarding the identification of the cyber risks that organisations may be exposed to, most participants indicated that they look at all the cyber risks that are out there and there was no elaboration as to why all the cyber risk but not specifically identifying the cyber risks that the

organisation may face. Few participants indicated that they look at the cyber risk that they might be exposed to, based on the organisation's vulnerability.

*"We look at the cyber risks we may face, i.e. based on the organisation, we look at the weakness of the business and infrastructure." (G1).*

*"Yes, we use information security so we look at all cyber risks that might affect the organisation." (H1).*

Regarding hardware and software vulnerabilities, the participants indicated that they have an established process, which includes identification, remediation, and documentation, for prioritisation of critical vulnerabilities. However, only few participants mentioned that they are looking at both hardware and software vulnerabilities, whereas most of the participant mentioned that they are looking at only software vulnerability identification.

*"We have suppliers that look after and provide our hardware and software, so we also have in place SLA with them because obviously, they are the ones who should know about these things …. It is documented from our side." (A1)*
*"Yes, and there is an established process for prioritisation of critical vulnerabilities, but for software only." (E1).*

*"There is an established process for prioritisation of critical vulnerabilities but remedial action is a challenge because our environment is old, so some of the things we cannot do away because of the old applications that are still running in the environment." (C2).*

One participant, (B1), mentioned that their IT environment is old, and therefore, they are experiencing challenges with remedial actions. Three participants indicated that they are lacking in documentation. (C1, D1 and E1).

*"Yes, and we identify critical vulnerabilities and remediated, but it is not documented. This is done partially." (H1).*

Organisations may be made vulnerable to cyber risks through weak cyber resilience of vital third-party service providers (for example contractors and suppliers) and clients (ASIC, 2015). Most of the participants mentioned that they have not considered reviewing the cyber risk and cyber resilience of the third-party providers. Few participants indicated that they do consider third-party cyber risks. Responses are indicated below:

C1, C2, D1, G1 and H1 indicated that they have never considered it. D2 and F1 indicated that they did not consider it, but relied on security screening of the third-party service providers.

"No, we have service providers that are actually within the organisation as vendors, as an organisation we don't' have control over what is happening in their network and be able to evaluate their systems. There is a policy in place for that but the enforcement of it is questionable or non-existent." (B1).

*"Yes, Part of the ISO 27001/15 they task you to make sure you have competence service providers. Part of the organisation tender specification and requirements is that the organisation must have proof of their strategies and resilience and that they can deliver the services as requested." (A1).*

*"Yes, the vital third-party is stationed in the organisation, i.e. on-site for the duration of the contract (3 years). We work with them, we do report, we check everything, it is an auditor's requirements." (F1).*

Conducting cyber threat intelligence can assist and improves the organisation's capability to identify, detect, and respond to cyber threats. Organisations can produce their own cyber threat intelligence, and/or they can receive it from third-party vendors, information sharing forums and sources. Most of the organisations specified that they make use of the cyber threat intelligence to inform protective activities. The cyber threats intelligence is either conducted internally or received from third parties. They further indicated that information received from third parties would provide them with different perspectives on cyber threats.

C2 indicated that they do not utilise threat intelligence to inform protection services. Some of the responses are illustrated below:

*"Yes, threat analysis is done internally and produce our own threat intelligence report that is presented at the risk management committee meetings." (B1).*

"*Yes, part of it but most of the time we look at what it is coming to us, although the intelligence is out there, they can tell us this is what is happening and provide solutions as well. We subscribed to a service that provides the threat intelligence report. But we also look at what our controls tell us and produce our own threat intelligence. We process multiple sources* "(C1).

*"Yes, we process multiple sources and produce our own threat intelligence. We are also registered with cybersecurity intelligent network." (F1)*
*"No threat intelligence is done, at the moment we do patch management, dependent on OEMs." (H1).*

### 4.4.3 Risk management

Cyber resilience risk management refers to the processes that identify, analyse, and mitigate cyber risks to critical assets and services that could have a negative impact on the delivery of critical services (NIST, 2017). This category aimed at investigating effective risk management practices in place to address cybersecurity risks and the effectiveness of the implementation of these practices is measured. Whether organisations have considered if cyber risks are well integrated into normal business risk management and procedures.

Organisations are required to have effective risk management in place to deal with cybersecurity risks. Participants mentioned that they have risk management in place, however, the risk management in place focuses not uniquely to cybersecurity risk, but on organisation-wide risks. The ICT and cyber risks are integrated into the organisational risk management system. Several participants indicated that risk management is the responsibility of one or more units within the organisation, for example, risk management unit, ICT governance directorate or internal audit chief directorate. Moreover, participants

mentioned that they make use of the risk register to document risks and actions, that is, either a corporate register with cyber risks as part of it or ICT risk register aligned to corporate register.

*"Yes, we do have risk management department from the organisation perspective and I know IT risk management falls into there ... from the risk management perspective, we have to identify the risks ourselves, and we are also measured as far as our performance is concerned against those risks. We'll specify the cybersecurity threats, and we will have mitigating tasks. … We have also to provide proof of portfolio of evidence. We've got a risk register department, i.e. internal audit, they actually handle the risk register which covers everything including cybersecurity." (B1).*

*"Yes, we do have a security unit, corporate governance, which looks at the risk from the organisation's perspective and ICT governance which looks at the ICT risk. There is an Audit risk committee that looks only at the ICT risks, there is a MEMCOM as well that looks at ICT risk. We have an ICT risk register that is separate from the corporate risk register but it is aligned to it, and these are well documented and understood." (D2).*

Risk management for it to be successful, the effectiveness of the implementation of risk management activities need to be measured to reach the desired goal and requires to be reviewed regularly. Several participants indicated that they measure the effectiveness of the risk management activities indicated in the risk register. Some participants said that they have not considered measuring the effectiveness.

*"…. the audits that they will be conducting they will be informed by this strategic risk, if they happen to come for that audit, they will be assessing the effectiveness of the controls we said they are in place for that risk. Audit might be once a year and there might be follow-ups if there are audit findings that were raised. We report monthly for those audit findings. Yes, and effectiveness is regularly in audit reporting" (C2).*

*"I do not think we are at the mature level where we measure." (A1.)*

## 4.5 Protect

This core function pertains to the development and implementation of appropriate safeguards to ensure delivery of critical infrastructure services as well as to support the ability to limit or contain the impact of a potential cybersecurity event (NIST, 2017). The interview questions for this function focused on the following categories: identity management and access control; data security; information protection processes and procedures; and protective technology; awareness and training.

### 4.5.1 Identity management and access control

Identity and management and access control refer to security measures that limit access to organisational systems and data, and related facilities to authorised users and is regularly managed (NIST, 2017). This category is aimed at investigating if physical access controls and remote access controls are implemented, maintained, and monitored across the organisation's facilities.

Organisations need to implement physical access controls to restrict access to facilities only to authorised users, particularly facilities that have sensitive or critical data and ICT systems. This serves as a baseline for the safeguarding of information and resources. Regular maintenance and monitoring are critical. Participants stated that they have physical access controls in place, however, most participants indicated that they were uncertain if physical access controls are implemented across the organisation. On the matter of maintenance and monitoring, most participants were uncertain but believed that security controls are reviewed on a regular basis.

Furthermore, what was mentioned is that physical access control is the responsibility of another security division. Few participants mentioned the types of access controls in place to secure critical facilities such as data centres or server rooms. They use a combination of

these controls: electronic card, cameras, biometrics, and a register. Some comments from participants are presented below:

*"Our server room is protected with electronic card access and only a limited number of employees have access to that. IT Security works closely with Physical Security. They are reviewed and monitored on a regular basis." (A1).*

*"Yes, there are controls in place, we use biometrics and we've got restrictions to certain areas, e.g. no one, but from IT, can enter IT and we have a security guard at the door. There are cameras and biometrics as well as the data centre. I (as in IT) review it on a monthly basis with security report that who's got to the data centre, but only data centre and IT because within the organisation, the biometrics physical control is not handled by IT but it is handled by another security department." (B1).*

*"Yes, there are controls in place, at a medium level but there is no routine review process. There is a room for improvement" (H1).*

Remote access provides an ability to access the organisation's network from a remote location. Security controls must be implemented and managed to protect the organisation's network and information from unauthorised access. The participants indicated that their organisations make use of remote access and there are security controls in place, such as securing with VPN. However, most of the participants indicated that there is no routine for maintenance and monitoring process. Two participants mentioned that remote access controls are maintained and monitored on a regular basis.

### 4.5.2 Information protection processes and procedures

Information protection processes and procedures refer to implementation and management of security policies, procedures, processes, guidelines, and best practices protecting information systems and assets (NIST, 2017). This category aimed at investigating if information security policies are reviewed and updated to incorporate the latest standards; IT systems, processes and procedures are tested for cyber resilience; security capabilities

of third-party providers are assessed; there are sufficient resources to manage with cyber risks.

Information security policies and procedures that are regularly updated to integrate the latest standards and best practices assisting an organisation to use resources efficiently and effectively; make certain that appropriate security controls are implemented and properly managed; and moreover, the best practices are adopted. Ten of the eleven participants stated that they review and update information security policies and procedures to incorporate the latest standards such as ISO/IEC 27001 and this is conducted on a regular basis. One participant mentioned that they do not review or update information security policies and procedures. B1 and D1 stated that:

*"Yes, it's been done on a yearly basis, we completed the ICT policy and referring to ISO27001 and ISO27002." (B1).*

*"Yes, we have. The last time it was done was May 2017. These are reviewed on a regular basis." (D1).*

The assessment of IT systems, processes and procedures for cyber resilience provides with knowledge and understanding of the level of capability to identify and detect cyber risks; respond to cyber-attacks and recover to provide adequate services after an attack. The participants indicated that they have never tested their information systems for cyber resilience, but they conduct network systems testing such as vulnerability scanning and penetration testing.

Inadequate security controls of the third-party provider can make an organisation vulnerable to cyber risks. Therefore, it is important for organisations to assess third-party to determine the level of security competence. Some participants mentioned that they assess third-party security capabilities through security screening, security audits, and vetting or third-party self-certification. This process is conducted, in most cases, during a tender process. Screening is either conducted by a structure within the organisation or by an external service provider such as the State Security Agency (SSA).

*"Yes, we conduct audit of third-party service providers and this is done by internal audit, twice a year." (F1).*

*"We conduct security screening and vetting of all third-party security capabilities. This is done by the SSA and they provide security clearance. But if they are already vetted, we take their security clearance (from SSA). Assessment is done as and when it is required." (G2).*

*"Security capability assessment is self-certification" (E1).*

Several participants mentioned that they have not considered conducting assessments of third-party providers.

*"We do not assess third-party security capabilities, we only rely on Gartner reports or on the benchmark with other departments on what they have done, but we don't necessarily test their security" (D1).*

Effective cyber resilience requires sufficient resources to manage cyber risks and thwart cyber-attacks. Resources include, but are not limited to, workforce (employees and contractors) with appropriate qualifications and capability, technology, devices, and budget. Most of the participants indicated that they do not have sufficient resources to deal with cybersecurity or security-related matters. Furthermore, of the participants who said they do not have sufficient resources, a few said they are using contractors and four participants specifically stated that they have only one person responsible for ICT security.

*"No sufficient resources, the organisation only has one person to deal with ICT security, but we do have contractors" (C2).*

*"No sufficient resources at all, only one person dealing with ICT security and governance" (H1).*

A few of the participants mentioned that they have sufficient resources, including skilled staff.

*"…the CIO is working on the restructuring process but for now I think we have sufficient coverage of the infrastructure and staff is skilled" (A1).*

*"Yes, we do have resource and it is sufficient for the size of the organisation. No need to invest a lot in cybersecurity whereas you are not that much vulnerable" (G1).*

### 4.5.3 Data security

Data security refers to the protection of information, both in physical and digital format, from unauthorised access, use, modification, disclosure, and destruction to ensure and safeguard the confidentiality, integrity, and availability of information. This category aimed at investigating the method in which the data is stored, is backed up, and the availability of a data loss prevention strategy.

Data is the crown jewel of any organisation, it always needs to be protected. Data loss prevention (DLP), encryption and data back-up systems are critical data security measures. DLP is "the mechanism by which an organisation identifies their most sensitive data, where the data is authorised to be stored or processed, who or what application(s) should have access to the data, and how to protect the loss of sensitive data" (Devlin, 2016). Data can be protected using encryption, that is, data at rests – protecting data when it is stored on the device and data in transit – protecting data when it is transmitted across networks (private network or internet). Data backup system is about making copies of data in different formats, different storage media and in another location to restore the data after a data loss event. Backup can be done in different formats such as full, incremental, and differential backup; different storage media such as cloud, online, tapes, disks, and so on; and can be in different locations such as on-site and off-site.

**Data loss prevention strategy:** the participants mentioned that they do not have a strategy specifically for DLP. Majority of the participants mentioned that although they do not have a comprehensive DLP strategy; DLP is partial because it is covered in other security

documentation such as security policy or standard operating procedure and it is aligned to critical systems and data only. Few participants mentioned that DLP is none existent in their organisations.

**Data storage and handling:** the participants mentioned that users are encouraged to connect to and work on the organisation's network, rather than their PC, to make use of the central storage, the server(s). Several participants indicated that the data stored in the server(s) is considered critical, therefore it is encrypted at rest. Two participants indicated that they also encrypt data at rest for users of official laptops. Some participants mentioned that there is no data encryption. Some participants that use encryption indicated that sometimes data might not be encrypted as encryption can render the system very slow. Participants were not certain if encryption for data-in-motion and data-in use is applied.

**Data backups:** the participants mentioned that they perform data backups. Six of the participants indicated that they back up all the data and in multiple formats. Four of the participants indicated that they only back up data considered critical, in multiple formats. One participant indicated that they have a challenge in performing data back up because they do not have a proper backup system and funds are not made available to procure such a system. Furthermore, participants indicated that some critical data are not backed up because of the poor system.

### 4.5.4 Awareness and training

Effective cyber resilience begins with a cybersecurity awareness programme to all employees in an organisation, starting from the general workers to executive management. Cybersecurity awareness can make employees aware of the broad range of cybersecurity risks, thereby fostering a cyber-aware culture. Furthermore, for employees to carry out their ICT security and cybersecurity-related roles and responsibilities, proper training is required (NIST, 2017). This category aimed to investigate if the organisations have considered the level of awareness of cyber risks within their organisations; all staff are provided with basic cyber training and additional training is provided to higher risk staff.

Cyber risks do not exclusively emanate from outside of the organisation, but can emanate from within the organisation as well, and therefore, conducting awareness sessions and encouraging cybersecurity good practices is important. Most participants stated that cyber risks awareness within their organisations is low, attendance to security (IT, Cyber) awareness sessions is very low, staff are not familiar with policies and procedures and there is a lack of support for good practices. Comments from participants are stated below:

**"***Yes, we have security awareness seminars with all the departments and attendance is extremely low. Management has tried to enforce this but still, the turnout is very low" (B1).*

"Yes, at a low level, our staff are not well informed of policies and procedures and good practice is not encouraged. There is cyber awareness conducted once a quarter, attendance is very low" (D1).

Two participants stated that they have not considered assessing the level of awareness of cyber risks within their organisations and that security (IT or Cyber) awareness sessions have never been conducted. The two participants indicated that they are considering conducting awareness sessions.

*"No, but we are in a process of doing an awareness training, so we will see after that how is the level. Awareness has never been done before. We will have some roadshows as well in …" (C1).*

Cyber resilience and cybersecurity require a skilled workforce to counter cyber threats and cyber-attacks, especially those who work with information security, cybersecurity, ICT security and other related fields. To have a skilled workforce, proper training that comes with assessment and certification should be provided. Several participants mentioned that training is made available predominantly to IT and ICT security divisions, however, most participants indicated that no assessment is conducted on completion of training. Some participants mentioned that cyber training has not yet been offered to IT or ICT security staff, let alone all members.

*"Yes, they are able to attend any training updates or upgrade should the need require. Assessment depends on the type of course they attend, e.g. certifications assessment is expected. We do ask of the assessment when we fill in training requests: whether the supplier assessor's competencies, the type of assessments etc." (A1).*

*"Yes, not all of them, few IT staff have gone through cybersecurity training. Although training is made available to all staff, no assessment is conducted. We don't have IT Security personnel." (G2).*

Regarding if additional training is provided to high-risk employees. Most participants mentioned that they do not have "high-risk" employees. It is either everyone in the organisation is considered high risk or there are no high-risk employees at all.

## 4.6 Detect

This core function is with regard to the development and implementation of appropriate activities to identify the occurrence of a cybersecurity event (NIST, 2017). The interview questions for this function focused on the following categories of this function: anomalies and events; and security continuous monitoring.

### 4.6.1 Anomalies and events

Anomalies and events are about a timeous detection of irregular activities and possible impact of events (NIST, 2017). This category aimed to investigate if the organisations have established and maintained a baseline of network operations and expected data flow; and if there are network detection and monitoring processes and controls in place.

A baseline of network operations is basic settings, configurations and performance that represent a normal network behaviour of an organisation. The baseline of network operations enables the organisation to detect and identify network anomalies and thereby compare the data from the network baseline with the current network data. The baseline of network operations can also assist in developing a data flow map to depict how information

transits within the organisation and to external associations. Some participants mentioned that they have established and managed a baseline of network operations and expected data flow. However, from these participants, it was indicated that some participants have not reviewed the baseline setting after it was established. Some participants indicated that they review and verify the baseline regularly.

*"Yes, I have and get that out of my security report every single month. It is reviewed and verified annually" (B1).*

*"Yes, we undertook this process but a review has not taken place" (E1).*

*"Yes, we do our reviews for network twice a year, it is an audit requirement." (G1).*

Some participants said they are not sure if the baseline has been established because it is the responsibility of another division. Few participants said they have not established the baseline of network operations and expected data flow.

*"Not so sure, that should be done by the network division, but we do have a network management team…" (D1).*

*"I would say no because we do not have an enterprise architecture infrastructure environment in place" (A1).*

### 4.6.2 Security continuous monitoring

Security continuous monitoring is about the identification of cybersecurity events and verifying of the effectiveness of defensive measures through the monitoring of information systems at discrete intervals (NIST, 2017). Network monitoring and detection processes and controls are critical because they can identify, detect, and alert the organisation of cyber threats, cyber-attacks, or any attempts to compromise the network. There are controls in place such as proactive, automated intrusion detection system (IDS) and intrusion prevention systems (IPS); and appropriate monitoring of the network usage, which can always be compared to the network baseline as stated in section 4.6.1.

Several participants mentioned that they have network detection and monitoring processes and controls in place. The tools that are used automatically analyse all events in the network that can compromise critical assets and functions. Some participants indicated that analysis is done in a manual mode as well. Few participants specified that they have an automated system in place, but it only highlights anomalies and not much analysis is undertaken.

*"Yes, we do, we have systems in place, it is analysed by me, it is automated, it takes the most hits and it will put them into top ten. So, it is manual and automated." (B1).*

*"We have a security operation centre where we do monitoring of logs of all the servers and traffic in production. We have a third-party which analyses all events for us. They analyse, recommend and warn." (D1).*

### 4.6.3 Vulnerability assessments and penetration testing

Vulnerability assessment and penetration testing (VAPT) is a structured investigation and analysis of the security posture of the information systems (Gupta & Kaur, 2013). VAPT is a two-part process, vulnerability assessment (VA) and penetration testing (PT), that can be performed separately or integrated for better knowledge of security status. VAPT should be performed regularly.

**Vulnerability assessment (VA) –** VA is a process of scanning ICT systems to detect security flaws that can compromise the systems using various set of tools, either automated or manual. Participants mentioned that they perform vulnerability scanning. Most of the participants indicated that the executive management has knowledge of the vulnerability programme, whereas few participants indicated that they are not sure if their executive management is knowledgeable about the performance of vulnerability scanning. Two of the participants indicated that they perform VA internally as well as make use of the third-party for verification purposes. The frequency of undertaking VA ranges from weekly to three times a year, with one participant indicating that VA is performed on an ad-hoc basis.

*"Yes, there is a regular programme in place and executive is informed, it is done internally and third-party hasn't been used. Vulnerability scanning is done every single monthly" (B1).*

*"Yes, we have a rolling programme, agreed at senior executive level, both internal and third-party. Vulnerability testing with third-party is done once a year and internally not so sure" (D2).*

**Penetration testing (PT) –** PT is an authorised attempt to break into the organisation's ICT systems by exploiting the vulnerabilities in that system. Majority of the participants mentioned that they conduct PT programme. Four participants indicated that they use a third-party for PT. Few participants indicated that PT has not been conducted. The frequency of undertaking PT ranges from once a year to four times a year, with one participant indicating that VA is performed on an ad-hoc basis.

*"Yes, there is a regular programme in place, it is done internally and third-party hasn't been used because the executive is not in agreement of using an external specialist, it is costly, but I'll love to use them for verification - Vulnerability scanning is done every single monthly" (B1).*

## 4.7 Respond

This core function is with regard to the development and implementation of appropriate activities to act regarding a detected cybersecurity incident (NIST, 2017). The interview questions for this function focused on the following categories of this function: response planning; communications; and analysis.

### 4.7.1 Response planning

Response planning refers to "response procedures and processes that are executed and maintained, to ensure timely detection of cybersecurity incidents" (NIST, 2017). This category aimed at investigating if the organisations have an adequate response plan. The

response plan incorporates the business continuity plan and cyber incident response plan. Documented; regularly tested, reviewed, and updated; and clearly communicated response plans can be more effective (ASIC, 2015). Response plans can assist the organisations to restrain impacts should any cyber incidents occur.

Participants mentioned that they do not have an adequate response plan because it misses one of the following: it is not clearly communicated; and it either not regularly tested, reviewed, or updated. Furthermore, most participants mentioned that they do not have a cyber incident response plan (or cyber incident policy or cyber incident procedure as it is referred to by some participants) and business continuity plan incorporated as response plan, but they use the two plans separately. Some participants mentioned that they only have the business continuity plan, and with only one participant indicating that they do not have a response plan at all. Most participants indicated that they tested the plans, either separately or against each other. Few of the participants indicated that they have not tested the plans.

*"Yes. We have a separate disaster recovery plan and a draft business continuity plan. These have been tested separately within the last 12 months and it is assumed that they can work collectively, but these have not been tested against a cyber incident because it doesn't exist…." (E1).*

*"We have a cyber incidents process and not a plan. There is an existing business continuity plan available but is not with IT. but it has not been tested against a cyber incident." (C1).*

### 4.7.2 Communications

Effective, timely and proactive communication is a critical part of the response plan. Organisations need to have a communication plan in place as to how they will communicate and coordinate response activities with internal and external stakeholders; notify clients, employees, and law enforcement of incidents; information sharing with other organisations. This category aimed to investigate if the organisations have data breach notification and information sharing process in place.

### 4.7.3 Data breach notification

Data breach notification is with regard to organisations notifying their employees and clients that their personal and sensitive data has been compromised or exposed to risks, as well as notifying law enforcement agencies of all the data breaches and cyber incidents subsequent to a discovery by an organisation.

Six participants mentioned that they do not have a "formal data breach notification policy". However, the participants indicated that data breach notification is covered in other security documents such as Acceptable Use Information Security Policy, Disaster Recovery Plan, and other related documents. One of the eleven participants indicated that they have data breach notification policy although it is still to be approved. Four of the eleven participants mentioned that they do not have a formal data breach notification policy, but they failed to clarify if it is part of other security policies or procedures. On whether employees, clients and law enforcement are notified after a security breach, most of the participants indicated that they inform the employees but uncertain about the clients. Two participants indicated that they notify the law enforcement agencies as well.

*"We haven't had any data breach notification policy but, I think first is to inform the CIO and security and it will end up with the CEO which then the breach will be communicated and worked on from there… If the breach occurs, we will not necessarily communicate with everyone, because it might create chaos or panic, but we do inform the CIO, CEO as well as COO and discuss with people involved of the machines that are infected. At the end, once that is resolved, there will be a communication that goes out to the organisation, kind of lesson learnt to say this is what happened and be aware of this kind of things." (A1).*

*"No formal breach notification policy but the incidence response only speaks about notifying the staff, law enforcement but do not talk about notifying the clients/customers. I Don't know but the organisation will have to inform the clients if there is data breach" (B1).*

*"There is a data breach notification policy but it is not approved.... the problem is we haven't experienced a data breach" (F1).*

### 4.7.4 Information sharing

Information sharing forms part of the response plan. It is about organisations participating in information sharing forums and sources as well as collaborating with organisations across all sectors to share information about (i) cyber threats and cyber-attacks; (ii) appropriate mitigation measures; (iii) best practices; and (iv) ensure coordination in countering cyber-attacks. Information sharing can be voluntary as well to address cybersecurity awareness in a broader way.

Several participants stated that they do not have information sharing as part of the response plan, and currently, they do not voluntarily share information with any organisations. Some of the participants indicated that they have information sharing as part of the response plan or security policy.

*"Yes, this part of our security policy this is expected and sharing requirements are clearly set out. But being practised is another story" (B1).*

Several participants indicated that they collaborate with some of the sectors, in the main public sector to share and improve cyber threat intelligence, however, it is not a formal arrangement nor consistent. Some of the participants stated that they currently do not collaborate with any organisations.

### 4.7.5 Analysis

To respond to this category, organisations need to conduct analysis to ensure satisfactory response and recovery activities (NIST, 2017). In addition to analysis indicated in Section 4.6, post incident or event analysis should be conducted to determine the root cause of the incident. This category aimed at investigating if the organisations have set thresholds aligned to incident impact for events and incidents to determine appropriate response; and if the organisations conduct forensic activities following an event and incident.

Most participants indicated that they do not have formal thresholds set for events and incidents. Whereas some participants indicated that they set thresholds to determine an appropriate response for an event and incident, and the thresholds are approved by either business or supporting IT function or both.

*"Yes, we do and these have been approved by supporting IT functions guided by the AG and IT risk audit." (D1).*

On the matter of forensic investigations, the participants stated that they do conduct forensic activities. Majority of the participants specified that forensic activities are conducted by the internal forensic unit and subsequently supported by a third-party forensic specialist such as KPMG or law enforcement agencies. Few of the participants stated that forensic is exclusively conducted by a third-party forensic specialist. One participant indicated that forensic activities are conducted internally by their own forensic auditors, there was never a situation which required them to make use of a third-party forensic specialist.

## 4.8 Recover

This core function is with regard to the development and implementation of appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event (NIST, 2017). The interview questions for this function focused on recovery planning.

Recovery planning refers to "recovery processes and procedures that are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity incidents" (NIST, 2017). This category investigated if the organisations have suitable recovery plans and if the organisations can timely recover to normal operations after a cybersecurity incident. The recovery plan incorporates the business continuity plan, disaster recovery plan and incident recovery plan. Documented, regularly tested, reviewed, and updated; and clearly communicated recovery plans can be more effective (ASIC, 2015). A recovery plan provides an organisation with an ability to timely restore systems to normal operations or to a pre-defined, acceptable level.

The participants stated that they have a recovery plan, which is composed of disaster recovery and business continuity plans, missing incident recovery plan. Most participants believed their recovery plan is not suitable, with some participants stating that they have a draft disaster recovery plan or a draft business continuity plan or the recovery plan has never been tested, reviewed, or updated in the past 12 months. Few participants, although the incident recovery plan is missing, believed that they have a suitable recovery plan that has been tested in the past 12 months.

*"Yes. We have separate documented disaster recovery and business continuity plans forming a recovery framework. The effectiveness of this framework has been tested in the last 12 months…BCP - twice a year & DRP - often tested. Yes, the recovery plan is suitable but there is always room for improvement." (D1).*

*"We have disaster recovery and business continuity plans forming a recovery plan … but these have not been tested … the current recovery plan is not suitable but one busy reviewing it. I think it will be suitable but we are in a process to include everything and it will be suitable." (F1).*

Several participants stated that their response plan refers to the timeframe for restoring critical systems to normal operations or acceptable level. The timeframe is regularly reviewed. Few of the participants have nothing in place to timely restore critical systems in view of the fact that they do not have an adequate recovery plan, that is, disaster recovery plan not in place. One of the participants stated that, although they have a suitable recovery plan in place, they do not have the recovery timeframe because executive management delegated the responsibility to the business functions rather than IT function, of which business disagrees with the executive management and wants IT to take the responsibility.

# PART B: FINDINGS: SECONDARY DATA

## 4.9 Governance and Leadership

Good governance and strong leadership are required for effective cyber resilience, which begins with executive management ensuring that their organisations have an approved cybersecurity strategy that is regularly reviewed; management roles and responsibilities relating to achieving cybersecurity agenda; and cybersecurity strategy and other related information security policies and procedures are aligned to international standards and good practices. The response for cybersecurity strategy, roles and responsibilities and standards from the respondents are depicted below.

### 4.9.1 Cybersecurity strategy

The objective of the survey was to investigate if the organisations have a cybersecurity strategy in place, and how often is it reviewed; an executive management responsible for the establishing and reviewing of the cybersecurity strategy and assigned cybersecurity roles and responsibilities; and the standards and best practices that they are aligned to.

#### Cybersecurity strategy status

None of the organisations has a fully functional cybersecurity strategy in place. However, nine (9) of the 10 organisations have a plan in place whereas 1 organisation indicated that they have no plan in place, and they have no plan to get one in the near future. Six (6) organisations have discussed the cybersecurity strategy, and they plan to establish and implement it in the future. Three (3) organisations have developed the plan and will implement it within the next 6 to 12 months. The status of the cybersecurity strategy is shown in Figure 4-1.

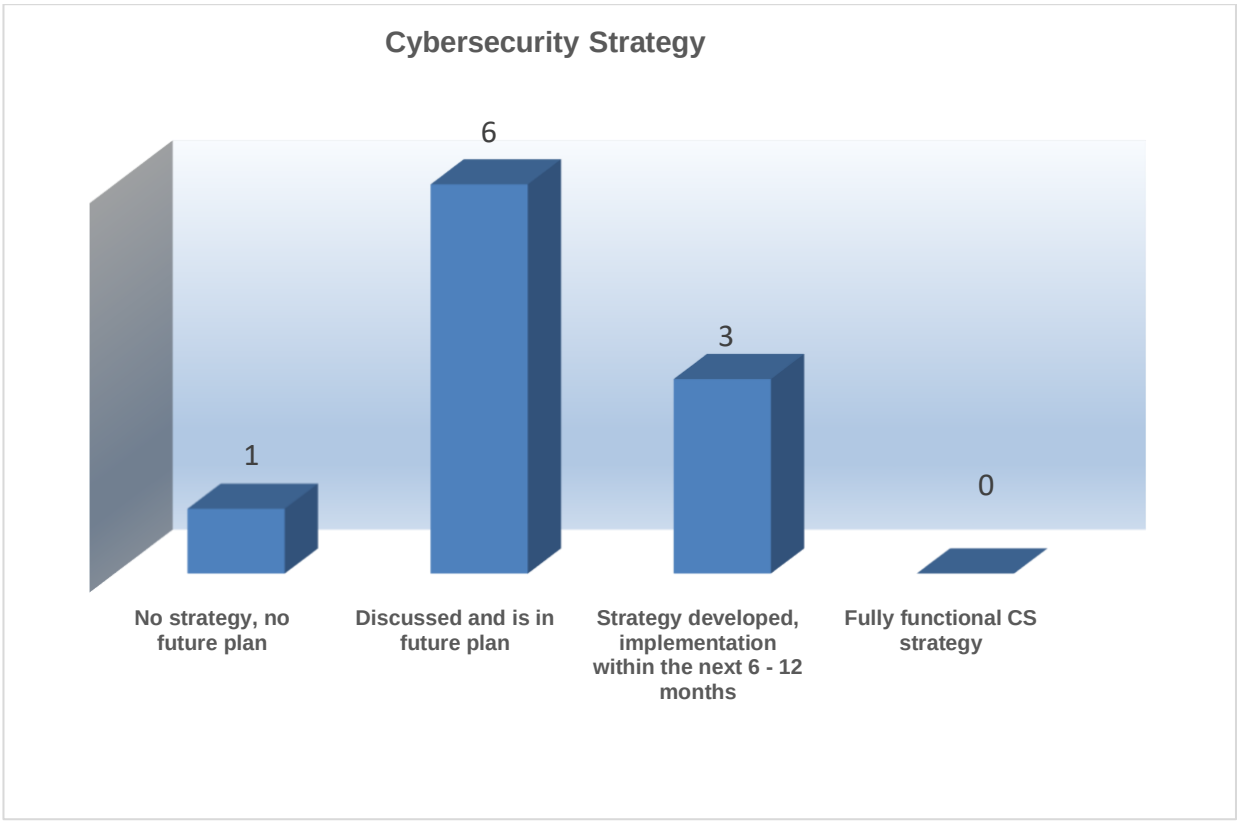



**Figure 4-1:** Cybersecurity strategy status

### Cybersecurity strategy review status

A cybersecurity strategy requires regular reviews and updates to keep up to the rapidly emerging cyber risks. According to the survey data, four of the ten organisations review their cybersecurity strategies and out of the four, two organisations review annually and the other two organisations review at different frequencies. Four organisations do not have a strategy to review, and two organisations have never reviewed their cybersecurity strategy. The cybersecurity strategy review status is illustrated in Figure 4-2.


**Figure 4-2:** Cybersecurity review status

For organisations to realise their cybersecurity agenda, the drive should start from the top, the Executive. The executive management needs to delegate at least one member to lead the development and implementation of the cybersecurity strategy. Nine of the ten organisations have a member of the executive management responsible for the cybersecurity strategy as follows: seven is led by a CIO or an IT Executive (ITE), one is led by the CRO or Risk Executive (RE), and one is the responsibility of the CISO. In one organisation, cybersecurity strategy is the responsibility of a member of management other than executive management, such as IT manager. See the illustration of the lead responsible person in Figure 4-3.

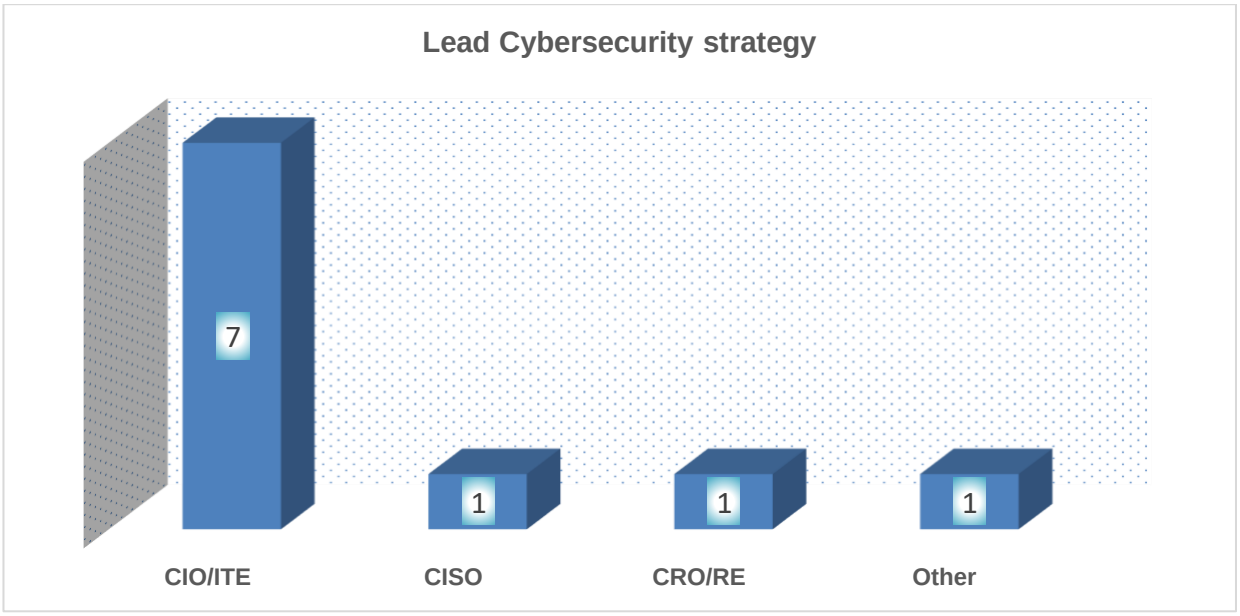



**Figure 4-3:** Lead person for cybersecurity strategy

### 4.9.2 Executive management

As discussed in section 4.3, effective cyber resilience requires the executive management commitment, understanding of the roles they need to play and the different responsibilities to be assigned to oversee development and implementation of a cybersecurity strategy, cyber resilience, cybersecurity, and other security-related responsibilities.

In all the organisations surveyed, there is at least one defined security role at the executive management level, and five of the organisations have two defined security roles. The CIO role is the most defined, see Figure 4-4 below. Nine of the ten organisations have the CIO, followed by the CRO from four of the ten organisations and last is the CISO from two of the ten organisations.

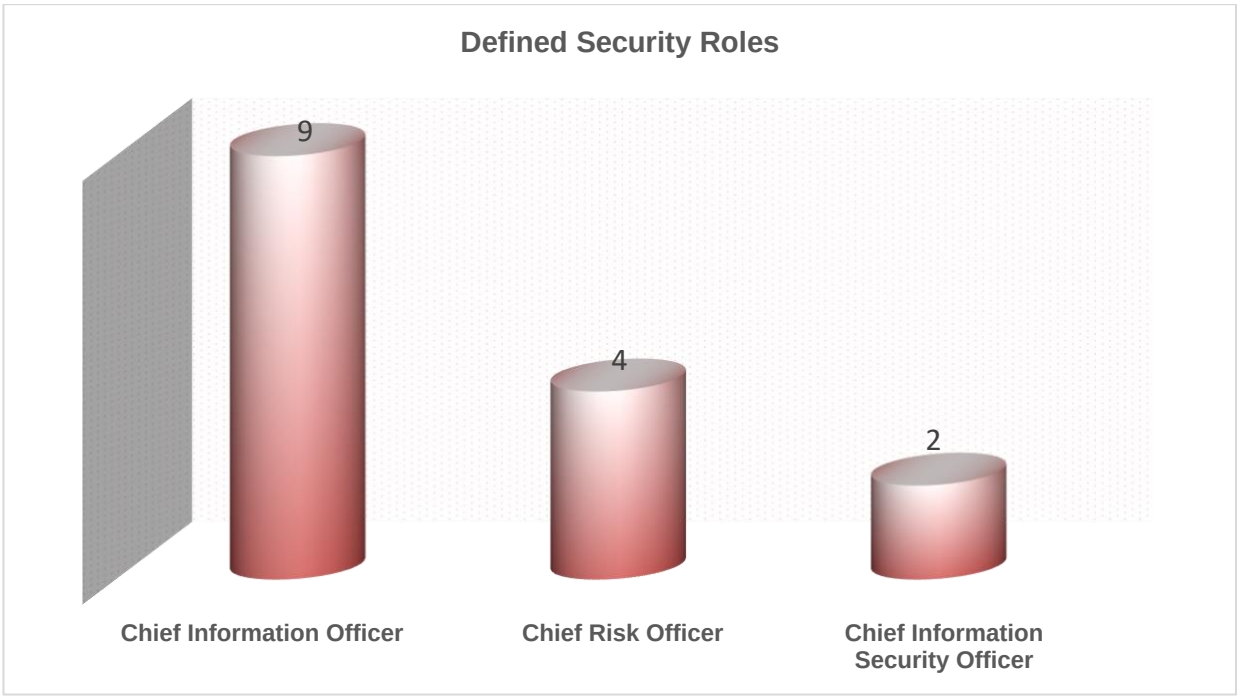



**Figure 4-4:** Security roles defined in the organisations

### 4.9.3 Assessing against NIST Cybersecurity Framework and other international standards

Aligning cybersecurity strategy or related policies to internationally recognised information and cybersecurity standards will assist the organisations to manage their information systems and critical data so that they continue to be secured. Few of the organisations are aligned to more than one standard.

The ISO/IEC 27001 family of standards is the option favoured by organisations, that is, seven out of ten organisations are aligned to it, as illustrated in Figure 4-5. Three organisations are aligned to the SANS standard, one organisation is aligned to NIST and one aligned to ISF standard of good practices. Two organisations indicated that they use other standards, such as the Minimum Information Security Standards (MISS).

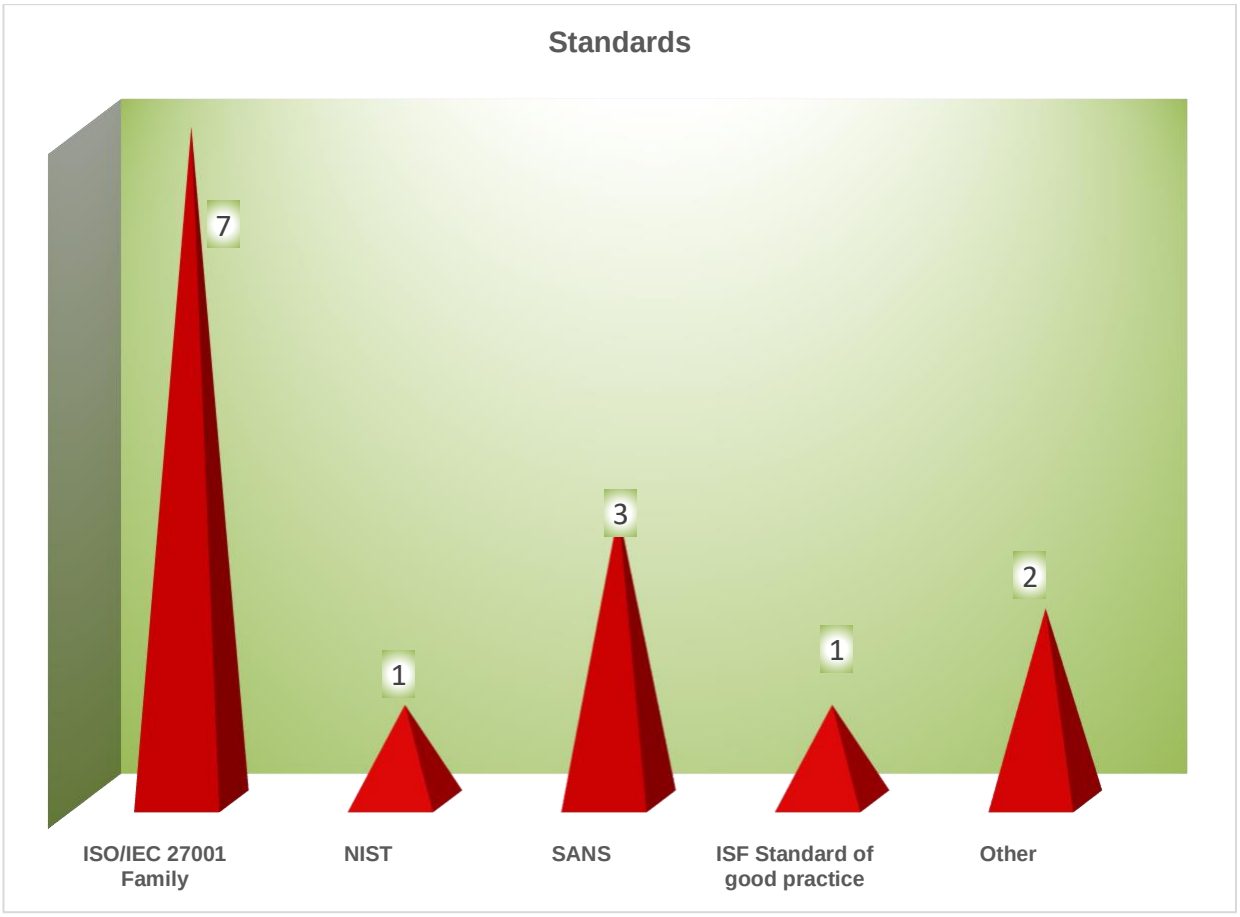



Figure 4-5: **Organisation's alignment to internationally recognised standards**

## 4.10 Identify

As discussed in chapter 4.9 this core function is about the development of an understanding to manage cybersecurity risks to systems, assets, data, and capabilities (NIST, 2017). It is critical to identify cybersecurity risks for the organisation's critical assets and functions, which could have a negative impact on the delivery of critical services. Further, critical assets and functions must be identified and managed as well.

Most of the organisations, eight out of ten organisations indicated that they formally identify critical assets. One organisation had not identified critical assets, and another one is uncertain if critical assets have been identified, as shown in Figure 4-6

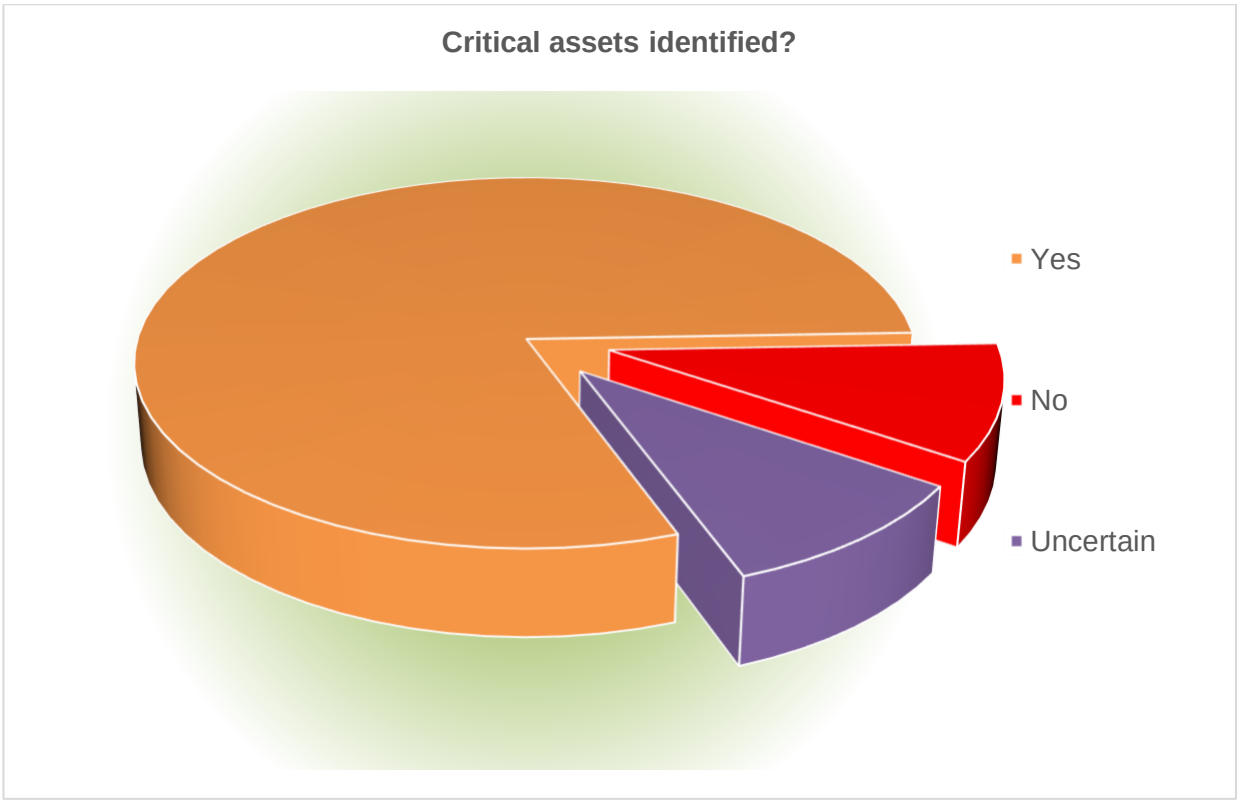



**Figure 4-6:** Identification of critical assets

Risk assessments should be regularly conducted to identify and analyse the risks to determine the appropriate actions to deal with the risks. Majority of the organisations conduct formal IT or cyber-related risk assessment at different frequencies: six conduct annual assessment; one conducts assessments twice in a year, and assessments are done more than once a year for one organisation; one organisation has assessments periodically, but not every year; and lastly, one organisation is uncertain if risk assessments are conducted, Figure 4-7.

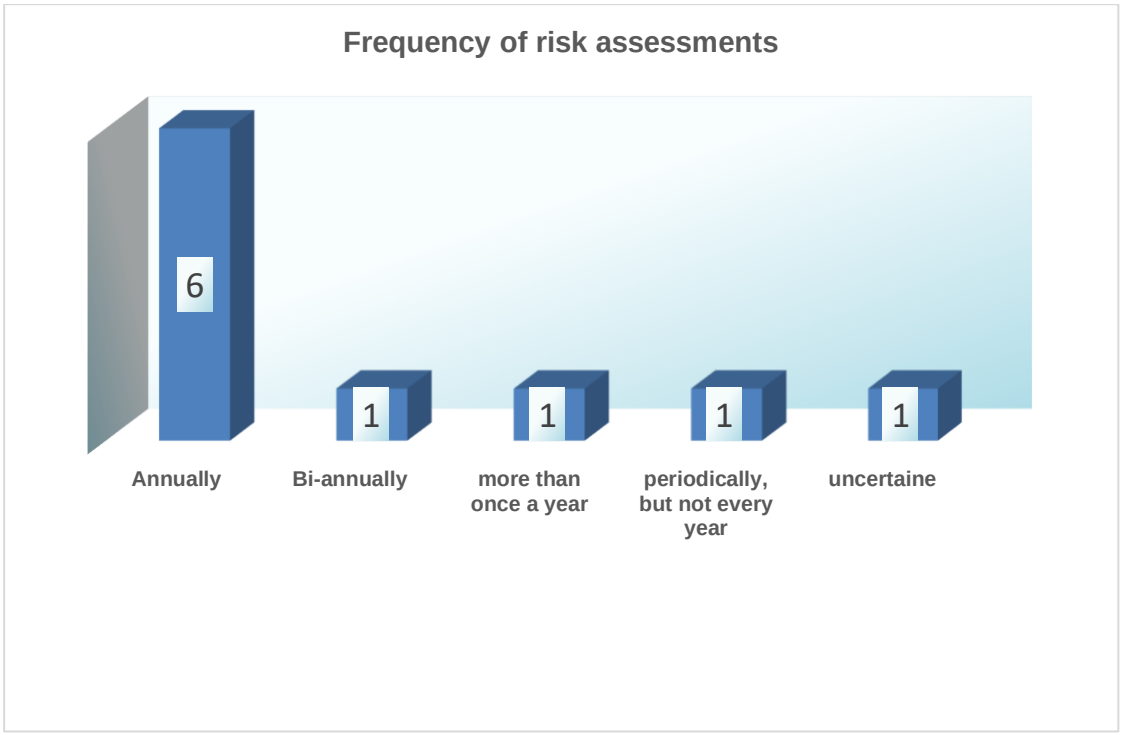



**Figure 4-7:** Frequency of IT or cyber risk assessment

Most of the organisations (8 out of 10) have taken actions in response to a previous risk assessment that was carried out, whereas two out of ten organisations were not aware of any actions taken in response to previous assessments (see figure 4-8). Six organisations acted on updating their policies, two organisations appointed more security personnel. Only one organisation saw a need for stronger education and training, while seven of the organisations implemented new technologies. One organisation took an action of outsourcing for assistance.

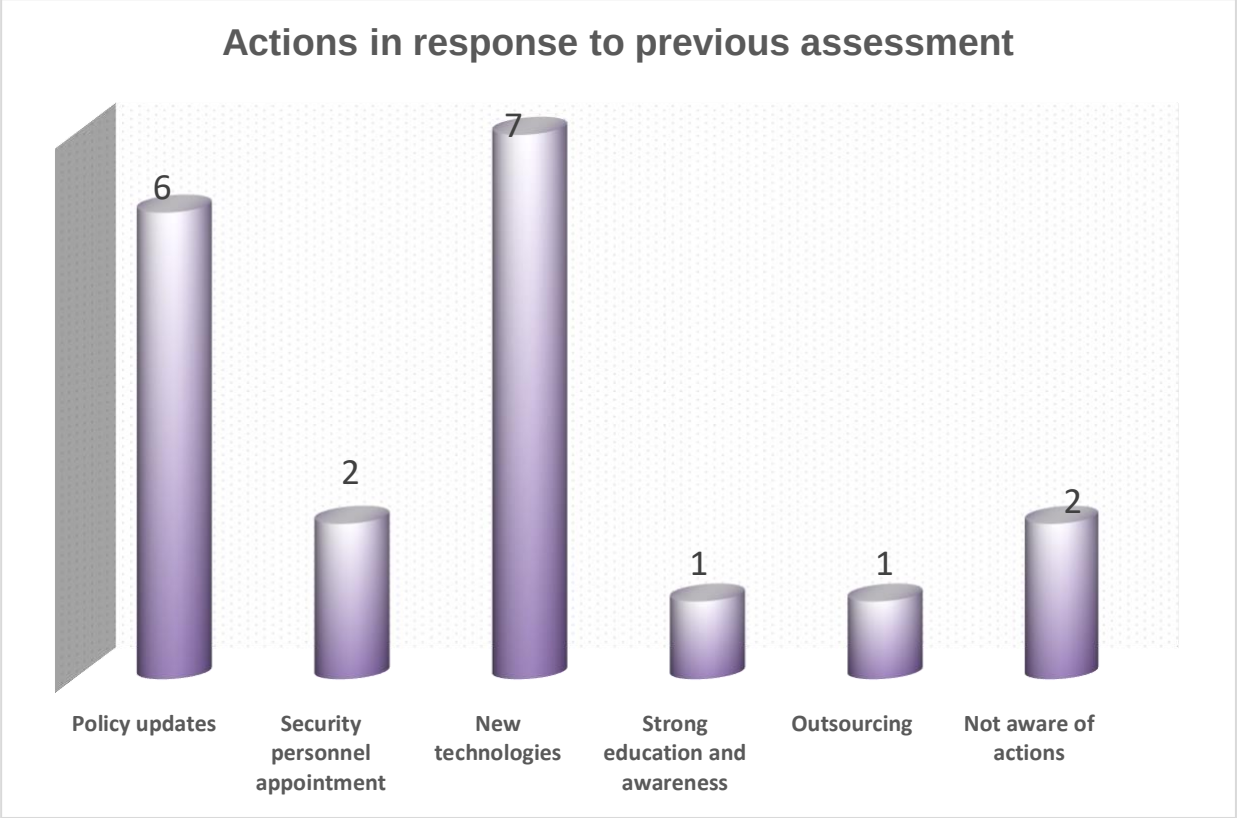



**Figure 4-8:** The actions taken in response to previous assessments

All organisations are faced with cyber risks (threats and vulnerabilities); however, organisations must identify the cyber risk they are exposed to or cyber risk that may be posing a serious threat to their critical assets. Consequently, organisations were given an option of selecting three top threats that their organisations are facing.

As illustrated in Figure 4-9, ransomware is indicated as a threat to most organisations (7 out of 10), followed by theft of mobile devices and laptops (6 out of 10) and last top threat is targeted malicious emails (5 out of 10). Other threats that organisations are facing are virus or worms' infection; Trojan; denial of service attacks; banking malware and rootkit malware.

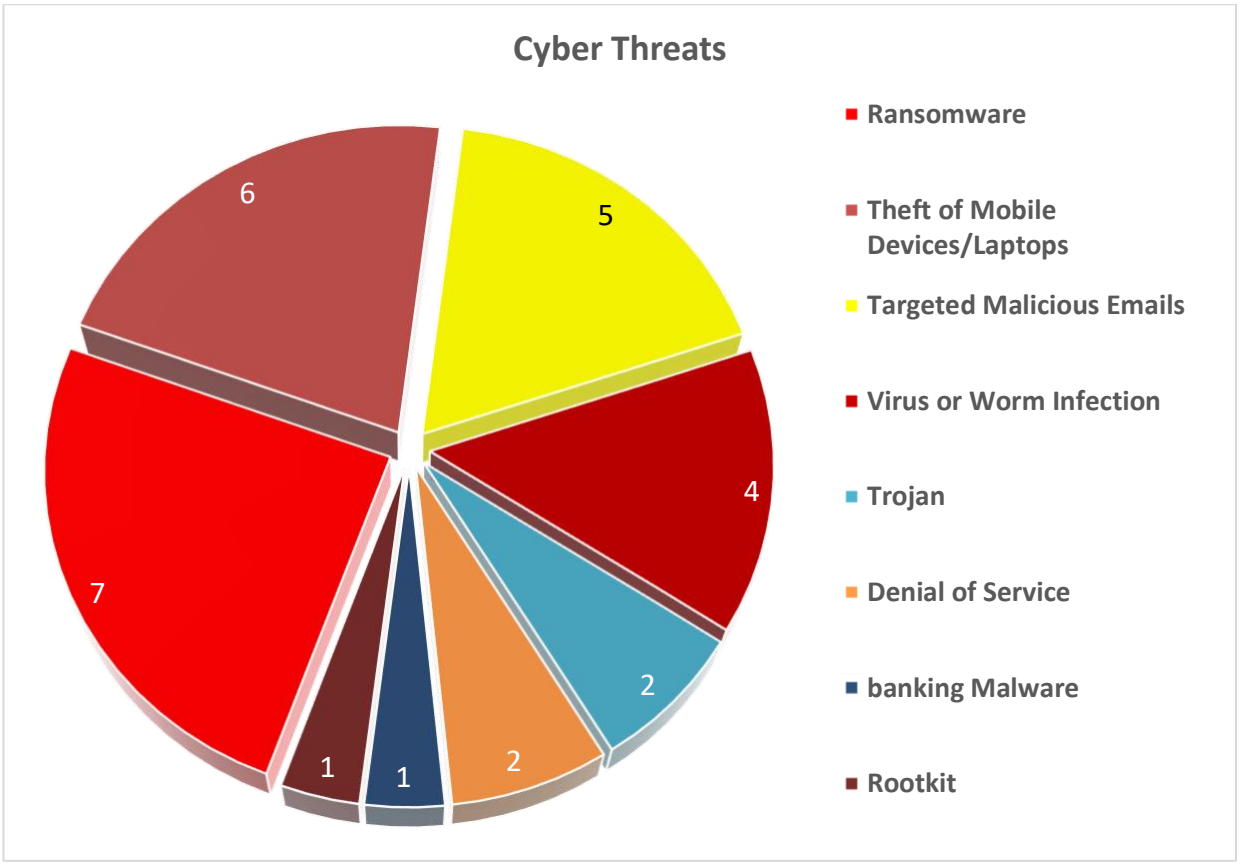



**Figure 4-9:** Cyber threats faced by organisations

Furthermore, respondents were asked to identify their possible threat actors. There are inside threat actors – someone within an organisation who have access and authority to the organisation's systems, such as employees and contractors; and outside threat actors – someone or an entity external from the organisation seeking to gain access to the organisation's system and they have no access and are not authorised.

Regarding the top four threat actors to organisations, employees (insiders) are indicated as the biggest threats for eight out of ten organisations, second are criminals from outside an organisation for six out of ten organisations, third are contractors for five out of ten organisations, and last being the hacktivist groups. Other threat actors that were indicated are customers, suppliers, terrorists, competitors, and lone hackers, see Figure 4-10 below.

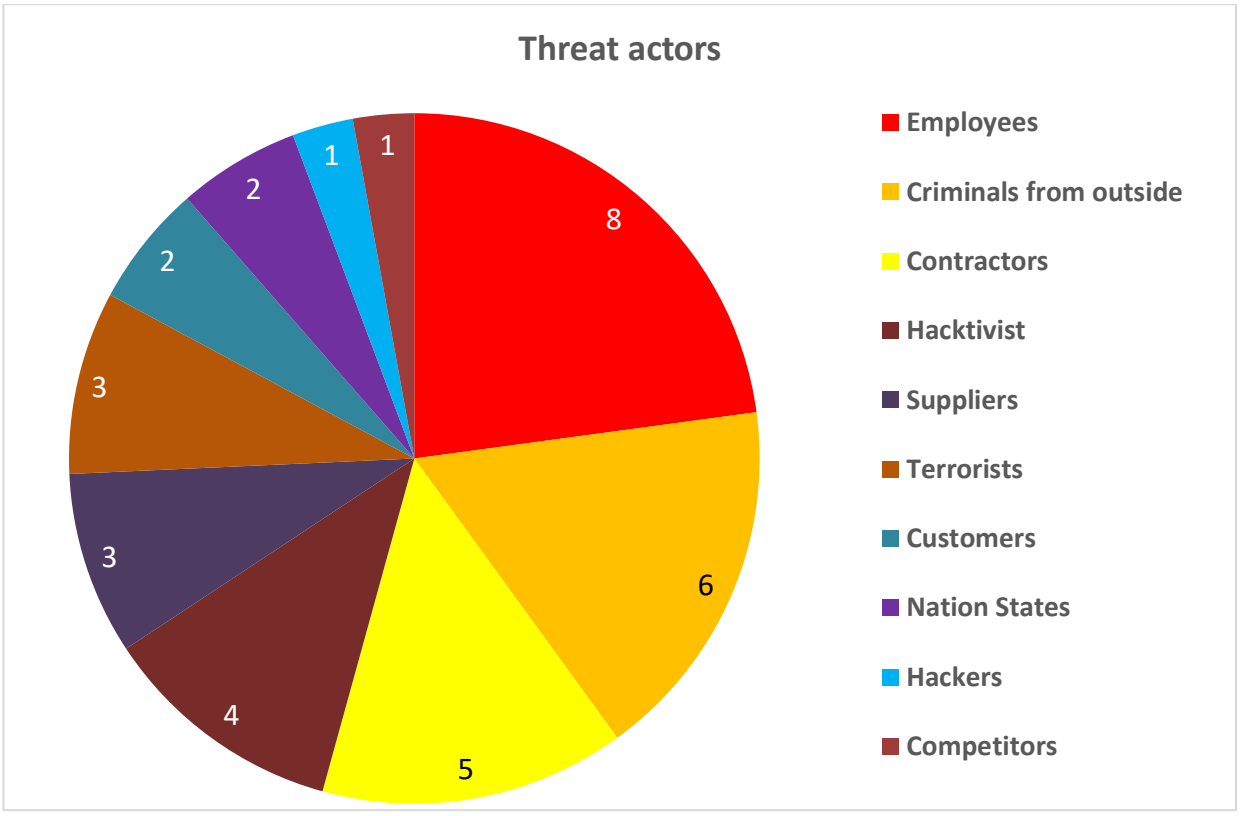



**Figure 4-10:** Threat actors posing cybersecurity threats to organisations

## 4.11 Protect

As discussed in section 4.5, this core function is about the development and implementation of appropriate safeguards to ensure delivery of critical infrastructure services as well as support the ability to limit or contain the impact of a potential cybersecurity event. (NIST, 2017). To protect critical data systems and assets, organisations need to consider building a strong cyber resilience foundation through the provision of regular cybersecurity awareness and training, sufficient resources as well as ensuring that there is sufficient and capable workforce to deal with cyber risks.

“Cybersecurity awareness provides knowledge about and application of cybersecurity principles by staff members in order to mitigate against cyber-attacks or cyber incidents. Although not all staff members may have equal knowledge or awareness, training in these issues could improve awareness” (DTPS, 2017b). To create strong cybersecurity and cyber

resilience foundation as well as cyber-aware employees, organisations require to provide their staff members with cybersecurity awareness training.

As illustrated in Figure 4-11, half of the organisations do not provide cybersecurity training. Only four out of ten organisations surveyed provide cybersecurity training, with one organisation being uncertain if training is provided. The level of cyber training offered by these organisations is at the beginner and intermediate. Training is provided in-house by most of the organisation (8 out of 10) and one organisation make use of their affiliated organisations

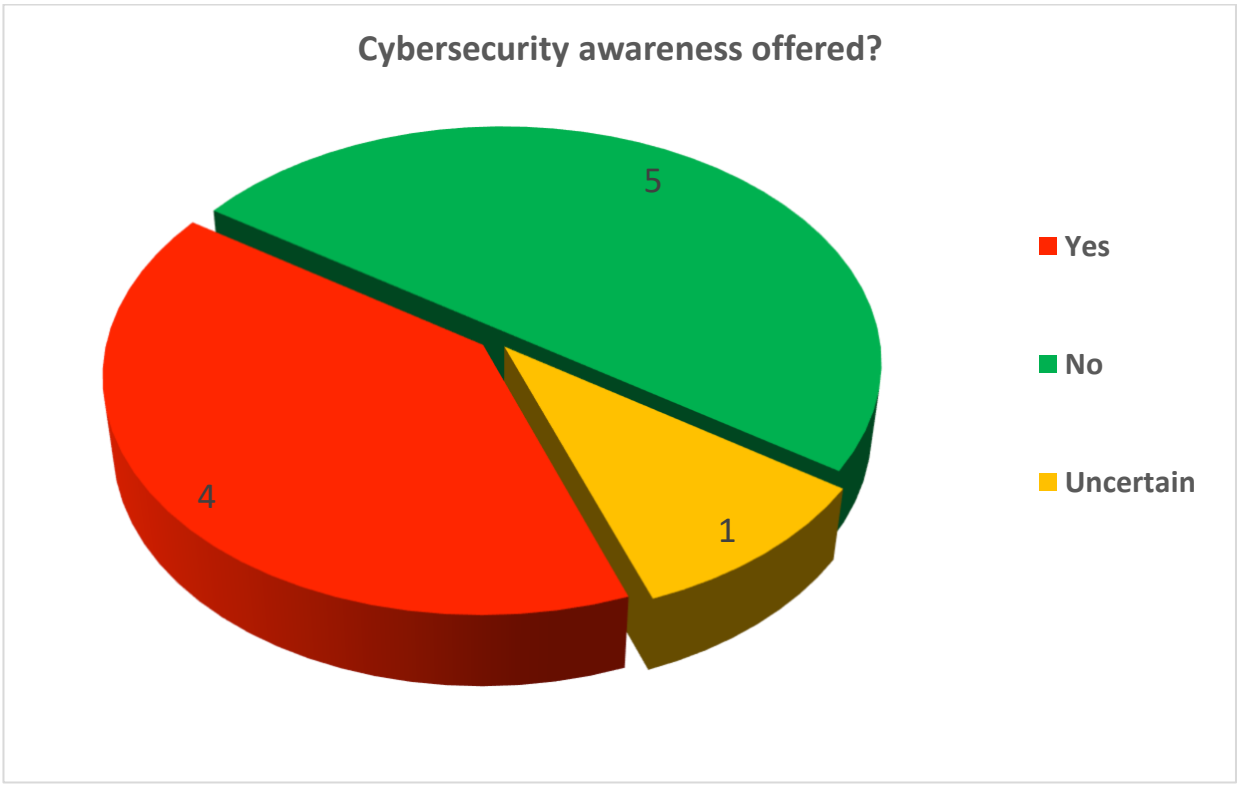



**Figure 4-11:** Status of cybersecurity awareness training offering

The results show that some organisations provide cybersecurity awareness training to all their staff members, that is, from top management to support staff, while other organisations provide to a certain level of staff members. The overall show that eight organisations provide training to core business staff, followed by middle management and support staff (seven

organisations), then functional managers for six organisations and last is top management for four organisation, figure 4-12. The frequency of providing cybersecurity awareness training is between annually and bi-annually.

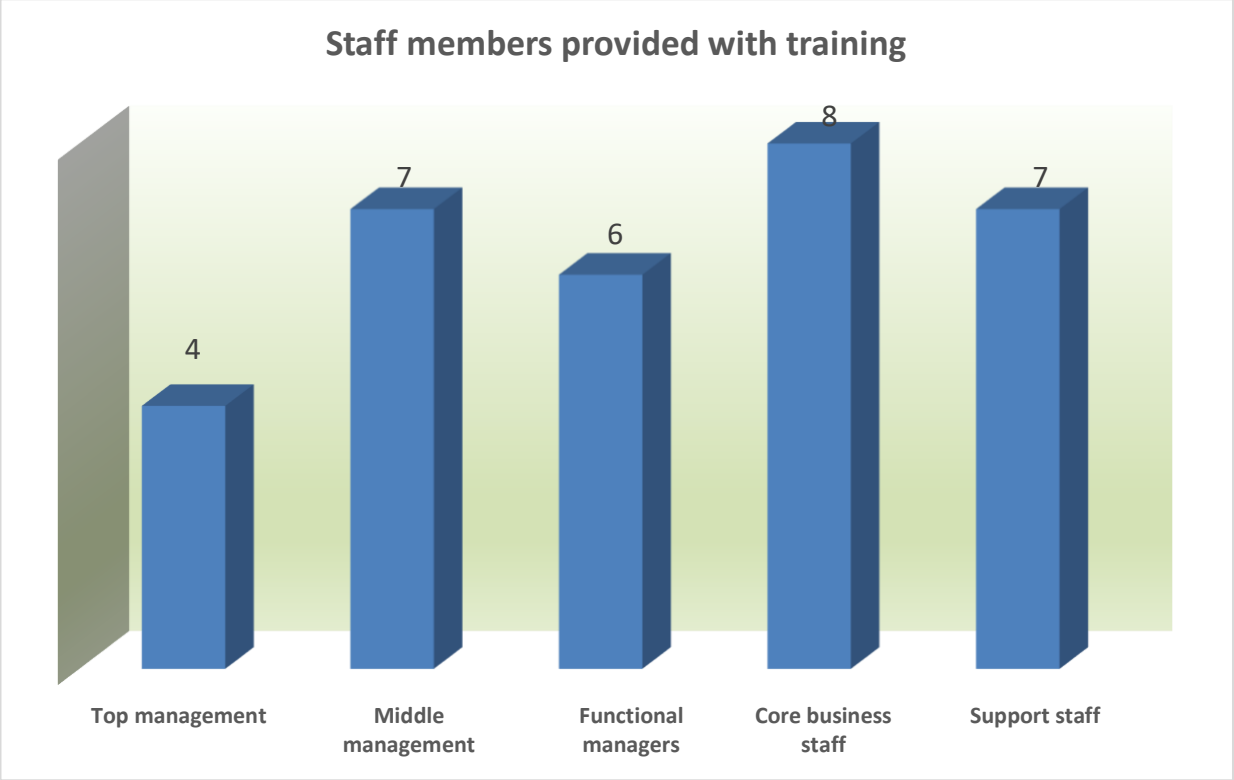



**Figure 4-12:** Staff members provided with cybersecurity awareness training

As discussed in section 4.5.2, effective cyber resilience requires sufficient resources to manage cyber risks and attacks. Resources include, but not limited to, workforce (employees and contractors) with appropriate qualifications; technologies; devices; and budget. There are potential challenges, regardless of having sufficient resources, organisations may face risks that can hinder the success of operations of cybersecurity or cyber resilience functions.

The results show that insufficient skilled staff in relation to cybersecurity, insufficient budget for improved technology resources and lack of awareness amongst staff are the challenges for six of the organisations. Five organisations see lack of information sharing through

CSIRT and complex, unclear compliance or regulatory requirements as a challenge, see Figure 4-13 for the potential challenges that organisations face.

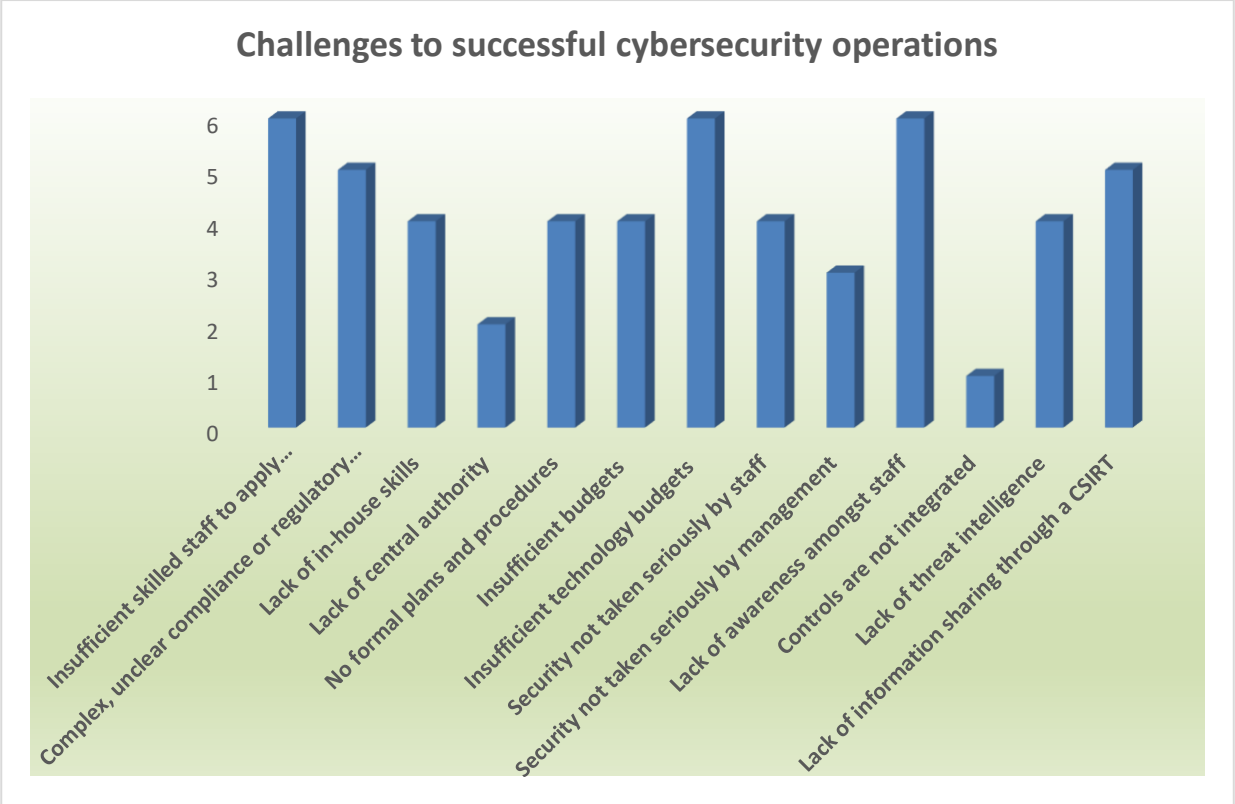



**Figure 4-13:** Potential challenges to the successful operations of the cybersecurity function

## 4.12 Respond and Recover

Response is about developing and implementing appropriate activities to take actions regarding a detected cybersecurity incident (NIST, 2017). Organisations require incident management, business continuity and recovery plans to respond to cyber incidents as well as recover to normal operations and continue with operations at an acceptable level.

Half of the organisations surveyed will not be able to respond to a wide range of potential incidents, while three organisations will be able to respond and two organisations are not certain if they will be able to respond. This is illustrated in Figure 4-14.

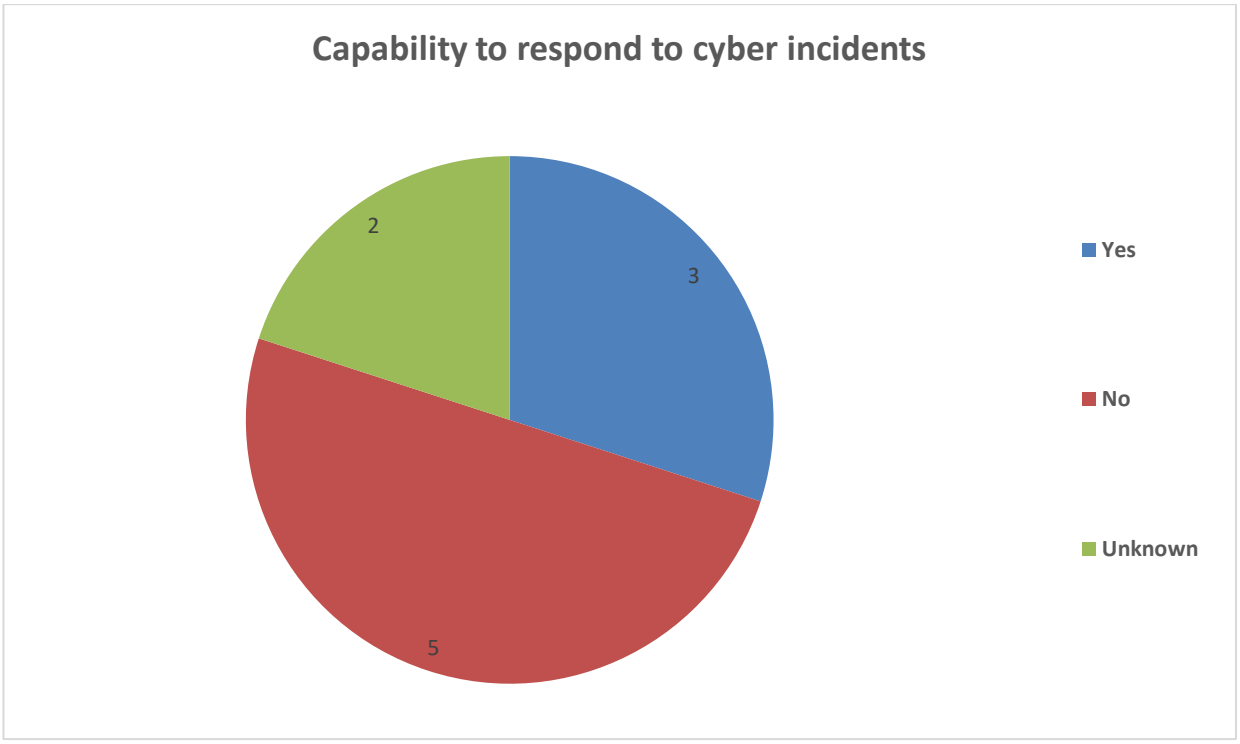



**Figure 4-14:** The ability of organisations to respond to a wide range of potential incidents.

To be certain of the level of incident handling in the organisation, incident response plan needs to be reviewed consistently, and the capability requires regular testing. Respondents were asked about the frequency of testing the incident response. Half of the respondents indicated that they have never conducted testing, while four of the respondents have tested the incident response capability once a year and only one respondent has tested twice in a year, see Figure 4-15.

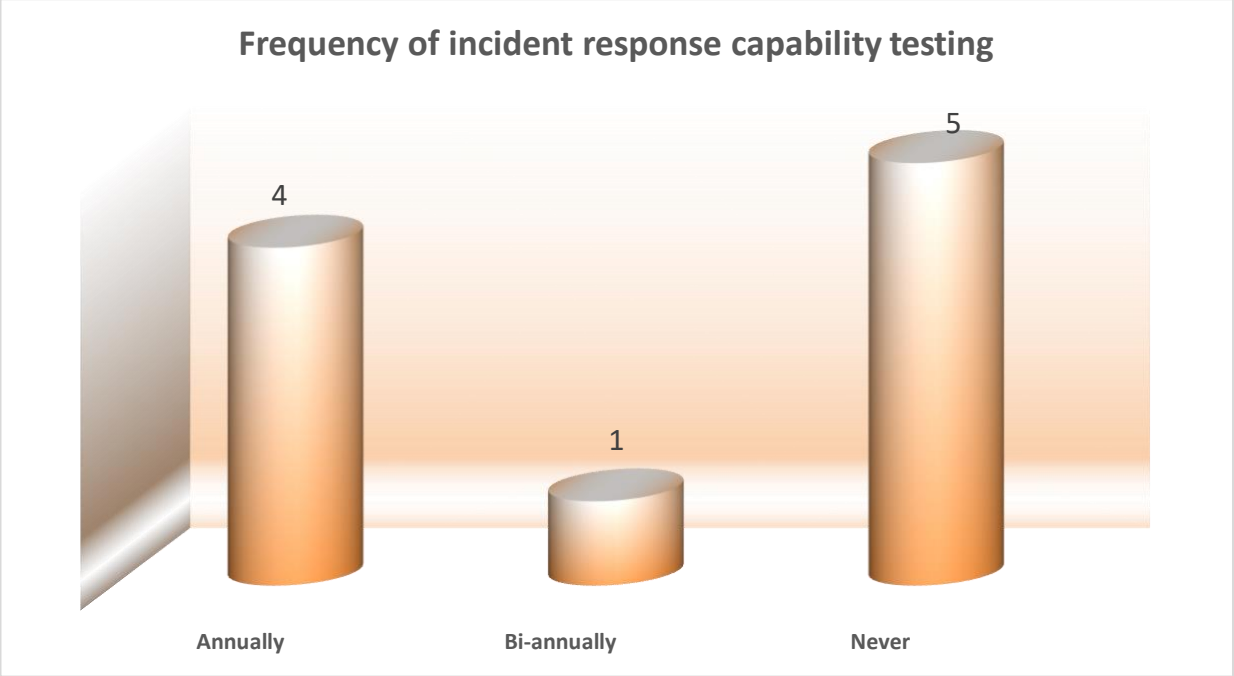



**Figure 4-15:** Frequency of incident response capability testing

Respondents were asked if their organisations will be able to recover their systems to normal operations or to a pre-defined acceptable level following a cybersecurity incident. Six of the respondents indicated that they are not certain if their organisation will recover, at least three organisations will be able to recover, and one organisation will not be able to recover to normal operations after a cybersecurity incident, see Figure 4-16 below.

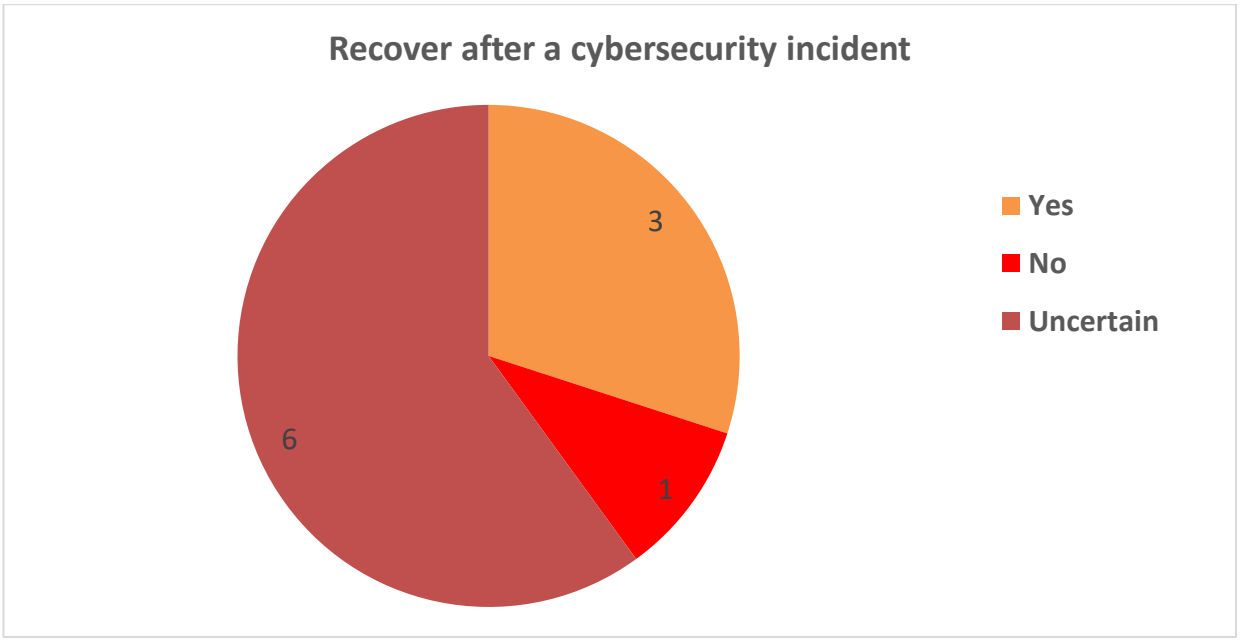



**Figure 4-16:** Recovery following a cybersecurity incident

## 4.13 Conclusion

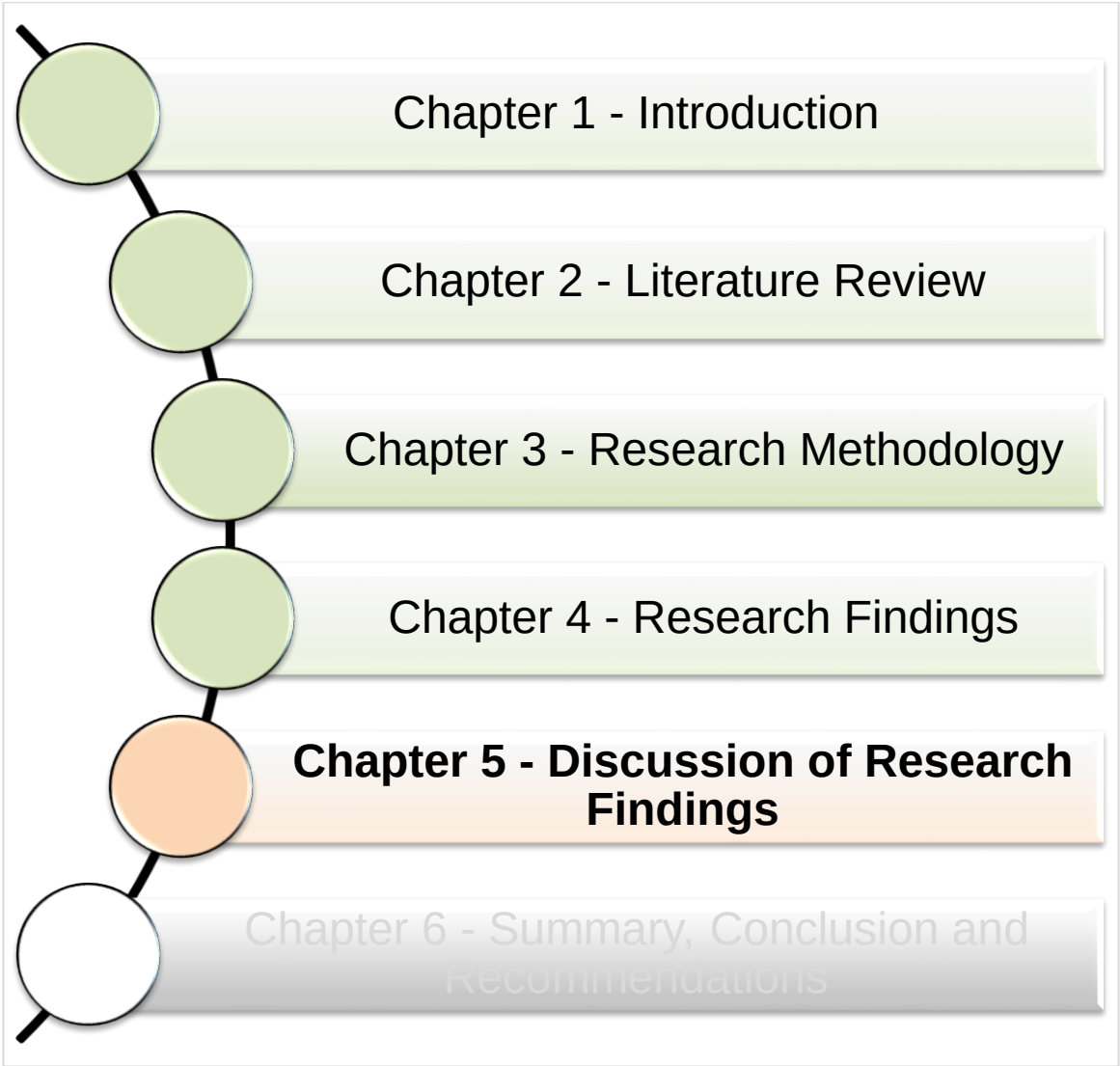
This chapter presented the findings of investigating cyber resilience of South African public-sector information systems against cyber threats and attacks. The researcher presented the research findings obtained from both the primary source and secondary sources. The primary source findings were from the semi-structured interviews conducted to eleven (11) participants. Due to the limited literature or published research regarding this research study, the researcher also used secondary data obtained from a third-party. The secondary data were from an online survey to determine cybersecurity readiness across all sectors in South Africa. However, the researcher extracted data, from the raw dataset, that was from the public sector in the Gauteng region, giving a total of 10 respondents.

The results were presented into two sections, and both sections were structured according to the themes, which are the core functions that address cyber resilience and effective cyber risk management as discussed in Chapter 3. The first section presented thematic findings obtained from qualitative semi-structured interviews, and the second section presented the statistical results obtained from the quantitative online surveys. The researcher used the

secondary data to increase confidence, confirm the validity of the thematic findings as well as to overcome the limitations from the primary source.

The next chapter will discuss the research findings to respond to the four research questions. The discussion of the findings will combine the two data sources to draw valid inferences as well as strengthen the understanding of the research topic.

# 5. CHAPTER 5 – FINDINGS DISCUSSION



## 5.1 Introduction

This chapter discusses the findings of the research study that was conducted in the public sector, in the Gauteng Province. The purpose of this study was to investigate if the South African public sector information systems have the capacity to survive cyber-attacks and can recover from those attacks. The study investigated the extent to which the South African public sector information systems are exposed to cyber risks. It also identified current cybersecurity threats and the impact they can cause to South African public sector information systems. Lastly, it proposes or recommends measures that can be used to mitigate cyber threats and attacks.

The researcher, as discussed in Chapter 3, used triangulation to strengthen and gain a better understanding of the study, increase confidence, and confirm the validity of the thematic findings; and to overcome limitations from the primary data source. The triangulation was to compare the thematic findings acquired from the qualitative semi-structured interviews, the primary source, and the statistical results acquired from the quantitative surveys, the secondary source, to strengthen the research findings. These triangulated findings were linked to the literature review.

The discussion of the research findings is presented according to the themes that were used to present the findings in Chapter 4, namely, (i) governance and leadership, (ii) identify, (iii) protect, (iv) detect, (v) respond, and (vi) recover.

## 5.2 Governance and Leadership

Cyber resilience requires good governance and strong leadership by the executive management to apply all the core functions. The objective of this theme was to determine if the organisations have an approved cybersecurity strategy; if the executive management is aware of the cyber risks faced by their organisations and that they understand the roles and responsibilities they need to play in achieving cyber resilience. It was also to determine if cybersecurity roles and responsibilities within the organisation have been aligned to the cybersecurity strategy where it exists and whether the organisation has considered

evaluating its cybersecurity strategy against the NIST Cybersecurity Framework and other International Standards, frameworks, or guidelines as well as possible partnerships across all sectors.

The interview findings revealed that the SAPSOs do not have an approved cybersecurity strategy in place, but they make use of security-related guidelines such as an Information (and Communication) Technology Security policy or information security strategy. These findings are corroborated by the survey results, which found that the organisations do not have a fully functional cybersecurity strategy in place. However, both findings are contrary to the literature review which has suggested that for organisations to be cyber resilience, they are required to have an approved and comprehensive cybersecurity strategy, which will describe holistic approaches and technical tools to mitigate cybersecurity risks and attacks.

As contended in the literature review, there are fundamental elements (Section 2.5.2) that should be promoted by the strategy and these elements do not form part of the ICT/IT policies, strategy or security guidelines used by the surveyed SAPSOs, such as legal measures; technical and procedural measures; organisational structures; capacity building; and cooperation and coordination with all sectors. The findings from both the interviews and survey reveal that some SAPSOs have future plans in establishing and implementing a cybersecurity strategy, which will be aligned to the business strategy. Few organisations do not have future plans in developing and implementing the strategy.

The findings, therefore, suggest that SAPSOs do not have a cybersecurity strategy in place that serves as a foundation in becoming a cyber resilient organisation and having cyber resilient information systems.

As asserted in the literature review, cybersecurity roles and responsibilities for cyber workforce need to be defined and aligned to the cybersecurity strategy. The interview findings indicate that organisations do not have defined cybersecurity roles and responsibilities, not because they do not have a cybersecurity strategy, but because they have roles and responsibilities aligned to the business strategy as according to their current functions and related security guidelines such as IT security officer.

As discussed in Chapter 2, the key to successful cyber resilience and management of cyber risks requires buy-in and commitment from the executive management, requires that executive management understands their roles and responsibilities to oversee the development and implementation of a cybersecurity strategy and cyber resilience framework/programme. Moreover, the executive management needs to be knowledgeable and take ownership of the cyber risks facing the organisation.

The primary findings show that executive management understands their roles and responsibilities in driving and overseeing the cybersecurity agenda as they have defined roles relating to either of the following functions: ICT security, information security or IT risk. These primary findings are supported by the secondary findings as they reveal that most organisations have, as the most defined role, the CIO followed by the CRO and very few organisations have CISO. It was also revealed that most organisations dedicated the CIO to lead the development and the implementation of cybersecurity strategy. However, the executive management and the defined roles are, at the moment, limited to the development and implementation of a cybersecurity programme, and not looking at a cyber resilience programme.

On the issue of executive management being aware of the cyber risks that their organisations might be exposed to, consistent with the literature, the research found that the executive management is aware of the cyber risk facing their organisations because cyber risk forms part of the organisation-wide risk management strategy. For most of the organisations, cyber risk is included in the risk register which is reported to and discussed by the executive managements as they are the owners of the organisational risks. However, the findings also suggest that, as *per* comments by various participants, executive management is aware of the cyber risk because it got to be reported to them and not as an initiative from them to identify the cyber risks.

Effective cyber resilience requires organisations to assess or align their cybersecurity strategy against internationally recognised standards, frameworks, and other best practices. These standards or frameworks can offer organisations with an ability to attain maximum security posture and risk management to secure critical information assets. Organisations

can integrate some of the standards or frameworks in developing a customised cybersecurity strategy. As noted in the literature, standards, frameworks, and other security best practices are fundamental in securing information systems. Moreover, organisations can adopt more than one of these security guidelines for their policies or strategies for effective cyber risk management and improving the resilience of information systems.

Although the SAPSOs do not have the cybersecurity strategy, the findings in Section 4.3 are consistent with the literature revealing that the SAPSOs are aligning their ICT/IT security policies, strategies, or related security guidelines against a combination of international standards, frameworks, or best practices. The most popular standard is ISO/IEC 27001, which focuses on safeguarding the confidentiality, integrity and availability of information based on a risk management process as well as specifying requirements for continuous improvement of information security management system (ISO/IEC, 2013). Some of the standards or frameworks that have been adopted are ISO/IEC 27002, COBIT, ITIL and the Minimum of Information Security Standards (MISS). Very few SAPSOs adopted the NIST Cybersecurity Framework.

Although the organisations do not have cybersecurity strategies in place, as discussed in Section 5.2.1, findings reveal that for their future plans in developing and implementing a cybersecurity strategy, a combination of information and cybersecurity standards and frameworks will be adopted. The framework that seemed to be the preferred is the NIST Cybersecurity Framework, which is among the most commonly used frameworks for cybersecurity. According to Moraetes (2018), a cybersecurity strategy comprises hybrid of standards and frameworks which enables the organisations to hand-pick security controls best suitable for security objectives, compliance, and effective cybersecurity strategy.

## 5.3 Identify

For organisations to successfully thwart a cyber-attack, they need to have an in-depth understanding of their security posture, critical information assets and how to identify and manage cybersecurity risks to systems, assets, data, and facilities. The objective of this

theme was to determine if the organisations have processes in place for asset management and risk management.

Asset management provides direction in establishing and managing an inventory of mission-critical assets that support critical services (Del Giudice & Wilkinson, 2016). Furthermore, asset management checks if ICT or cybersecurity structures support the delivery of those critical services as well as assess the integrity of data required for the delivery of critical services.

The interview findings, corroborated by the survey results, revealed that organisations have a process in place to identify critical assets for critical functions or services except for a few that do not identify essential assets. IT and ICT security functions support the delivery of critical business functions. However, it was revealed that the process to identify critical assets is decentralised to risk management or to business units identify their own critical functions or services.

The MISS compels organisations that have in their possessions information that is, to some degree, sensitive in nature to have security measures in place. The sensitivity of information dictates the level of protection and thereby information to be classified accordingly (SSA, 1998). SAPSOs have in their disposal sensitive data, such as any information that is not yet available or will never be made available to the public, such as employee records, financial and procurement data, bilateral and multilateral information, organisational policies, and standard operating procedures.

The interview findings reveal that the SAPSOs are inconsistent with the MISS policy document, which clearly states that “sensitive information which in the national interest, is held by, is produced in, or is under the control of the State, or which concerns the State and which must by reasons of its sensitive nature, be exempted from disclosure and must enjoy protection against compromise.” This research study found that most SAPSOs do not assess the sensitivity and integrity of data and do not have a data classification system. Furthermore, findings indicate that although there are organisations that assess the sensitivity and integrity

of data, they failed to elaborate on the data classification system and the researcher observed that they were not convincing that they classify their information at all.

Cyber risk management refers to the processes that assess (identify, analyse, evaluate) and mitigate cyber risks to critical assets, services, functions as well as external services providers that could have a negative impact on the delivery of critical services. To address cyber risks, organisations must implement effective risk management practices (risk identification, risk analysis, risk evaluation and risk mitigation). Effective risk management practices involve formal documentation of risks, the risk register; official reporting of risks to all stakeholders; implementing risk solutions; conduct continuous monitoring and review of the effectiveness of the implementation of risk management practices (University of Adelaide, 2014).

Most SAPSOs have a separate unit which focuses not solely on cyber risks but on all organisational risks. ICT and cyber risks are integrated into the organisational risk management system. The risks are documented to the risk register which includes actions to be taken; official reporting to the executive management, which report to the audit and risk committee on a regular basis; and there are regular monitoring and review of the practices, which is conducted at the audit and risk committee as well. Therefore, these findings are in line with the literature. Additionally, the research study found that some of the organisations have included risk management as part of the annual individual performance management.

The literature considers cyber risks (threats and vulnerabilities) as one of the foremost and challenging risks in today's world. The interview findings indicate that there is an acknowledgement by the SAPSOs that they are facing cyber risks since they are connected to the internet and they are dependent on third-party suppliers for technology, IT hardware and software. The literature substantiates this view, for instance, Olsen (2013) argues that any organisation that connects to the internet or rely on third-party technology vendors or carry personally identifiable information faces cyber risks.

Organisations face various cyber risks that are frequently changing, ranging from internal to external threats and vulnerabilities. Nonetheless, it is imperative that organisations identify cyber risks that they may face because they can determine the measures needed to mitigate risks as well as improve cyber resilience (ASIC, 2015). Correspondingly, this research found that few SAPSOs identify the cyber risk that they may be exposed to; these risks are based on the operations or line of work of the organisations. On the contrary, most SAPSOs believed that they need to look at all cyber risks covered in the cybersecurity spectrum, however, they failed to elaborate on the reasons as to why all cyber risks as well as listing the top or prioritised cyber risks to the organisations. According to ASIC (2015), it is impossible for any organisation to protect themselves against all cyber risks.

One of the cyber risks that will always be there is the vulnerability that may be brought by a weak cybersecurity posture of vital third-party service providers. Therefore, it is essential that organisations assess cyber risk management and cyber resilience of third-party service providers. Contrary to the literature and the survey results that found most SAPSOs consider third-party service providers as among the top three threat actors, this research study found that majority of the SAPSOs do not consider the cyber risk and cybersecurity posture of the third-party service providers. However, there are few SAPSOs that would rather have third-party on-site for the duration of the contract term as a way of their risk mitigation strategy. This implies that SAPSOs do not consider that they can be made vulnerable or exposed to more cyber risks either directly or indirectly through their third-party service providers.

On the issue of software and hardware vulnerabilities, findings indicate that SAPSOs have a process, which includes identification, remediation, and partial documentation, for prioritisation of critical vulnerabilities. However, most of the SAPSOs conduct only software vulnerability identification. The research established that although SAPSOs attempt to document the processes, it is seen as a serious challenge because there is inconsistency since not everyone adheres in documenting the processes, and it is not enforced.

According to the literature, cyber threat intelligence enables the organisation to share and comprehend cyber threats to improve the capability to identify, protect, detect, and respond. Organisations can produce their own cyber threat intelligence or they can receive information

from third-party vendors, information sharing forums and sources. The research established that SAPSOs create a cyber threat intelligence report by extracting information from multiple sources, such as an internal, technology vendors, global cyber threats networks and so on. They use the threat intelligence report to analyse new cyber threat trends and determine security solutions to reduce cyber risks. However, the findings also suggest that, as *per* comments by various participants and observation by the researcher, cyber threat intelligence information is neither given attention nor properly analysed due to the insufficient skilled personnel to analyse such information.

## 5.4 Protect

Once critical information assets and services have been identified, integrity and sensitivity of data associated with the critical information assets and services have been assessed and effective risk management practices are in place, then requisite steps to protect the critical information assets and services can be taken. Protection involves developing and implementing appropriate defences to ensure delivery of critical infrastructure services as well as supporting the ability to limit or contain the impact of potential cybersecurity events (NIST, 2017).

Cyber resilience will not be complete if there is no implementation and management of security measures that limit access to critical IT systems, networks, data, and related facilities to authorised users only. The management of these security controls entails that the security controls are frequently maintained, monitored, and reviewed. This study looked at two primary access controls that require identity management: (i) physical access control which restricts access to facilities that house sensitive or critical data, networks, and IT systems such as server rooms, IT offices or high security zones, and (ii) remote access control to prevent unauthorised access to the organisation's networks, system files and information. Remote access controls that can be put in place are the use of VPN, encryption and remote access permission given to exclusive individuals.

In today's world, a single layer of security is not enough. Multi-layered security is essential even for access controls and these security controls are developed to minimise security risk. There is a perception that for cybersecurity or cyber resilience, physical access controls are

not as important as remote access control. However, what is not understood is that unauthorised physical access to a computer or server can be as disastrous as unauthorised remote access to networks. The research study discovered that most SAPSOs have security controls in place for both physical access and remote access but these are inadequate. For instance, there are areas that physical access controls are not implemented; there is uncertainty whether security controls for both remote access and physical access are regularly maintained, monitored, and reviewed. The uncertainty for physical security access is due to the fact that the responsibility lies with the physical security component.

As discuss in the literature review, Section 2.4, effective information security processes and procedures are essential for effective cyber resilience. This entails implementation and management of security policies, procedures, processes, and best practices protecting information systems and assets (NIST, 2017). Effectiveness implies information security policies, process and procedures are frequently reviewed and updated to align to the latest internationally recognised standards; IT systems, process and procedures are regularly evaluated for cyber resilience; cybersecurity capability of third-party service providers is assessed, and there are sufficient resources to manage cyber risks.

This research study found that SAPSOs are in line with the literature and this is corroborated by early finding in Section 5.2 that SAPSOs use a combination of recognised standards to align to their information security policies, processes, and procedures. As revealed in Section 5.2, and findings for this section, SAPSOs incorporate ISO/IEC 27001 information security standard to their information security policies and procedures.

Findings reveal that SAPSOs have never tested their existing information systems for cyber resilience. These findings are contrary to the literature which suggests that organisations need to regularly test their information systems to ensure that they can detect, withstand, respond to, and recover from cyber-attacks as well as improve the cyber capability of the organisation. The SAPSOs at the minimum conduct, as part of network systems security testing, vulnerability scanning and penetration testing. Failure of SAPSOs to test their information systems for cyber resilience implies none of the SAPSOs has certainty that their

systems will remain available and operate reliably during a disruptive cyber incident and that they will be able to recover their business-critical systems at an acceptable level and time.

Many SAPSOs rely on third-party service providers for ICT supplies, technology support or information security advisory, and this is a significant information security concern. Assessing security capability should be considered during the contracting process, and it is part of the requirement for the information security management systems. The objective of assessing information security capabilities of third-party service providers is to ensure the protection of assets and information that the third-party service providers have access to. Further, it provides SAPSOs with an understanding of the overall enterprise security posture of third-party service providers.

This research study found that SAPSOs are not aligned with information security management system requirements in terms or personnel security screening. Several SAPSOs do not conduct security assessments of third-party service providers. The SAPSOs that conduct these assessments make use of different methods such as security screening, vetting, security audit of processes and controls or rely on third-party self-certification. In most cases, these assessments are conducted at an early stage or prior to the signing of the contract agreements by either a structure within the organisation or law enforcement. This implies the process is a “once-off”.

The findings also revealed that the SAPSOs that rely on the third-party service providers’ security self-certification does not verify the information provided by the third-party service providers. This implies that some of the information provided might be unreliable, particularly that the security screening is not conducted formerly. Therefore, this category of SAPSOs that rely on self-certification security assessment can fall under the category of “no security assessment”.

In view of the above, the researcher can conclude that most of SAPSOs do not assess the security capabilities of the third-party service provider.
Chacko, et al. (2016) argues that there is no organisation that has resources to completely eradicate cyber risks. Although cyber-attacks are escalating, organisations do not allocate

sufficient resources to manage cyber risks. Sufficient resources are critical for effective cyber risk management and cyber resilience. These resources include, but are not limited to, properly trained cyber workforce (employees and contractors), security technologies and devices as well as sufficient budget.

This research has found that there are no sufficient resources to deal with cybersecurity or IT security related matters in the SAPSOs. None of SAPSOs has more than two people responsible for cybersecurity. In addition, those people either do not have cyber training, or they are insufficiently skilled or trained. Some SAPSOs are of the view that they are not highly vulnerable, therefore there is no need to invest many resources on cybersecurity. However, what SAPSOs do not realise is that, even if they think they are not highly vulnerable, they are still exposed to a range of cyber risks unknown to them at that time and that these can have a damaging impact on the organisation. SAPSOs perceptions in this regard are inconsistent with the focus of cyber resilience – to anticipate the 'unknown unknown' cyber risks. These findings are supported by the survey results: The potential resource challenges for SAPSOs to achieve successful operation of the cybersecurity function is:

- insufficiently skilled employees to apply cybersecurity,
- insufficient budget to support risk management initiatives,
- insufficient budget to update available applications or software,
- insufficient budget for improved technology resources and security solution,
- lack of awareness programmes and in-house training, and
- lack of information sharing through CSIRT and threat intelligence.

Data is the "crown jewels" of any organisation and protection must be throughout its life cycle because data loss can be very costly. Data breaches are becoming frequent, and as shown in Section 2.3.1, the SAPSOs have suffered several data breaches, which compromised sensitive information. To prevent data breaches, organisations need to set up data security. Data security is a key to business continuity, and it concerns managing information and data in relation to the organisation's risk strategy, to protect the confidentiality, integrity and availability of information and data (NIST, 2017).

Huq (2015) suggests that organisations should consider making a data loss prevention (DLP) strategy as an essential function of daily organisational operations. DLP is a process to identify, monitor, and protect sensitive data at rest, in motion and at end-point as well as reduce risks of data leakage or loss (Tahboub & Saleh, 2014). The DLP strategy should incorporate appropriate mechanisms, such as defining sensitive data types, data storage, data flow; DLP policies to encompass all potential loss modes (data at rest, data at the endpoint and data in motion); enforce security controls to prevent incidents; be used for data risk management and incident handling (Reed, 2017).

Considering the importance of data security and DLP strategy, the findings for this study revealed that SAPSOs do not have a data loss prevention strategy in place to counter data breaches and this finding contrast with literature. However, data protection is partially covered in other security documentation such as IT security policy or standard operating procedure. The “partially covered” DLP implies that the SAPSOs might not address all critical factors of DLP, thereby rendering the DLP ineffective.

This finding provides confirmatory evidence that SAPSOs do not assess, or define sensitive data as revealed in this chapter’s Section 5.3.

Part of the DLP strategy is to define data storage, and handling and this study looked at how data is stored, that is, at rest (server or database), and at endpoint (laptop or PC) and how it is handled or protected. One of the commonly used data protections is encryption. Organisations can encrypt sensitive data when stored, in use or in motion. The findings reveal that SAPSOs enforce employees to conduct daily functions on the internal network for data to be stored in a central storage rather than individual PCs. Data stored in the central storage is considered sensitive, therefore it is encrypted, and on the other hand, data stored on individual PCs is not encrypted since it is not considered sensitive.

Moreover, findings revealed that device encryption (data at rest encryption) is enabled on the server and official laptops provided to employees. Findings also revealed that encryption is not continuously and effectively applied, for instance, sometimes encryption is deactivated

because it slows down the system, and it is uncertain whether data-in-motion or data-in-use is encrypted or not.

Data backup is an essential part of data security and data loss prevention, and it should be mandatory for any organisation especially given the cyber risks that are faced these days. Data backup is the process of duplicating and archiving data stored in computer systems so that original data can be restored after a data loss incident. Data backup process covers what data to backup; how often to back up; type of backup system; storage media; and storage location. This research study found that backing up of data differs as per organisational priorities, needs and objectives. Most SAPSOs indicated that their backups are hosted by the State Information technology Agency (SITA). There was no further elaboration on the relationship between SITA and SAPSOs because it was considered sensitive. However, findings revealed that organisations backup all the data that is stored in the central storage, as it is considered critical, and it is stored in multiple formats. Multiple formats, for instance, imply that organisations backup data using:

- More than one backup type: full back, incremental backup, and differential backup.
- More than one storage media: tape, Optical Discs, hard disk, SSD, or cloud.
- Backup frequency: hourly, daily, weekly, and monthly.
- Storage location: at least one offsite location.

There is an instance where a PSO has a challenge in backing up and encrypting some critical data because the backup system is obsolete and there is a lack of funds to procure a new system. The use of obsolete systems increases exposure to cyber risk because these systems have no or limited software updates and upgrades as well as vendor technical support.

In view of the above, the SAPSOs do not have DLP and they do not define and assess the sensitivity of data. Although the SAPSOs conduct data backups and data encryption, it is insufficient to implement those controls alone without an approved comprehensive process of protecting data given that most SAPSOs have a challenge with documentation. This could

lead to the lack of accountability of data flow and usage monitoring, lack of secure communication platform for sensitive data, enforcing data classification will be non-existent.

One of the biggest cyber risks to an organisation is the lack of proper cyber capacity building in the form of cybersecurity awareness, technical cyber training, education, and development. As mentioned in the literature review, cyber capacity building is one of the criticalities for cyber resilience. Cybersecurity awareness is the first line of defence in securing information systems, and most importantly, it develops a cybersecurity culture in the organisation. What is critical as well as the ability for organisations to educate, train and develop highly-skilled technical cybersecurity workforce to effectively mitigate cyber risks and prevent cyber-attacks.

The NCPF articulates, as one of its key objectives, the promotion of cybersecurity culture. In promoting a cybersecurity culture, the NCPF provides among others implementation of cybersecurity awareness programmes for the private sector, public sector and civil society and the development of awareness of cyber risks and available solutions.

In this regard, SAPSOs are not in line with the NCPF because the awareness of cyber risks in the organisations is poor and the approach to cybersecurity awareness programmes is not prioritised, not enforced, and attendance, at a rare occasion when awareness is conducted, is very low. Moreover, there is a lack of support for good practices to manage cyber risks and poor compliance with or unfamiliar with ICT security policies and procedures. The majority of the SAPSOs have not considered assessing the level of cyber risks awareness within the organisation. Additionally, these SAPSOs have never conducted cybersecurity awareness programmes. This finding is corroborated by the survey results which indicated the lack of awareness among employees in most organisations; which then leads to security not taken seriously by management and employees.

A cybersecurity awareness programme lays a foundation for a strong security posture of the organisation. Without an awareness programme, therefore, this indicates that employees including management are oblivious of the cyber risks that they may face as an organisation

and individually, of which this could also have an impact on the organisation. Even robust technological security solutions can be weakened due to the weakness in the human factor.

The NCPF acknowledges “a need to create an enabling environment for cybersecurity training, education, research and development and skills development programmes in South Africa”. To be cyber resilient implies that cyber workforce must be highly-skilled and qualified, provided with continuous proper training which comes with assessments and certifications at the end of the training. The findings revealed that the majority of SAPSOs have not provided their IT or ICT security employees with proper cybersecurity training. Finding also revealed that some SAPSOs have informal training and this kind of training does not have assessments and certification. These findings are reflected in the survey results, which indicated that SAPSOs have insufficiently skilled employees to apply cybersecurity. South Africa is still developing in the areas of professional training courses and education programmes.

### 5.5 Detect

This core function focuses on developing and implementing appropriate activities to rapidly identify the occurrence of cybersecurity events, evaluating information systems that may be affected and make sure that there is a prompt response (NIST 2017; Symantec 2014).

Anomalies and events are about timeous detection of abnormal activities that do not match up to systems behaviour or performance, and the understanding of the possible impact of events by everyone in the organisation (NIST, 2017; Choudhary, 2017). For organisations to effectively assess and advance their resilient networks, they need to establish and maintain a baseline of network operations and expected data flow that supports critical functions and services.

A baseline of network operations of systems and technology assets comprise documented information of basic settings, configurations and performances that represent a normal network architecture behaviour of an organisation. The baseline is continuously reviewed and maintained. The baseline of network operations also depicts how data flows through

the networks. This research study found that only half of the SAPSOs have an established baseline of network operations and expected data flow. They establish a baseline of network operations when the network performance level is at the peak, and this is considered normal performance so that it will assist in identifying and detecting anomalies on the network and data flow to determine if malicious activities are taking place. However, documentation, maintenance and reviewing of the baseline seem to be a challenge for most SAPSOs.

O'Neill (2016) asserts that documenting baseline readings for network traffic is the foremost course of action to efficiently identify potentially suspicious activities. Kerravala (2016) and AlienVault (2018) agree, stating that it is critical to establish a network baseline for what amounts to normal performance of the network. This study found as well that there are SAPSOs who are contrary to the literature, which indicates that these SAPSOs have not established the baseline of network operations and data flows. This implies these SAPSOs will not be able to easily identify and detect anomalies in their network and compare them with the normal performance for spotting the deviation on the network infrastructure, including traffic flow. Therefore, unidentified or undetected vulnerabilities and attacks can last an extended period and be very costly to the organisations.

Security continuous monitoring is about the identification of cybersecurity events and verifying the effectiveness of defensive measures through the monitoring of information systems at discrete intervals (NIST, 2017). After establishing the baseline of network operations and data flows, organisations need to have network detection and monitoring procedures, processes, and controls in place; as well as perform vulnerability assessment and penetration testing.

One of the crucial components of the core function ‘detect’ is network monitoring and detection processes and controls because it identifies, detects, and alerts the organisation of cyber threats, cyber-attacks, or any attempts to compromise the network. Anderson (2017) states that effective ways to analyse and prevent cyber incidents are to conduct continuous monitoring and searches for threats. Effective and efficient network monitoring and detection necessitate the use of integrated technologies (Tenable Network Security, 2013). Technologies such as proactive, automated intrusion detection system (IDS) and Intrusion

prevention system (IPS), security information and event management (SIEM) tools, and appropriate monitoring of the network usage, which can always be compared to the network baseline as stated in earlier in this section. The IDS, IPS and SIEM can analyse the anomalies in the network system.

The findings of this research study are in line with the literature, revealing that SAPSOs have processes and controls in place for continuous network detection and monitoring. Although SAPSOs were not comfortable to mention the type of technologies they use; the research study discovered that SAPSOs rely mostly on automated tools, which automatically analyse all events for any irregular activities occurring on the system. In some cases, an analysis is done manually or by a third-party. However, very few of the SAPSOs do not undertake the analysis of the anomalies.

Some SAPSOs acknowledged the challenges of the automated tools such as the tools that can identify lots of incidents and potential threats that they found it difficult to analyse all of them because of lack of capacity and capability. Another challenge was that the tools also alert to false positives.

Another key component, which provides proactive cyber defence is vulnerability assessment and penetration testing (Goel & Mehtre, 2015). Vulnerability assessment and penetration testing (VAPT) is a structured investigation and analysis of the security posture of the information systems (Gupta & Kaur, 2013). VAPT is a two-part process, vulnerability assessment (VA) and penetration testing (PT), that can be performed separately or integrated, and for better knowledge of security status. This research study found that SAPSOs perform regular VAPT and the executive managements have the knowledge and approve of the VAPT. The VAPT is conducted in two ways, first, they are conducted internally and secondly, the SAPSOs make use of third-parties to conduct VAPT for verification purposes.

## 5.6 Respond and Recover

This core function focuses on developing and implementing appropriate measures involving people, systems, and processes to detect, respond to and restore any capabilities or services that were impaired due to a cybersecurity event (NIST 2017; PWC 2010).

Cyber resilience requires a prompt and effective response to cyber incidents; therefore, organisations need to have an adequate incident response plan (IRP) in place which incorporates business continuity plan (BCP), disaster recovery plan (DRP) and cyber incident response plan. An effective IRP is documented and approved by the executive management; regularly tested, reviewed, and updated; as well as clearly communicated (ASIC, 2015). The IRP outlines how to manage cyber incidents and it can assist the organisations to restrain impacts should any cyber incident occurs and thereby reducing the cost of that incident to the organisation compared to the increased cost that could have been accumulated if without IRP. IRP also explicitly refer to recovery activities to timely restore systems to normal operations or to a pre-defined, acceptable level.

This research study found that none of the SAPSOs has a robust IRP in place because it does not incorporate a business continuity plan, a disaster recovery plan, and a cyber incident response plan (or cyber incident policy or cyber incident procedure as it is referred to by some participants). Furthermore, it was discovered that the existing IRP either misses one of the following: clear communication to relevant stakeholders, regular testing, regular review, or regular update The SAPSOs use and manage the plans separately. The finding is consistent with the literature, for instance, Ewing (2017) asserted that most organisations are still regarding IRP, DRP and BCP as distinct functions.

On the other hand, there are some SAPSOs that either had the business continuity plan only or did not have an IRP at all. The implications of this finding are that these SAPSOs will not be able to manage, respond to and recover from cyber incidents. This finding is corroborated by the results from the survey which show that more than half of SAPSOs would not be able to respond to cyber incidents.

As indicated in Chapter 4, Section 4.7.2, effective, timely and proactive communication is a critical part of the incident response plan. Organisations need to have a communication plan in place as to how they will communicate and coordinate response activities with stakeholders; notify clients, employees, and law enforcement of incidents; information sharing with other organisations. Data breach notification set out a procedure to be followed in an event of a data breach or when a data breach is suspected to have occurred. This procedure outline steps to take in notifying employees and clients about the breach of their personal and sensitive data, as well as notifying law enforcement agencies of all the data breaches and cyber incidences subsequent to a discovery by an organisation.

The research findings revealed that none of the SAPSOs has an effective data breach notification policy in place. However, it was discovered that a procedure to notify about a data breach is covered by other security documents such as Acceptable Use Information Security Policy, Disaster Recovery Plan, and other related documents. Moreover, clients are not notified of a data breach that exposes their personal or sensitive information to cyber risks. South Africa does not enforce privacy laws nor mandate organisation to notify clients, customers, employees about data breaches, therefore no organisation is forced to disclose about a data breach, and clients will have no knowledge that their personal or sensitive information is at risks.

Information sharing forms part of the response plan and it is critical in mitigating cyber risks. It is about organisations participating in information sharing forums and sources as well as collaborating with organisations across all sectors to exchange information on cyber threats and attacks; appropriate mitigation measures; best practices; and can ensure coordination in countering cyber-attacks. Information sharing can be voluntary as well to address cybersecurity awareness in a broader way. This research study found that SAPSOs do not have information sharing as part of the IRP and currently, SAPSOs do not voluntarily share information with any organisation.

As indicated in Chapter 4, organisations need to conduct a post-incident analysis to ensure satisfactory response and recovery activities (NIST, 2017). In addition to the analysis

conducted in Section 4.7.3, post-incident or event analysis should be conducted to determine the root cause of the incident.

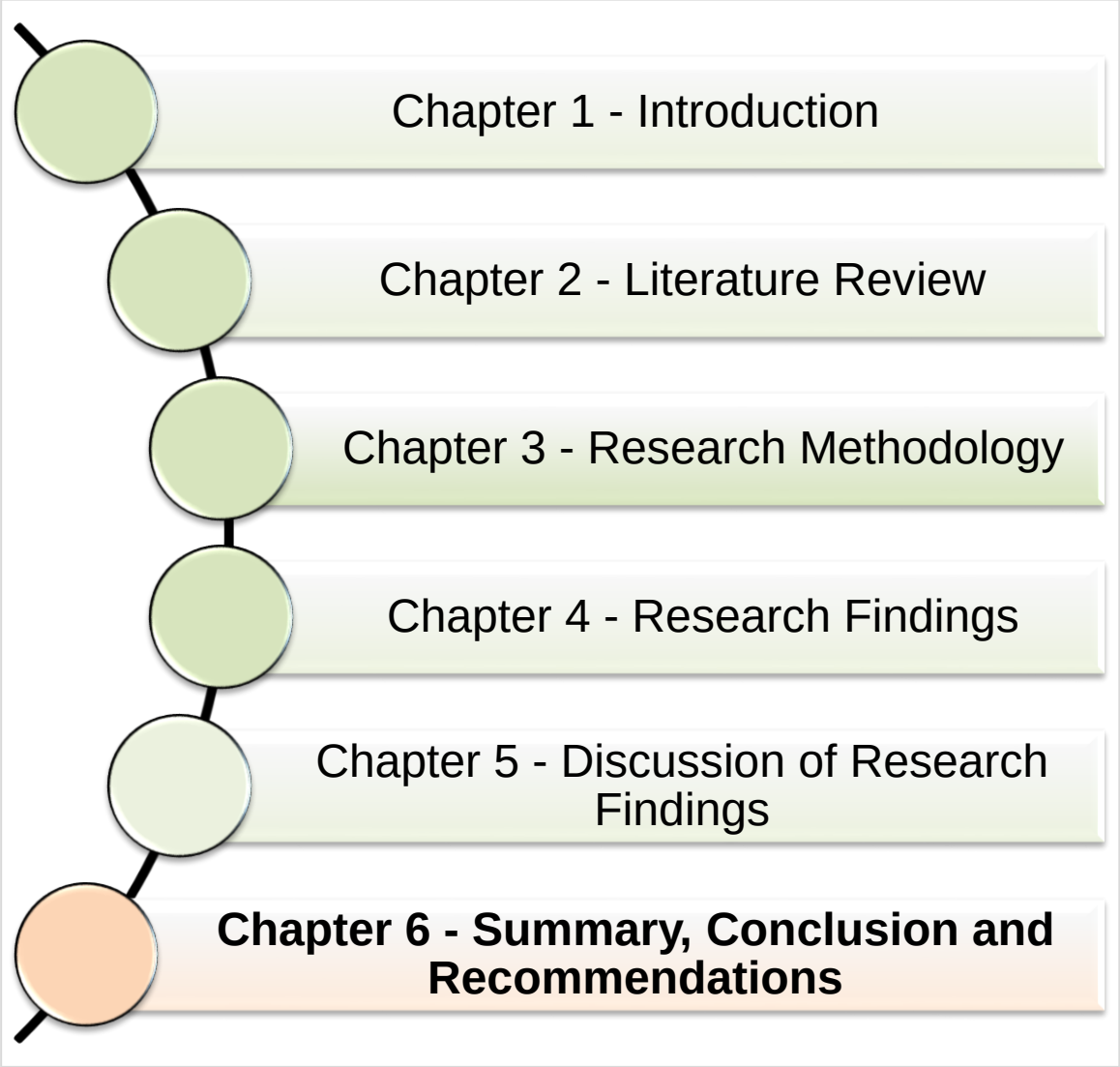
The research finding revealed that forensic investigation is conducted after a cyber incident by either the internal forensic unit and subsequently substantiated by a third-party forensic specialist or is exclusively conducted by a third-party forensic specialist such as KPMG or law enforcement agencies. The researcher could not determine if the incident reports were compiled and included the lessons learned so that the report can be used as a case study and as part of training and planning for future cyber incidents.

## 5.7 Conclusion

This chapter discussed the research findings, which combined the two data sources, primary, in the form of interviews and secondary, in the form of a survey, in order to draw valid inferences as well as strengthen the understanding of the research topic. These findings were linked to the literature review to support the outcomes of the findings.

The next chapter responds to the research questions that were posed in Chapter 1. It will also provide recommendations for further research, the limitations of the study and finally presents the conclusion.

# 6. CHAPTER 6 – RESEARCH SUMMARY, RECOMMENDATIONS AND CONCLUSION



## 6.1 Introduction

The objective of this study was to assess cyber resilience of public sector information systems against cyber risks. To achieve this objective, the researcher adopted a qualitative method and interpretive approach to collect and analyse data. The researcher used two methods of data collection, the primary source in a form of semi-structured, face-to-face interviews with eleven participants from SAPSOs in the Gauteng Province; and the secondary source in a form of a survey's raw dataset and survey report. The latter was unpublished when received and pertained to ten SAPSOs in the Gauteng Province. Thematic coding was used for data analysis. Furthermore, data triangulation was used to strengthen and validate the thematic findings. This was accomplished by comparing the thematic finding from the primary source with the statistical results from the secondary source.

The rest of the chapter addresses the research questions, discusses the limitations as well as make recommendations for future research.

## 6.2 Research Questions

In Chapter 1, the researcher raised a set of questions to address the topic of this study "Assessing Cyber Resilience of Public Sector Information Systems – A South African Perspective". This section will provide answers to the research questions based on the research findings and the literature review. The sub-questions will be addressed first and followed by the main research question.

### 6.2.1 Sub-question 1 – what are the cyber risks that South African public sector organisations may face?

Chapter 2, Section 2.3 listed nine possible cyber risks to SAPSOs and three principal risks that could result from a cyber incident. The SAPSOs are aware that, since they make use of the internet to pursue their mandate, and are dependent on a variety of third-party service providers such as technology vendors that they are exposed to cyber risks. SAPSOs failed

to identify the possible cyber risks that they may face but look at all cyber risks. In view of that, and given the cyber incidents to PSOs in South Africa as illustrated in Chapter 2, SAPSOs may be exposed to the following cyber risks:

- Hacktivism – literature has shown that hacktivism acts directed towards SASAPSOs are escalating. This is a cyber risk that is mostly reported through the media.

- Data breaches – another area of cyber risks that is seemingly gaining momentum.

- Restricted availability of online services – this is mostly directed at the SAPSOs' website, making them inaccessible.

- Third-party service providers, legacy systems and applications, and outdated software –potentially exposing SAPSOs to various cyber risks such as data manipulation, data exposure or theft and identity theft.

Furthermore, SAPSOs are more at (cyber) risks because they have no cybersecurity strategy; no defined cybersecurity roles and responsibilities from the executive management and senior management; no processes in place to assess data sensitivity; they have inadequate incident response and recovery plans; failure to identify and prioritise on possible cyber risks as specific to the organisation; and lastly, insufficient resources - insufficient budget for improved technology security solutions, poor cybersecurity awareness programmes, and lack of properly trained and skilled cyber workforce. In an event of a successful cyber-attack, the SAPSOs could face business operational risk, reputational risk, and litigation risk.

### 6.2.2 Sub-question 2 – what are the current cyber threats and the impact of cyber-attacks on the South African public sector information systems?

The scale of cyber threats is escalating in the public sector and however, in South Africa many of the cyber incidents, especially in the public sector, are either under-reported or are not reported at all. Nevertheless, this study identified that out of the seven common cyber

threats to the public sector (globally), the South African public sector faces six of the seven cyber threats indicated in Chapter 2, Section 2.3.1:

- Phishing
- Malware
- Hacktivism
- Data breach
- Insider threat
- Cybercrime

The impact of cyber-attacks on the public sector information systems will be very devastating because none of the SAPSOs has a skilled cyber workforce and adequate and resilient incident response plan to effectively and efficiently recover all critical ICT functions and assets in the event of a cyber disruption. Not only can data breaches embarrass the SAPSOs for exposed citizens' or employee data, but can result in cyber criminals using the personal information to commit fraud or sell to other cyber actors to be used later for other reasons such as extortion.

Insufficient resources to deal with cyber risks, difficulty in identifying and detecting anomalies in ICT systems as well as the use of obsolete ICT systems for critical functions will have huge social and economic implications. Sometimes SAPSOs can be oblivious to or perceives as low the impact of cyber-attacks. However, the impact thereof can be damaging to other parties (for instance citizens, employees, third-party suppliers, partners, and so on) linked to that specific PSO. A data breach from PayCity (online traffic fine payments), for example, exposed personally identifiable information such as identity numbers, full names, email addresses and passwords and violated people's privacy.

### 6.2.3 Main Question – how cyber resilient are the information systems of the South African public sector organisations?

*Cyber resilience is the ability of information systems and the organisation to* ***anticipate, withstand, prepare for, respond to, recover from, adapt to, and evolve*** *to improve*

*capabilities in the face of, adverse conditions, cyber-attacks, cyber incidents, or compromise on cyber resources (Bodeau & Graubart, 2017; Clark-Ginsberg, 2017).*

And

*Cyber resilience = information security + cybersecurity + cyber risk management + business continuity + incident response.*

In view of the above, for an organisation to be cyber resilient, it must achieve all the seven cyber resilience goals: anticipate, withstand, prepare, respond, recover, adapt, and evolve.

Currently, SAPSOs are lacking in addressing cybersecurity and there is no indication whatsoever that they are moving towards cyber resilience or that cyber resilience is on their agenda.

It has been established from this study that none of the SAPSOs has a cybersecurity strategy in place. The SAPSOs have no dedicated cybersecurity structures in place to specifically deal with cybersecurity issues. The SAPSOs have no more than two people responsible for cybersecurity, and these people main responsibilities are with ICT, or ICT security or risk management. In addition, these people are insufficiently skilled to deal with cybersecurity matters because they have no formal cybersecurity training or qualifications. Moreover, there is a lack of properly defined cybersecurity roles and responsibilities. The majority of SAPSOs rely on third-party service providers for cyber expertise, which in turn can – in some respects - weaken SAPSOs' cybersecurity posture.

This study found a high-level of assumed executive management commitment to cybersecurity. Nonetheless, a lack of advanced cybersecurity defence tools and insufficient budget for improved technology resources are a continuing concern. SAPSOs have in their possessions huge amounts of critical data and information systems, of which the data can be lost and information systems crippled during a cyber-attack. Nevertheless, many of the SAPSOs still use legacy IT systems and outdated software or applications as well as have no data loss prevention plan. None of the SAPSOs has a robust incident response plan which incorporates a disaster recovery plan, business continuity plan and incident response plan.

The SAPSOs lack established and coordinated communication processes, partnerships, and information sharing. SAPSOs are deficient in an adequate data breach notification policy in order to communicate properly to employees, clients, stakeholders and law enforcement of any data breaches or cyber incidents that have been experienced.

There are no organisation-wide, continuous cybersecurity awareness programmes that promote a cyber culture and cyber aware organisation. This affects the posture of cybersecurity and cyber resilience of the SAPSOs.

None of the SAPSOs has considered testing their information systems for cyber resilience. This implies that the SAPSOs cannot verify whether they can respond to and recover their information systems at an acceptable time and access critical systems, network, and data.

For SAPSOs, cyber resilience = information or ICT security policies or procedures + no cybersecurity strategy and limited cybersecurity programmes + no established organisation-wide cyber risk management + inadequate business continuity management + inadequate incident response.

Therefore, SAPSOs they are unaware of how poorly they are prepared and they lack the capacity and the capability to anticipate, withstand prepare for, respond to, and recover from any cyber incident. Many of the SAPSOs will not be able to recover critical systems to normal operations at an acceptable level and time.

### 6.2.4 Sub-question 3 (recommendations) – what are the measures in place for the South African public sector organisations to mitigate cyber risks?

There is no single solution to cyber resilience. Different approaches are prescribed by different standards, frameworks, or best practices. However, an organisation needs to develop its own cyber resilience framework or programme (CRF/P) that fits and talk to the organisation's strategic objectives. Organisations can determine whether to adopt or align their CRF/P and cybersecurity strategy to industry standards, frameworks, and best practices. The approach to cyber resilience cannot be siloed, it needs to be institutionalised and operationalised, that is, integrated into the organisation's success factors: People,

Processes and Technology. Cyber resilience is as much about people and processes as it is about technology.

## A. People

**The Executive / Board** – Cyber resilience starts from the top. The executive management buy-in and commitment is critical. The executive management must define and assign roles and responsibilities to establish and oversee CRF/P. They need to take ownership of the cyber risks that the organisation may face as well as ownership of cyber risk management. They must ensure the development and implementation of an organisation-wide continuing culture of cybersecurity and cyber resilience awareness programmes that put emphasis on cyber risks and available solutions. There must be, at least, one member of the Executive or the Board who will take overall responsibility for cyber resilience. The executive management must foster partnerships with the private sector, academia and other SAPSOs to share information on threat intelligence, solution, and skills development.

The Executive or the Board needs to continuously ask themselves these key questions: (i) What are the potential or current cyber risks (that is, looking at vulnerabilities, cyber threats, and impact) to the organisation? (ii) what is the likelihood of these cyber risks? (iii) what will be the potential impact to the organisation (looking at the financial loss, disruption or damage to the systems, reputational damage and so on)? (iv) which controls are required for cyber risks mitigation? (v) what are the required resources to invest in? (vi) are our current policies, frameworks, standards, processes protect our most critical assets and provide recovery and continuity of the systems after a cyber incident?

**All employees –** the first line of defence and foundation to a resilient organisation is to have all employees being aware of the cyber risks to the organisation and their roles and responsibilities to mitigate the cyber risks. Effective cyber resilience depends on people with the correct knowledge, skills, attitude, and culture because without all the mentioned traits and good processes, the investment to advanced technologies will be futile.

**Cyber workforce –** SAPSOs must invest in:

- Sufficiently skilled, dedicated cyber workforce;
- technical cyber training to have skilled personnel dedicated to achieving effective cybersecurity and cyber resilience, scenario-based /simulation training;
- training that will address the required competencies (knowledge, skills, and attitude) of specific functions in cybersecurity and cyber resilience; and
- simulation and emulation training exercises such as a tabletop, wargames, blue team/red team to enhance cyber technical skills.

## B. Process

The processes of the organisations answer to the following questions: Who? What? Why? Where? When? and How? to achieve the desired end. Processes are sets of actions or steps or procedures an organisation need to take to achieve its strategic objective. The process focuses on identifying, developing, and implementing strategies, policies, processes and procedures, standards, best practices and so on. This success factor affords an organisation with an ability to design, develop, and implement, suitable processes to achieve cyber resilience. Without those policies, frameworks, programmes, or guidelines a proper direction for cybersecurity and cyber resilience approach will be inadequate.

To be cyber resilient, SAPSOs need to have appropriate, robust, and clearly communicated strategies, policies, plans, processes, and frameworks, in place. These must be regularly tested, reviewed, and updated. They must clear on defining roles, responsibilities, and level of authority:

- Cybersecurity strategy;
- cyber resilience framework/programme;
- business continuity management;
- disaster recovery management;
- incident response plan;
- data loss prevention plan;

- cyber risk assessment processes and cyber risk management;
- (cyber) legal and compliance; and
- education, training, and development strategy (strategy on how to approach cyber awareness, cyber training and cyber research and development, skilling, upskilling and reskilling).

Therefore, these will provide guidance for organisations to determine and prioritise their key components of cyber resilience such as:

- Asset management – identifying organisation critical systems, network, and data;
- cyber threats identification and vulnerability management;
- continuous monitoring;
- logical and physical control management;
- training and awareness;
- incident response;
- third-party risk management;
- adopting a defence in depth approach: user security, application security, network security, operation system security, data security, physical security, secure configuration, etcetera, and.
- identify technologies to be used for the protection of critical systems, networks, and data.

### C. Technology

SAPSOs need to invest in essential new technology security solutions and tools that are key to achieving cyber resilience. Technology that will assist in assessing cyber threats – in speed, severity, and volume, and at the same time afford an ability to reduce the time to identify, detect, mitigate, and contain; and respond and recover. SAPSOs need to implement technologies that will monitor and record, for both digital and physical activities. They must keep software and applications up-to-date. There are several types of tools and advanced technologies that SAPSOs need to consider for detection of cyber threats; prevention, protection and recovery from cyber incidents ranging from next-generation firewalls to

intrusion detection and intrusion prevention systems, from Security analytics to security information and event management, from advanced threats and deep packet detection and inspection to network security monitoring and network traffic analysis from secure configuration to encryption, from file integrity checking software to deception technologies and so on.

### D. External dependencies (Third-party service providers, partners, contractors)

External dependencies can bring various cyber risks to the organisation. It is essential that SAPSOs must make it their business to examine the cybersecurity and cyber resilience posture of the external dependencies. SAPSOs must understand the cyber risks faced by the external dependencies and analyse their cyber risk management to establish appropriate countermeasures to protect critical assets. SAPSOs need to have an external dependency risk management plan incorporated to their enterprise risk management. It is also critical that proper and detailed security investigation is conducted on the external dependencies prior to the signing of agreements or contracts. Cyber risks and cyber resilience of the external dependencies must be addressed throughout the life cycle of the relationship between the PSO and external dependencies.

## 6.3 Research Limitations

The study had the following limitations:

- It is worth noting that to date, there is no research conducted, in a South African context, to investigate and determine the cyber resilience of any SAPSOs. There is insufficient information available regarding the state of cybersecurity readiness of SAPSOs of which some of this information cannot be verified for reliability because the information is neither supported nor confirmed by the government. This has limited the verification of the research findings. In addition, globally, there is limited published industry or academic research relating to the topic.

- Another limitation to note is that the topic of cybersecurity was considered to be "too sensitive" by most of the organisations that were requested to participate. Hence the researcher could not meet the desired sample size of 34, from 35 public sector organisations that were invited to participate.

- The study was limited to the Gauteng Province.

## 6.4 Recommendations for Future Research

Cyber resilience is a relatively new area in the cyber field; published academic and industry research on this topic in relation to South Africa is very limited or non-existent. The concept of information systems resilience will have implications for the design of information systems and for policy-makers. Therefore,

1. Future research on cyber resilience that can be extended to SAPSOs in all provinces can provide valuable insight on cyber resilience status or readiness nationally and/or the respective (other) provinces. To inform cyber resilience on a national level, research in other sectors would be equally valuable.

2. ICT governance (in relation to information systems (IS) governance) is at the top agenda of every national organisation as prescribed by the Department of Public Services and Administration, therefore more research is needed to extend the ICT (IS) governance to ICT (IS) resilience.

3. Some SAPSOs adopted or are considering adopting the NIST Cybersecurity Framework as a guideline or response to cybersecurity, therefore it would be of great importance to look at the weaknesses of NIST's framework and other frameworks, standards, guidelines towards building and assessing resilient information systems.

4. Cybersecurity awareness approaches are still lacking within the organisations, research is needed in formulating an organisational cybersecurity awareness framework that promotes cyber resilience culture.

5. Lastly, research on developing a cyber resilience framework and best practice guidelines or assessment tools that the SAPSOs can use as a baseline would constitute a contribution of critical importance.

## 6.5 Conclusion

The scope of this research study was to assess the cyber resilience of the South African public sector organisations Due cognisance is taken of the fact that there is no complete protection from ever-escalating and sophisticated cyber threats and cyber-attacks. However, cyber resilience offers a robust, comprehensive and risk management-based solution to counter cyber threats and cyber-attacks as well as mitigate the accompanying risks.

This research found that South African public sector organisations are more exposed to cyber risks because they don't have adequate security controls in place - starting with a fundamental such as having a cybersecurity strategy. A main cyber risk that the South African public sector organisations are exposing themselves to is not assessing the cybersecurity posture or cyber resilience of their third-party service providers or at the most conducting cyber risk assessments of the third-party service providers.

One of the biggest challenges facing the South African public sector organisations and which could be the hindrance in advancing cybersecurity and cyber resilience programmes, is under-reporting or no reporting at all of their experiences of cyber incidents. Hence there is no "reliable" information that can make other organisations aware to improve on their security approaches and solutions. This proves the lack of collaboration within the South African public sector organisations and with other sectors.

Despite the under-reporting, at least two of the cyber threats that have been identified and gaining momentum have resulted in successful cyber incidents, that is, hacktivism and data breaches. The data breaches are because of third-party service providers. This also indicates a lack of data protection and data privacy regulations and compliance.

In an event of a disastrous cyber incident, the South African public sector organisations would not be able to withstand, respond, and recover their critical systems, networks, and data to normal operations at an acceptable level and time. This is because the South African public sector organisations lack the capacity and the capability to anticipate, prepare and identify cyber risks. The plans that the South African public sector organisations have, that is, business continuity, disaster recovery, incident response need to be integrated into a cyber resilience plan that will be tested regularly to challenge it, find gaps as well as learning from the drills. The drills will also assist in problem or incident solving and improving the cyber resilience plan as the number and frequency of sophisticated cyber risks keeps escalating.

For the South African public sector organisations to be resilient, they need to address the basic requirements for cybersecurity such as developing and implementing a cybersecurity strategy and incident response plan, they need to invest in suitable qualified cyber workforce and cybersecurity education, training, and awareness programmes, invest in advanced technological security solutions and promote and implement a cyber risk management-based approach. Without implementing these controls, a proper direction for cybersecurity and cyber resilience approach will be deficient.

Cyber resilience of information systems cannot be achieved without proper planning, adequate resources and of the utmost importance, the interrelationships of critical factors of information systems and information systems resilience: people, processes and technology cannot be ignored. Cyber resilience therefore needs to be regarded as a critical strategic objective in the evolution of digital South African public sector organisations because it is a major factor in a rapid successful recovery and continued operations of information systems. It is critical that the South African public sector organisations not only ensure the protection of critical services and information systems but that there will be continued service delivery even in the event of a cyber incident.

# 7. REFERENCES

Ablon, L., 2018. Data Thieves The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data. [Online] Available at: https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT490/RAND_CT490.pdf [Accessed 18 August 2018].

Accenture, 2017. Cyber Threatscape Report: Midyear Cybersecurity Risk Review Forecast and Remediations. [Online] Available at: https://www.accenture.com/za-en/insight-cyber-threat-scape-report-2017 [Accessed 23 January 2018].

Ahmad, S. Z. & Khalid, K., 2017. The adoption of M-government services from the user's perspectives: Empirical evidence from the United Arab Emirates. International Journal of Information Management, 37(5), pp. 367-379.

Al Mourad, M. B. & Hussain, M., 2014. The Impact of Cloud Computing on ITIL Services Strategy Process. International Journal of Computer and Communication Engineering, 3(5), pp. 367-371.

Alhabeeb, M., Almuhaideb, A., Le, P. D. & Srinivasan, B., 2010. Information Security Threats Classification Pyramid. Perth, WA, Australia, 2010 IEEE 24th International Conference on Advanced Information Networking and Applications Workshops. IEEE, pp. 208-213.

Ali, S. M. & Soomro, T. R., 2014. Integration of Information Security Essential Control into Information Technology Infrastructure Library - A Proposed Framework. International Journal of Applied Science and Technology, 4(1), pp. 95-100.

AlienVault, 2018. USM Anywhere User Guide: Establishing Baseline Network Behavior. [Online] Available at: https://www.alienvault.com/documentation/usm-anywhere/user-guide/getting-started/baseline-network-behavior.htm [Accessed March 2018].

Alshammari, T., Cheung, Y. & Messom, C., 2018. M-government Adoption Research Trends: A Systematic Review. Sydney, Australi, Australasian Conference on Information Systems.

Alshammari, T., Cheung, Y. & Messom, C., 2018. M-government Adoption Research Trends: A Systematic Review. Sydney, Australia, Australasian Conference on Information Systems.

Anderson, E., 2017. Blog: How to Comply with the 5 Functions of the NIST Cybersecurity Framework. [Online] Available at: https://www.secmatters.com/blog/how-to-comply-with-the-5-functions-of-the-nist-cybersecurity-framework [Accessed 13 March 2018].

Antonucci, D., 2017. The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities. Hoboken, New Jersey: John Wiley & Sons, Inc.

Armasu, L., 2018. Backdoors Keep Appearing in Cisco's Routers. [Online] Available at: https://www.tomshardware.com/news/cisco-backdoor-hardcoded-accounts-software,37480.html [Accessed 20 July 2018].

Arraj, V., 2013. ITIL: the basics White Paper, London: AXELOS.

ASIC, 2015. Cyber resilience: Health check. [Online] Available at: https://download.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf [Accessed 10 October 2015].

Avison, D. E. & Myers, M. D., 1995. Information systems and anthropological perspective on IT and organizational culture. Information Technology & People, 8(3), pp. 43-56.

Bhattacherjee, A., 2012. Social Science Research: Principles, Methods, and Practices, 2nd edition. 2nd Edition ed. Florida: Textbooks Collection 3.

Björck, F., Henkel, M., Stirna, J. & Zdravkovic, J., 2015. Cyber Resilience – Fundamentals for a Definition. New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Com, Volume 353, pp. 1-7.

Björck, F., Henkel, M., Stirna, J. & Zdravkovic, J., 2015. Cyber Resilience – fundamentals for a definition. ResearchGate, Published by Springer, pp. 1-7.

Blackman, A., 2014. The Main Types of Business Risk. [Online] Available at: https://business.tutsplus.com/tutorials/the-main-types-of-business-risk--cms-22693 [Accessed 27 January 2019].

Boddy, C. R., 2016. Sample size for qualitative research. Qualitative Market Research, 19(4), pp. 426-432.

Bodeau, D. & Graubart, R., 2017. Cyber Resiliency Design Principle. [Online] Available at: https://www.mitre.org/publications/technical-papers/cyber-resiliency-design-principles [Accessed 8 October 2017].

Boslaugh, S., 2008. Target Population in Encyclopaedia of Epidemiology. Thousand Oaks (CA): SAGE Publications, Inc.

Breakfast, S., 2018. The South African: A hacker has claimed responsibility for attack on Environmental Affairs website Another government website was down as a result of apparent hacking. [Online] Available at: https://www.thesouthafrican.com/environmental-affairs-website-cyber-attack/ [Accessed 12 September 2018].

Brown, G., 2013. Cyber Resilience – Implementing the Right Strategy. [Online] Available at: http://csd.ncb.mu/English/Pages/Presentations/Mauritius%20Event%20Dec2013v1%20Symantec.pdf [Accessed 27 February 2018].

Buckingham, R., Hirschheim, R., Land, F. & Tull, C., 1987. Information Systems Education: Recommendations and Implementation. Cambridge: Cambridge University Press.

Burmeister, O. K. J., Phahlamohlaka, J. & Al-Saggaf, Y., 2014. National security governance exemplified by South Africa's cyber security policy implementation. [Online] Available at: http://researchspace.csir.co.za/dspace/handle/10204/7615 [Accessed 4 April 2015].

Caballero, A., 2017. Information Security Essentials for Information Technology Managers: Protecting Mission-Critical Systems. In: J. R. Vacca, ed. Computer and Information Security Handbook. Third Edition. s.l.: Morgan Kaufmann, pp. 393-419.

Chacko, L., Herbolzheimer, C. & Sekeris, E., 2016. Quantifying Cyber Risks: can you put a dollar amount on your company's cyber risk? Oliver Wyman Risk Journal, Volume 6, pp. 1-4.

Check Point Research, 2018. 2018 Security Report: Welcome to The Future of Cyber Security. [Online] Available at: https://www.checkpoint.com/downloads/product-related/report/2018-security-report.pdf [Accessed 30 September 2018].

Cheng, L., Liu, F. & Yao, D., 2017. Enterprise data breach: causes, challenges, prevention, and future directions. WIREs Data Mining and Knowledge Discovery published, Volume 7, pp. 1-14.

Cherdantseva, Y. & Hilton, J., 2013. A Reference Model of Information Assurance & Security. Regensburg, Germany, 8th International Conference on Availability, Reliability and Security (ARES).

Choudhary, P., 2017. DataScience.com: Introduction to Anomaly Detection. [Online] Available at: https://www.datascience.com/blog/python-anomaly-detection [Accessed February 2018].

Ciampa, M., 2017. Security Awareness: Applying Practical Security in Your World. Boston: Cengage Learning.

Cisco, 2017. Cisco 2017 Midyear Cybersecurity Report. [Online] Available at: https://www.cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html [Accessed February 2018].

Clark-Ginsberg, A., 2017. Technial Report: What's the Difference between Reliability and Resilience? [Online] Available at: https://www.researchgate.net/publication/320456274_What%27s_the_Difference_between_Reliability_and_Resilience [Accessed 9 June 2018].

Clark, V. & Ivankova, N., 2016. Why use mixed methods research?: identifying rationales for mixing methods. In: Mixed methods research: A guide to the field. Thousand Oaks: SAGE Publications Ltd, pp. 79-104.

Cohen, L., Manion, L. & Morrison, K., 2007. Research Methods in Education. 6th Edition ed. New York: Routledge.

Creswell, J. W., 2003. Research Design Qualitative, Quantitative, and mixed methods approaches. 2nd Edition ed. California: SAGE Publications.

Cybersecurity Insiders, 2017. Insider Threat 2018 Report. Crowd Research Partners. [Online] Available at: http://crowdresearchpartners.com/wp-content/uploads/2017/07/Insider-Threat-Report-2018.pdf [Accessed 23 February 2018].

Dagada, R. & Eloff, M. M., 2013. Integration of policy aspects into information security issues in South African Organisations. African Journal of Business Management., 7(31), pp. 3069-3077.

Dalton, W., Jansen van Vuuren, J. & Westcott, J., 2017. Building Cybersecurity Resilience in Africa. Dayton, USA, ICCWS 2017 12th International Conference on Cyber Warfare and Security, pp 112-120. Academic Conferences and Publishing International Limited.

Daniel, J., 2012. Sampling Essentials: Practical Guidelines for Making Sampling Choices. Thousand Oaks (CA): SAGE Publications, Inc.

Davis, S., 2015. Though Leadership: Combating Cybercrime. [Online] Available at: http://www.wbsjournal.co.za/articles/combating-cybercrime-919.html

de Crespigny, M., 2012. Building cyber-resilience to tackle threats, s.l.: Network Security.

de Crespigny, M., 2012. Building cyber-resilience to tackle threats. Network Security Volume, Issue 4, pp. 5-8.

Death, D., 2017. Information Security Handbook: Develop a threat model and incident response strategy to build a strong information security framework. Birmingham: Packt. Publishing.

Del Giudice, M. & Wilkinson, C., 2016. Cyber Resilience – Going Beyond Security to a New Level of Readiness. [Online] Available at:

https://www.crowehorwath.com/insights/asset/cyber-resilience-readiness-level/ [Accessed 4 November 2016].

Denning, D. E., 2001. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. In: Networks and Netwars: The Future of Terror, Crime, and Militancy. s.l.: RAND Corporation, pp. 239-288.

Devlin, R., 2016. Data Loss Prevention, s.l.: The SANS Institute.

Dimension Data, 2017. The Executive's Guide to the 2017 Global Threat Intelligence Report: Cybersecurity insights for protecting your digital business. [Online] Available at: https://www.google.com/search?client=safari&rls=en&ei=QBWdXIzgAomCjLsPrJauuAY&q=The+Executive%E2%80%99s+Guide+to+the+2017+Global+Threat+Intelligence+Report%3A+Cybersecurity+insights+for+protecting+your+digital+business&oq=The+Executive%E2%80%99s+Guide+to+ [Accessed 24 February 2018].

Dlamini, Z. & Mapule, M., 2012. Cyber Security Awareness Initiatives in South Africa: A Synergy Approach. Seattle, 7th International Conference on Information Warfare and Security.

Donaldson, S. E., Siegel, S. G., Williams, C. K. & Aslam, A., 2015. Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats. s.l.: A press.

DTPS, 2017a. Department of Telecommunications and Postal Services. National e-Government Strategy and Roadmap. [Online] Available at: https://www.gov.za/sites/default/files/41241_gen886.pdf [Accessed 13 March 2018].

DTPS, 2017a. Department of Telecommunications and Postal Services. National e-Government Strategy and Roadmap. [Online] Available at: https://www.gov.za/sites/default/files/41241_gen886.pdf [Accessed 9 March 2018].

DTPS, 2017b. National Cybersecurity Readiness Survey, Pretoria: DTPS.

Dudovskiy, J., 2016. Research Methodology. [Online] Available at: https://research-methodology.net/about-us/ebook/ [Accessed 16 October 2017].

Dutton, J., 2017. Three pillars of cyber security. [Online] Available at: https://www.itgovernance.co.uk/blog/three-pillars-of-cyber-security/ [Accessed 17 November 2017].

Dworkin, S. L., 2012. Sample Size Policy for Qualitative Studies Using In-Depth Interviews. Archives of Sexual Behavior, Volume 41, pp. 1319-1320.

Edwards, J., 2017. Three Pillars of a Successful Security Strategy. [Online] Available at: https://solutionsreview.com/security-information-event-management/three-pillars-of-a-successful-security-strategy/ [Accessed 23 June 2018].

Eling, M. & Schnell, W., 2016. What do we know about cyber risk and cyber risk insurance? The Journal of Risk Finance, 17(5), pp. 474-491.

ENCA, 2016. UPDATE: Hackers shut down SABC websites. [Online] Available at: https://www.enca.com/south-africa/hackers-shut-down-sabc-websites [Accessed 7 June 2016].

ENISA, 2018. ENISA Threat Landscape Report 2017 15 Top Cyber-Threats and Trends. [Online] Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017 [Accessed 22 February 2018].

Fadilpasic, S., 2017. Security researchers uncover new global cyber espionage campaign in Beta News. [Online] Available at: https://betanews.com/2017/04/05/new-cyber-espionage-campaign/ [Accessed 5 November 2017].

Farbat, V., McCarthy, B. & Raysman, R., 2001. Cyber Attacks: Prevention and Proactive Responses, New York: Practical Law Publishing Limited.

Feng, N. & Li, M., 2011. An Information Systems Security Risk Assessment Model Under Uncertain Environment. Applied Soft Computing, Issue Elsevier, pp. 43332-4340.

Flick, U., 2007. Concepts of triangulation. In: Managing quality in qualitative research. London: SAGE Publications Ltd, pp. 38-54.

Flick, U., 2009. An Introduction to qualitative research. 4th Edition ed. London: Sage.

Fusch, P. I. & Ness, L. R., 2015. Are We There Yet? Data Saturation in Qualitative Research. The Qualitative Report, 20(9), pp. 1408-1416.

George, D., 2014. Press Release: Democratic Alliance. [Online] Available at: http://www.da.org.za/2014/08/pics-security-risk-following-website-hacking/ [Accessed 18 March 2015].

Gerić, S. & Hutinski, Ž., 2007. nformation system security threats classifications. Journal of Information and Organizational Sciences, 31(1), pp. 51-61.

GIBSON, D., 2011. Managing Risk in Information Systems. Sudbury: Jones & Bartlett Learning.

Giudice, M. D., 2016. Cyber resilience – going beyond security to a new level of readiness. [Online] Available at: https://www.crowehorwath.com/folio-pdf/Cyber-resilience-readiness-level_RISK-17005-004G.pdf [Accessed 23 October 2017].

Goche, M. & Gouveia, W., 2014. Forbes. Business. [Online] Available at: https://www.forbes.com/sites/sungardas/2014/01/15/why-cyber-security-is-not-enough-you-need-cyber-resilience/#6d9db1bc4bb6 [Accessed 15 August 2016].

Goede, R. & de Villiers, C., 2003. The applicability of Grounded Theory as Research Methodology in Studies on the use of Methodologies in IS Practices. Johannesburg, In Proceedings of the Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists (SAICSIT 2003): IT Research in Developing Countries, pp 208-217.

Goel, N. J. & Mehtre, B., 2015. Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology. s.l., Elsevier B.V.

Grobler, M., Jansen van Vuuren, J. J. & Leenen, L., 2012. Implementation of a cyber security policy in South Africa: Reflection on progress and the way forward. Berlin Heidelberg, IFIP International Conference on Human Choice and Computers, pp. 215-225. Springer., pp. 215-225.

Grove, 2018. Grove Aplied Intelligence: Recent Cyber Attacks in South Africa. [Online] Available at: https://www.groveis.com/blog/grove-mitigate-cyber-attacks-in-south-africa-mimecast-darktrace [Accessed 12 September 2018].

Guest, G., Namey, E. E. & Mitchell, M. L., 2013. Collecting Qualitative Data: A Field Manual for Applied Research. London: SAGE Publications, Ltd.

Gupta, A. & Kaur, K., 2013. Vulnerability Assessment and Penetration Testing. International Journal of Engineering Trends and Technology, 4(3), pp. 328-333.

HarvardX, 2018. Class notes: Harvard Cybersecurity: Managing Risk in the Information Age Online Short Course, s.l.: Harvards's VAP.

Heeks, R. & Ospina, A. V., 2019. Conceptualising the link between information systems and resilience: A developing country field study. Information Systems Journal, Volume 29, pp. 70-96.

Hendriks, C. J., 2012. Integrated Financial Management Information Systems: Guidelines for effective implementation by the public sector of South Africa. SA Journal of Information Management, 14(1.529), pp. 1-9.

Hox, J. J. & Boeije, H. R., 2005. Data Collection, Primary vs. Secondary. In: K. Kempf-Leonard, ed. Encyclopaedia of Social Measurement. s.l.: Elsevier/Academic Press, pp. 593-599.

Hua, J., Bapna, S. & Chen, Y., 2015. Industrial Cyber Espionage. Journal of Management Systems, 25(3), pp. 67-80.

IOL, 2017. IOL: BREAKING NEWS: Department of Basic Education website hacked. [Online] Available at: https://www.iol.co.za/news/breaking-news-department-of-basic-education-website-hacked-10015779 [Accessed 30 June 2017].

ISACA, 2012. COBIT 5 A Business Framework for the Governance and Management of Enterprise IT, Meadows: ISACA.

ISO 22301, 2012. Societal security - Business continuity management systems - Requirements. [Online] Available at: https://www.sis.se/api/document/preview/914731/ [Accessed January 2019].

ISO/IEC, 2013. ISO/IEC 27001:2013, Second edition, Information technology — Security techniques — Information security management systems — Requirements, s.l.: ISO/IEC.

ISO/IEC, 2018. Information technology — Security techniques — Information security risk management. [Online] Available at: https://www.sis.se/api/document/preview/80005503/ [Accessed January 2019].

ISO/IEC, 2018. ISO/IEC 27000:2018, Fifth edition, Information technology — Security techniques — Information security management systems — Overview and vocabulary, s.l.: ISO/IEC.

ISO/IEC27001:2013, n.d. [Online] Available at: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534

ITU, 2011. ITU National Cybersecurity Strategy Guide, Geneva: International Telecommunication Union.

ITWeb, 2013. Home: Governance, Risk and Compliance: ITWeb. [Online] Available at: http://www.itweb.co.za/index.php?option=com_content&view=article&id=62035#prcontacts [Accessed 8 June 2015].

Jansen van Vuuren, J., Leenen, L., Phahlamohlaka, J. & Zaaiman, J., 2013. Development of a South African Cybersecurity Policy Implementation Framework. Denver Colorado, USA, ICIW 2013 Proceedings of the 8th International Conference on Cyber Warfare and Security, pp 106-115. Academic Conferences International Limited.

Jaquire, V. & von Solms, S., 2017. Towards a Cyber Counterintelligence Maturity Model. Dayton, USA, Academic Conferences and publishing limited.

Jin-fu, W., 2009. E-government Security Management: Key Factors and Countermeasure. s.l., 2009 Fifth International Conference on Information Assurance and Security. IEEE.

Jouini, M., Rabai, L. B. A. & Aissa, A. B., 2014. Classification of Security Threats in Information Systems. Procedia Computer Science, Volume 32, pp. 489-496.

Kaur, S., Sharma, S. & SIngh, A., 2015. Cyber Security: Attacks, Implications and Legitimations across the Globe. International Journal of Computer Applications, 114(6), pp. 21-24.

Kerravala, Z., 2016. Broadband Wan: The Importance of Setting Network Baselines. [Online] Available at: http://blog.silver-peak.com/the-importance-of-setting-network-baselines [Accessed March 2018].

Khanyile, S. & Abdullah, H., 2012. COBIT 5: an evolutionary framework and only framework to address the governance and management of enterprise IT, Pretoria: University of South Africa (UNISA).

Kinkayo, 2017. Cyber Exposure Index. [Online] Available at: https://cyberexposureindex.com/introduction/ [Accessed 16 October 2017].

Klein, H. K. & Myers, M. D., 1999. A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. MIS Quarterly, 23(1), pp. 67-94.

Klopper, H., 2008. The qualitative research proposal. Curationis, 31(4), pp. 67-72.

Kneller, M., 2010. Executive Briefing: The Benefits of ITIL - White Paper, s.l.: The Stationery Office.

Korjan, N. & von Solms, R., 2014. A conceptual framework for cyber security awareness and education in SA. South African Computer Journal, Volume 52, pp. 29-41.

Koslowski, T. G., 2014. Resilience Management Information Systems-Achieving Sustainability in Turbulent Environments. [Online] Available at: https://d-nb.info/1123481008/34 [Accessed 23 February 2019].

Kosutic, D., 2010. Disaster recovery vs Business continuity. [Online] Available at: https://advisera.com/27001academy/blog/2010/11/04/disaster-recovery-vs-business-

continuity/?icn=free-blog-27001&ici=bottom-disaster-recovery-vs-business-continuity-txt [Accessed January 2019].

Kushchu, I. & Kuscu, H. M., 2003. From E-government to M-government: Facing the Inevitable. Dublin, Ireland, pIn the 3rd European Conference on e-Government, pp. 253-260. MCIL Trinity College.

Lannon, J., 2013. Students: Certified Public Accountants. [Online] Available at: http://www.cpaireland.ie/docs/default-source/Students/F2-Info-Systems/understanding-the-role-nbsp-and-the-impact-of-information-systems-on-today%27s-business-environment.pdf?sfvrsn=0 [Accessed 28 March 2015].

Larrocha, E. R. et al., 2010. Filling the gap of Information Security Management inside ITIL: Proposals for postgraduate students. Madrid, IEEE.

Laudon, K. C. & Laudon, J. P., 2007. Management Information Systems: Managing the Digital Firm. 10th ed. Upper Saddle River, NJ: Pearson Prentice-Hall.

Lehto, M., 2013. The Ways, Means and Ends in Cyber Security Strategies. University of Jyväskylä, Finland, Proceedings of the 12th European Conference on Information Warfare and Security: ECIW 2013. Academic Conferences Limited.

Lloyd, 2018. The Department of Labour acknowledges an attempted cyber-attack on its website. [Online] Available at: http://www.labour.gov.za/DOL/media-desk/media-statements/2018/the-department-of-labour-acknowledges-an-attempted-cyber-attack-on-its-website [Accessed 12 September 2018].

Malterud, K. & Siersma, V. D. G. A. D., 2016. Sample Size in Qualitative Interview Studies: Guided by Information Power. Qualitative Health Journal, 26(13), pp. 1753-1760.

Maphumulo, S., 2015. Apartheid spook ‘sold secrets’, Independent Online. [Online] Available at: https://www.iol.co.za/news/politics/apartheid-spook-sold-secrets-1828648 [Accessed November 2017].

Martin, B. C., 2002. Disaster Recovery Plan Strategies and Processes. Version 1.3. [Online] Available at: https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-strategies-processes-564 [Accessed 29 January 2019].

Mason, M., 2010. Sample Size and Saturation in PhD Studies Using Qualitative Interviews. Forum: Qualitative Social Research, 11(3).

Maxwell, J. A., 2012. Qualitative Research Design: An Interactive Approach. 3 Edition ed. Los Angeles: SAGE Publications.

Mbelli, T. M. & Dwolatzky, B., 2016. Cyber Security, a Threat to Cyber Banking in South Africa: An approach to Network and application security. Beijing, China, 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud), pp. 1-6.

McAfee, 2018a. Economic Impact of Cybercrime— No Slowing Down. [Online] Available at: https://www.mcafee.com/us/resources/reports/restricted/economic-impact-cybercrime.pdf [Accessed 16 February 2018].

McAfee, 2018b. McAfee Labs Threats Reports: Insights into malware, ransomware, and other cybersecurity threats from the McAfee threat research team. [Online] Available at: https://www.mcafee.com/enterprise/en-us/assets/infographics/infographic-threats-report-sep-2018.pdf [Accessed September 2018].

McClure, D. L., 2000. Electronic Government: Federal Initiatives are Evolving Rapidly but They Have Significant Challenges. [Online] Available at: https://www.gao.gov/new.items/a200179t.pdf [Accessed 24 January 2018].

Mengistu, D., Zo, H. & Rho, J. J., 2009. M-Government: Opportunities and Challenges to Deliver Mobile Government Services in Developing Countries. Seoul, Korea, 2009 Fourth International Conference on Computer Sciences and Convergence Information Technology.

Merkow, M. S. & Breithaupt, J., 2014. Information Security: Principles and Practices. 2nd Edition ed. s.l.: Pearson Education, Inc.

Metzler, M. G., 2018. Understand your company's risks with an enterprise risk assessment - Smart Business Magazine. [Online] Available at: http://www.sbnonline.com/article/understand-companys-risks-enterprise-risk-assessment/ [Accessed 27 January 2019].

Mims, N., 2017. The Botnet Problem. In: J. R. Vacca, ed. Computer and Information Security Handbook. Third Edition. s.l.: Morgan Kaufmann, pp. 265-274.

Mohapi, T., 2018. iAfrikan: South Africa's ViewFines suffered major data leak. [Online] Available at: https://www.iafrikan.com/2018/05/24/south-africas-viewfines-suffered-major-data-leak/ [Accessed 25 May 2018].

Moraetes, G., 2018. Security Intelligence: Choosing the Right Security Framework to Fit Your Business. [Online] Available at: https://securityintelligence.com/choosing-the-right-security-framework-to-fit-your-business/ [Accessed 23 October 2018].

Moyo, A., 2017. Data breach hits 30m South Africans. ITweb. [Online] Available at: https://www.itweb.co.za/content/DVgZeyvJGRJ7djX9 [Accessed 18 October 2017].

Mukherjee, I., 2013. Cloud Security through COBIT, ISO 27001 ISMS Controls, Assurance and Compliance. Marina Bay Sanda, Singapore, RSA Conference Asia Pacific 2013.

Müller, G., Koslowski, T. G. & Accorsi, R., 2013. Resilience - A New Research Field in Business Information Systems? Berlin, Heidelberg, In International Conference on Business Information Systems (pp. 3-14), Springer.

Musakwa, W. & Mokoena, T. B., 2017. Smart cities in South Africa! A case of misplaced priorities? Adelaide, Australia, Conference: Computers in Urban Planning and Urban Management. July 2017.

Mutemwa, M., Mtsweni, J. & Mkhonto, N., 2017. Developing a Cyber Threat Intelligence sharing platform for South African Organisations. Umhlanga, South Africa, 2017 Conference on Information Communication Technology and Society (ICTAS), pp. 1-6. IEEE.

Mutula, S. M., 2013. e-Government Divide: Implications for Sub-Saharan Africa. In: Information Ethics for Africa: Cross-cutting Themes. Pretoria: ACEIE, pp. 59-69.

Myers, M. D. & Avison, D. E., 2002. An Introduction to Qualitative Research in Information Systems. In: Qualitative Research in Information Systems: A Reader. London: SAGE Publications Ltd, pp. 4-12.

Myers, M. D., 2013. Qualitative Reseaarch in Business and Management. 2nd ed. London, UK: Sage Publications.

Mzekandaba, S., 2018. ITWeb: Home: IOT: More municipalities go digital to boost service delivery. [Online] Available at: https://www.itweb.co.za/content/G98YdMLxONXMX2PD [Accessed November 2018].

NCPF, 2015. South African Government National Cybersecurity Policy Framework. [Online] Available at: https://www.gov.za/documents/national-cybersecurity-policy-framework-4-dec-2015-0000 [Accessed 13 July 2016].

Netwrix, 2017. 2017 IT Risks Report. [Online] Available at: https://www.netwrix.com/2017itrisksreport.html [Accessed 23 February 2018].

Niselow, T., 2018. Mail & Guardian: Five massive data breaches affecting South Africa. [Online] Available at: https://mg.co.za/article/2018-06-19-five-massive-data-breaches-affecting-south-africans [Accessed 19 June 2018].

NIST, 2013. National Institute of Standards and Technology NIST Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, s.l.: NIST.

NIST, 2013. NIST Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations. [Online] Available at: http://dx.doi.org/10.6028/NIST.SP.800-53r4 [Accessed 19 October 2018].

NIST, 2017. Framework for Improving Critical Infrastructure Cybersecurity, s.l.: NIST.

NIST, 2018. Framework for Improving Critical Infrastructure Cybersecurity. [Online] Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [Accessed 21 October 2018].

Noaks, L. & Wincup, E., 2011. The development of qualitative approaches to criminology research. In: Introducing Qualitative Methods: Criminological research. London: SAGE Publications Ltd, pp. 2-18.

Norman, A. A. & Yasin, N. M., 2013. Information systems security management (ISSM) success factor: Retrospection from the scholars. African Journal of Business Management, 7(27), pp. 2646-2656.

North, J. & Pascoe, R., 2016. Cyber security and resilience — it's all about governance. Governance Directions, 68(3), pp. 146-151.

O'Neill, P. F., 2016. Building Resilience Through Risk Analysis. In: Resilience and Risk: Methods and Application in Environment, Cyber and Social Domains. Azores: Springer, pp. 451-468.

OECD/ITU, 2011. M-Government: Mobile Technologies for Responsive Governments and Connected Societies, Paris: OECD Publishing. http://dx.doi.org/10.1787/9789264118706-en.

Oest, A. et al., 2018. Inside a Phisher's Mind: Understanding the Anti-phishing Ecosystem Through Phishing Kit Analysis. In 2018 APWG Symposium on Electronic Crime Research (eCrime). San Diego, CA, USA, 2018 APWG Symposium on Electronic Crime Research (eCrime). IEEE, pp. 1-12.

Ogunleye, O. S. & Van Belle, J. P., 2014. Exploring the success, failure and factors influencing m-Government implementation in developing countries. Mauritius, 2014 IST-Africa Conference Proceedings, pp 1-10. IEEE Conferences.

Old Dominion University, 2013. Systems Assessment: Common Information Systems Risks. [Online] Available at:

https://www.odu.edu/about/policiesandprocedures/computing/standards/08/01 [Accessed 8 March 2018].

Olsen, T., 2013. Insurance Cyber Risk, s.l.: Willis.

Olsen, W., 2004. Triangulation in social research: qualitative and quantitative methods can really be mixed. Developments in sociology, Volume 20, pp. pp.103-118.

Orlikowski, W. & Baroudi, J., 1991. Studying Information Technology in Organisations: Research Approaches and Assumptions. Information Systems Research, pp. 1-29.

Otjacques, B., Hitzelberger, P. & Feltz, F., 2007. Interoperability of E-Government Information Systems: Issues of Identification and Data Sharing. Journal of Management Information Systems, 23(4), pp. 29-51.

Pandey, M. K., Kumar, S. & Karthikeyan, S., 2013. Information Security Management System (ISMS) Standards in Cloud Computing-A Critical Review. s.l., International Conference on Control Computing Communication & Materials (ICCCCM).

Passeri, P., 2018. 2017 Cyber Attacks Statistics. [Online] Available at: http://www.hackmageddon.com/2018/01/17/2017-cyber-attacks-statistics/ [Accessed January 2018].

Peter, A. S., 2017. Cyber resilience preparedness of Africa's top-12 emerging economies. International Journal of Critical Infrastructure Protection, Volume 17, pp. 49-59.

Phahlamohlaka, L. J., Jansen van Vuuren, J. C. & Coetzee, A., 2011. Cyber security awareness toolkit for national security: an approach to South Africa's cyber security policy implementation. Gaborone, Botswana, Proceedings of the first IFIP TC9/TC11 South African Cyber Security Awareness Workshop (SACSAW), 12 May 2011, pp1-14.

PhishLabs, 2018. 2018 Phishing Trends & Intelligence Report: Hacking the Human. [Online] Available at: https://info.phishlabs.com/hubfs/2018%20PTI%20Report/PhishLabs%20Trend%20Report_2018-digital.pdf [Accessed 28 August 2018].

PhishMe, 2018. South Africa Phishing Response Trends. [Online] Available at: http://www.nu.co.za/images/2018/Phishme/Phishing-Response-Trends_South-Africa_NU.pdf [Accessed 23 February 2018].

Pijoos, I. & Grobler, R., 2018. News24: EXCLUSIVE: Notorious hacker shuts down government website... again. [Online] Available at: https://www.news24.com/SouthAfrica/News/exclusive-notorious-hacker-shuts-down-government-website-again-20180828 [Accessed 29 August 2018].

Pompon, R., 2017. Doxing, DoS, and Defacement: Today's Mainstream Hacktivism Tools. [Online] Available at: https://f5.com/Portals/1/PDF/labs/ARTICLE-Doxing_DoS_Defacement_Mainstream_Hacktivism.pdf [Accessed 18 October 2017].

Ponemon Institute LLC, 2018. 2018 Cost of a Data Breach Study: Global Overview. [Online] Available at: https://public.dhe.ibm.com/common/ssi/ecm/55/en/55017055usen/2018-global-codb-report_06271811_55017055USEN.pdf [Accessed 12 September 2018].

PWC, 2010. Cyber Security Building confidence in your digital future., s.l.: PriceWaterCoopers.

Rance, S., 2014. Cyber resilience: bridging the business and technology divide. White paper. [Online] Available at: http://www.inxelerate.com/wp-content/uploads/2015/02/Cyber-Resilience.pdf [Accessed 5 March 2018].

Rapid7, 2016. National Exposure Index Inferring Internet Security Posture by Country through Port Scanning. [Online] Available at: www.rapid7.com [Accessed 16 October 2017].

Rapid7, 2018. National Exposure Index 2018 Inferring Internet Security Posture by Country Through Port Scanning. [Online] Available at: www.rapid7.com [Accessed 10 September 2018].

Ravitch, S. M. & Carl, N. M., 2015. Qualitative Research: Bridging the Conceptual, Theoretical, and Methodological, s.l.: SAGE Publications, Inc.

Refsdal, A., Solhaug, B. & StØlen, K., 2015. Cyber-Risk Management. Sheffield: Springer Briefs in Computer Science.

Resilens, 2016. Realising European ReSILiencE for Critical INfraStructure Deliverable D2.2: Qualitative, Semi-Quantitative and Quantitative Methods and Measures for Resilience Assessment and Enhancement. [Online] Available at: http://resilens.eu/wp-content/uploads/2016/08/D2.2-Methods-for-Resilience-Assessment-Final.pdf [Accessed 10 February 2019].

Rockart, J. F., 1979. Chief Executives Define Their Own Data Needs. Harvard business review, March, 57(2), pp. 81-93.

Roege, P. E. et al., 2016. Bridging the Gap from Cyber Security to Resilience. In: Resilience and Risk: Methods and Application in Environment, Cyber and Social Domains. Azores: Springer, pp. 383-414.

Roulston, K., 2014. Analysing interviews. [Online] Available at: in The sage handbook of qualitative data analysis [Accessed 01 November 2017].

RSA, 2016. Cyber Risk Appetite: Defining and Understanding Risk in the Modern Enterprise. [Online] Available at: https://www.rsa.com/content/dam/en/white-paper/cyber-risk-appetite.pdf [Accessed 10 September 2018].

Rubenstein, D., 2014. Nation State Cyber Espionage and its Impacts. [Online] Available at: http://www.cse.wustl.edu/~jain/cse571-14/ftp/cyber_espionage.pdf [Accessed 5 November 2017].

Rubin, R. B., Rubin, A. M. & Haridakis, P. M., 2010. Communication Research: Strategies and Sources. 7 ed. Boston: Wadsworth Cengage Learning.

Ruth, M. & Goessling-Reisemann, S., 2019. "Introduction to resilience of socio-technical systems" in: Handbook on Resilience of Socio-Technical Systems. [Online] Available at: https://www.elgaronline.com/view/edcoll/9781786439369/9781786439369.00006.xml [Accessed 23 February 2019].

Ryan, G. W. & Bernard, H. R., 2000. Data Management and Analysis Methods. In: In Handbook of Qualitative Research. s.l.: SAGE Publications, pp. 769-802.

Salkind, N. J., 2010. Encyclopaedia of Research Design, Thousand Oaks: SAGE Publications, Inc.

Sarkar, A., Wingreen, S. C. & Ascroft, J., 2016. Governing information systems resilience: a case study. Krakow, Poland, Conference: 13th European, Mediterranean & Middle Eastern Conference on Information Systems (EMCIS 2016).

Shakarian, P., Shakarian, J. & Ruef, A., 2013. Introduction to Cyber-Warfare: A Multidisciplinary Approach. Waltham: Syngress.

Shareef, S. M., 2016. Enhancing Security of Information in E-Government. Journal of Emerging Trends in Computing and Information Sciences, 7(3), pp. 139-146.

Siponen, M. & Willison, R., 2009. Information security management standards: Problems and solutions. Journal of Information and Management, Volume 46, pp. 267-270.

SMEX, 2018. Beirut-Based Global Cyber-Espionage Campaign a Threat to Local Freedoms. [Online] Available at: https://smex.org/beirut-based-global-cyber-espionage-campaign-a-threat-to-local-freedoms/ [Accessed 18 January 2018].

Smith, S. & Jamieson, R., 2005. Key Factors in E-Government Information System Security. Bled, Slovenia, 18th Bled eConference eIntegration in Action.

Software AG, 2014. Press Release: Software AG. [Online] Available at: http://www.softwareag.com/corporate/Press/pressreleases/20141111_Ekurhuleni_Smart_City_on_ZAs_Gold_Reef_page.asp [Accessed November 2018].

SonicWall, 2018. 2018 SonicWall CyberThreat Report Threat Intelligence, Industry Analysis and Cybersecurity Guidance for the Global Cyber Arms Race. [Online] Available at: https://cdn.sonicwall.com/sonicwall.com/media/pdfs/resources/2018-snwl-cyber-threat-report.pdf [Accessed 20 September 2018].

SOPHOS, 2018. The State of Endpoint Security Today. [Online] Available at: https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/endpoint-survey-report.pdf [Accessed 22 February 2018].

South African Parliament, 2017. Information Memorandum: Department of Public Enterprises Republic of South Africa to Parliamentary Question No. 92. [Online] Available at: https://www.parliament.gov.za/storage/app/media/Docs/exe_r_ncop/0dd2ee03-045b-488c-af56-1ec2a2029f37.pdf [Accessed 12 September 2018].

SSA, 1998. Minimum Information Security Standards, s.l.: SSA.

Susanto, H. & Almunawar, M. N., 2018. INFORMATION SECURITY MANAGEMENT SYSTEMS A Novel Framework and Software as a Tool for Compliance with Information Security Standards. s.l., Apple Academic Press.

Sutherland, E., 2017. Governance of Cybersecurity – The Case of South Africa. African Journal of Information and Communication (AJIC), Volume 20, pp. 83-112.

Symantec, 2014. White Paper - The Cyber Resilience Blueprint: A New Perspective on Security. [Online] Available at: https://www.symantec.com/content/en/us/enterprise/white_papers/b-cyber-resilience-blueprint-wp-0814.pdf [Accessed October 2017].

Symantec, 2018. Executive Summary 2018 Internet Security Threat Report. [Online] Available at: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en.pdf [Accessed 20 September 2018].

Tahboub, R. & Saleh, Y., 2014. Data Leakage/Loss Prevention Systems (DLP). s.l., IEEE.

Talabis, M. & Martin, J., 2012. Information Security Risk Assessment Toolkit. 1st Edition ed. Waltham, MA 02451, USA: Syngress.

Telos, 2017. 2017 Public Sector Risk Management Report. [Online] Available at: https://www.telos.com/new-public-sector-report-reveals-83-percent-favor-mandate-nist-cybersecurity-framework-across-federal-agencies/ [Accessed 20 March 2018].

Tenable Network Security, 2013. Continuous Network Monitoring Eliminate periodic assessment processes that expose security and compliance programs to failure, s.l.: Tenable Network Security.

The European Cybersecurity Hub, 2018. Cyber-resilience: The Key to Business Security. Panda Security Summit, s.l.: The European Cybersecurity Hub.

Torres, J. M., M, S. J., Javier, S. & Serrano, N., 2006. Managing Information Systems Security: Critical Success Factors and Indications to Measure Effectiveness. Springer, Berlin, Heidelberg., International Conference on Information Security (pp. 530-545).

Trauth, E. M., 2001. Choosing Qualitative Methods in IS Research: Lessons Learned. In: Qualitative Research in IS: Issues and Trends. s.l.: Idea Group Publishing, pp. 271-287.

Trimi, S. & Sheng, H., 2008. Emerging trends in M-government. Communications of the ACM, 51(5), pp. 53-58.

Tu, Z. & Yuan, Y., 2014. Critical Success Factors Analysis on Effective Information Security Management: A Literature Review. Savannah, Twentieth Americas Conference on Information Systems.

Twum-Darko, M., 2007. The role of information System in legislation led reform: A case study in the context of the new municipal property rates Act of South Africa. [Online] Available at: https://www.researchgate.net/publication/264048794_The_role_of_information_System_in_legislation_led_reform_A_case_study_in_the_context_of_the_new_municipal_property_rates_Act_of_South_Africa [Accessed 24 January 2019].

UKAIS, 1997. Newsletter for the United Kingdom Academy for Information Systems. [Online] Available at: http://www.scs.leeds.ac.uk/ukais/Newsletters/vol3no4.html [Accessed 5 June 2015].

UN, 2018. United Nations E-Government Survey 2018: Gearing E-Government to Support Transformation Towards Sustainable and Resilient Societies. [Online] Available at: https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2018-Survey/E-

Government%20Survey%202018_FINAL%20for%20web.pdf [Accessed 9 September 2018].

UNDESA, 2014. United Nations E-Government Survey 2014: E-Government for the Future We Want, New York: United Nations Department of Economic and Social Affairs.

UNDESA, 2016. United Nations E-Government Survey 2016: E-Governement in Support of Sustainable Development. [Online] Available at: http://workspace.unpan.org/sites/Internet/Documents/UNPAN97453.pdf [Accessed 20 February 2018].

University of Adelaide, 2014. Risk management Handbook. [Online] Available at: https://www.adelaide.edu.au/legalandrisk/docs/resources/Risk_Management_Handbook.pdf

US Department of Homeland Security, 2018. Cyber Resilience and Response 2018 Public-Private Analytic Exchange Program. [Online] Available at: https://www.dhs.gov/sites/default/files/publications/2018_AEP_Cyber_Resilience_and_Response.pdf [Accessed 18 September 2018].

US_CERT, 2017. Assessments: Cyber Resilience Review (CRR). [Online] Available at: https://www.us-cert.gov/ccubedvp/assessments [Accessed January 2017].

van Niekerk, B., 2017. An Analysis of Cyber-Incidents in South Africa. African Journal of Information and Communication (AJIC), Issue 20, pp. 113-131.

van Zyl, G., 2016. Anonymous 'hacks' Armscor website. Fin24tech. [Online] Available at: https://www.fin24.com/Tech/News/anonymous-hacks-armscor-website-20160712 [Accessed 17 June 2018].

Vergelis, M., Demidova, N. & Shcherbakova, T., 2018. Spam and phishing in Q2 2018. [Online] Available at: https://securelist.com/spam-and-phishing-in-q2-2018/87368/ [Accessed August 2018].

Verizon, 2017. 2017 Data Breach Investigations Report 10th Edition. [Online] Available at: www.verizon.com [Accessed 24 November 2017].

Vermeulen, J., 2016. Anonymous hacks SA government database. mybroadband. [Online] Available at: https://mybroadband.co.za/news/security/155030-anonymous-hacks-sa-government-database.html [Accessed 18 June 2018].

von Solms, B. & von Solms, R., 2017. Cyber security and information security – what goes where? Information & Computer Security, 26(1), pp. 2-9.

von Solms, B., 2015. Improving South Africa's Cyber Security by cyber securing its small companies. Malawi, 2015 IST-Africa Conference.

von Solms, B., 2016. Towards a cyber governance maturity model for boards of directors. International Journal of Business & Cyber Security (IJBCS), 1(1), pp. 1-9.

Walsham, G., 2006. Doing Interpretive Research. European Journal of Information Systems, Volume 15, p. 320–330.

Walsham, G., 2009. Interpreting Information Systems in Organizations. s.l.: A Gobla Text.

Ward, J. & Peppard, J., 2002. The Evolving Role of Information Systems and Technology in Organizations: A Strategic Perspective. In: Strategic Planning for Information Systems, 3rd Edition. Bedfordshire: John Wiley & Sons, Ltd, pp. 1-63.

Watson, A., 2017. We track down the hackers who shut down presidency website. [Online] Available at: https://citizen.co.za/news/south-africa/1610234/hackers-shut-down-the-presidency-website/ [Accessed August 2017].

WEF, 2012. World Economic Forum: Partnering for Cyber Resilience. [Online] Available at: www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf [Accessed 11 October 2015].

WEF, 2015. Partnering for Cyber Resilience Towards the Quantification of Cyber Threats, In collaboration with Deloitte, s.l.: World Economic Forum.

WEF, 2017. Advancing Cyber Resilience Principles and Tools for Boards. [Online] Available at: http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf [Accessed 16 October 2017].

WEF, 2018. The Global Risks Report 2018 13th Edition. [Online] Available at: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf [Accessed 10 September 2018].

West, D. M., 2004. Global Perspective on E-Govenment. Chicago, Illinois, American Political Science Association.

Whitman, M. E. & Mattord, H. J., 2014. Introduction to Information Security. Fifth Edition. In: Principles of Information Security. Boston: Cengage Learning.

Zefferer, T., 2011. E-government for Mobile Societies Stocktaking of Current Trends and Initiatives Contents. [Online] Available at: https://www.semanticscholar.org/paper/E-government-for-Mobile-Societies-Stocktaking-of/4bc01bcdaf4d97d5b898b122a2f87dd98c72b359?navId=citing-papers [Accessed 25 July 2018].

Zhu, Q., Wei, D. & Ji, K., 2016. Hierarchical Architectures of Resilient Control Systems: Concepts, Metrics, and Design Principles. In: Cyber Security for Industrial Control Systems from the Viewpoint of Close-Loop. s.l.: CRC, pp. 151-182.