

ACHIEVING OPERATIONAL RESILIENCE BY ALIGNING CYBERSECURITY VULNERABILITIES, NEEDS AND RESPONSES IN PROVINCIAL GOVERNMENT

Donovan Quinton Harris

Student No. 2277645

Supervisor: Dr Lucienne Abrahams

**A research report submitted to the Faculty of Humanities,
University of the Witwatersrand, in partial fulfilment of the
requirements for the degree of Master of Arts (in the field
of ICT Policy and Regulation)**

April, 2021

ABSTRACT

It is unclear how government departments have incorporated cybersecurity in their strategic planning processes, policies and operations to promote organisational and operational resilience. The government stores a significant amount of data and often uses legacy systems vulnerable to complex cyber threats and attacks. Vulnerabilities mitigated through cybersecurity frameworks, standards, people management and backed up by good vulnerability intelligence can provide an understanding of how and why threat actors are targeting particular vulnerabilities.

The case study method was chosen as it was considered highly suitable for the research setting because this method provided a provincial government department view by focusing the study on cybersecurity practice in government departments in an unidentified province. This data enabled the researcher to understand the current vulnerabilities, needs and historical responses as the basis for designing future cybersecurity responses to ensure operational resilience.

The research methodology identified the appropriate methods which the researcher exploited to address the research purpose and research questions. Methods of research design were examined in relation to the research diagram. Qualitative constructivism method research approach allowed the researcher to comprehend the provincial government's cybersecurity challenges. Constructivism was selected as new knowledge that needed to be collected rather than merely acquiring it via memory or solely communication from those who know to those who do not know about cybersecurity in the provincial government. A systematic mapping study provided an unbiased and systematic mechanism to answer research questions by finding the research outcomes. The lighter systematic mapping method was chosen as a more comprehensive systematic literature review was not required at this research level. Using systematic mapping, existing research on cybersecurity was better understood by identifying the limitations and gaps of current research.

One of the main findings is that provincial government departments are exposed to cybersecurity vulnerabilities and threats because they do not have adequate controls in place. The provincial government visibility of cybersecurity vulnerabilities and threats has been identified as lacking. A critical implication is that there is no alignment between provincial departments regarding cybersecurity. The outcome of the research is that the provincial government is not in line with the national cybersecurity policy framework because the identification of cybersecurity risk is low. These factors can potentially influence the availability of government information systems and affect the department's operational resilience. The Government Information Technology Council, which is involved in the investigation, formulation and development of ICT security policies, e-government and strategy, and ICT procurement, has key objectives which focus on the alignment of ICT and ICT Security (Cybersecurity) in the province with government business objectives.

The identification of cybersecurity vulnerabilities and threats is critical for the provincial government to respond to cyberattacks, this cybersecurity risks can be mitigated by incorporating people management with programs such as cybersecurity awareness. Cybersecurity vulnerabilities, responses and people management are interlinked and need to be aligned to improve the provincial government's operational resilience.

The GITO council should be making departments HOD's and the premier aware of non-compliance in departments and implement measures to ensure that cybersecurity incidents in the departments are reported to the provincial GITO council to ensure that the cybersecurity incidents get a response and cybersecurity controls amended to mitigate future incidents.

DEDICATION

To my wife and daughter, I dedicate this achievement to you. I hope I will be an inspiration to my daughter. Thank you for being loving, caring and supportive and having patience and belief in my abilities.

ACKNOWLEDGEMENT

I want to thank all those who contributed to this study. I would not have managed to complete this study without the support, help, and guidance provided. Dr Lucienne Abrahams, my supervisor, I would like to acknowledge that I would not have managed to complete this research study without your help, encouragement, constant support, and professional guidance.

DECLARATION

I declare that this report is my own, unaided work. It is submitted in partial fulfilment of the requirements of the degree of Master of Arts (in the field of ICT Policy and Regulation) at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination to any other University.

**DQ Harris
25 April 2021**

TABLE OF CONTENTS

ABSTRACT.....	ii
DEDICATION	iv
ACKNOWLEDGEMENT	v
DECLARATION.....	vi
List of Acronyms	x
Chapter 1: Closing the gap in cybersecurity to achieve operational resilience	1
1.1 Introduction.....	1
1.2 Research problem statement.....	1
1.3 Research purpose statement	2
1.4 Research questions.....	2
1.5 Background discussion: Facts and figures about the state of cybersecurity in government in South Africa.....	2
1.5.1 Cybersecurity Globally.....	2
1.5.2 Cybersecurity incidents in the South African Government.....	4
1.5.3 Case study of the Provincial Government.....	6
1.6 Research benefits and limitations	7
1.7 Research chapter outline	7
Chapter 2: Promoting cybersecurity through better understanding vulnerabilities, needs and responses	11
2.1 Nature of vulnerabilities in public sector information systems.....	11
2.1.1 Cyber threats and vulnerabilities in government.....	11
COVID-19 pandemic and cybersecurity	13
2.2 Approach to the alignment of cybersecurity responses with vulnerabilities and needs in government departments	15
2.2.1 Cybersecurity frameworks	15
2.2.2 Cybersecurity standards.....	16
2.3 Responding to improve cyber resilience	18
2.3.1 Cybersecurity alignment	19
2.4 Analytical framework	19

Chapter 3: RESEARCH Methodology: QUALITATIVE CONSTRUCTIVIST AND SYSTEMATIC MAPPING METHODOLOGY	21
3.1 Introduction	21
3.2. Research design: Steps to collect and analyse data towards the research goal	21
3.3. Research methodology: Qualitative constructivism and systematic mapping.....	21
3.3.1 Qualitative constructivism	22
3.4 Research approach: Data collection and data analysis	23
3.4.1 Primary Data.....	24
3.4.1.1 Interviews.....	24
3.4.1.2 Participant observation: MS Teams Virtual Meetings	25
3.4.2 Secondary Data	25
3.4.2.1 Document review	25
3.4.2.2 Systematic Mapping.....	25
3.4.4 Data analysis.....	27
3.4.4.1 Data coding	28
3.4.4.2 Pattern matching.....	29
3.4.4.3 Atlas.ti for qualitative data analysis	29
3.4.4.4 Inductive and deductive reasoning	32
3.4.4.5 Synthesis.....	32
Chapter 4: Inside the Government Cybersecurity Landscape	34
4.1 Introduction	34
4.2 Primary data collection and analysis	34
4.2 Digital and cybersecurity skills of the provincial government	37
4.3 Government perception of cybersecurity vulnerabilities.....	39
4.4 Improving operational resilience through effective cybersecurity	43
4.5 Mitigating cybersecurity vulnerabilities.....	48
4.6 Government responding to Cybersecurity	52
4.7 Emerging Theme - ICT Security trends and threats during Covid 19	58
4.8 Conclusion	60

Chapter 5: ANALYSIS OF the GOVERNMENT CYBERSECURITY LANDSCAPE.....	61
5.1 Introduction	61
5.2 Current cyber vulnerabilities of government information systems to external threats	61
5.3 Identification of cybersecurity vulnerabilities in government departments	62
5.4 Needs with respect to improving operational resilience through effective cybersecurity	63
5.5 Government departments’ responses to cybersecurity incidents	65
5.5 Conclusion: Integrated view of vulnerabilities, responses and people management	67
Chapter 6: Cybersecurity in provincial government: Research Summary, recommendations and conclusion	69
6.1 Introduction	69
6.2 Research justification	69
6.3 Results determined by research questions	69
6.3.1 Question 1 - What are the current cyber vulnerabilities of government information systems to external threats?.....	69
6.3.2 Question 2 - How do government departments currently respond to cybersecurity incidents?	70
6.3.3 Question 3 - How should provincial government departments mitigate cybersecurity vulnerabilities?	71
6.3.4 Main Question - How can provincial government departments improve operational resilience through effective cybersecurity?	73
6.4 Research limitations	75
6.5 Recommendations for future research	76
6.6 Conclusion: Contribution to knowledge.....	76
LIST OF References.....	78
APPENDIX A:.....	86
INTERVIEWS QUESTIONS GUIDE	86
APPENDIX B:	90
Document Review Guide	90
APPENDIX C:	94
Ethics clearance certificate	94

List of Acronyms

CGICTP	Corporate Governance Information Communication Technology Policy
COBIT	Control Objectives for Information and Related Technologies
CSF	NIST Cybersecurity framework
DDoS	Distributed Denial of Service
DoS	Denial of Service
GCI	Global Cybersecurity Index
GITO	Government Information Technology Officer
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IoT	Internet of Things
ISO	International Organisation for Standardisation
NCPF	National Cybersecurity Framework
NIST	National Institute of Standards and Technology
PGITOC	Provincial Government Information Technology Officer Council
SITA	State Information Technology Agency
SQLi	Structured Query Language Injection

CHAPTER 1: CLOSING THE GAP IN CYBERSECURITY TO ACHIEVE OPERATIONAL RESILIENCE

1.1 Introduction

This introductory section defines the research rationale by defining the problem, scope, limitations, objectives, and questions intended to fill the research gap by covering the need for alignment between cybersecurity and strategies, frameworks, and policies. Global technological advancement has influenced the public sector in South Africa, and this technological advancement has brought about an environment whereby cybersecurity has become a necessity. South Africa, like other developing countries is perceived as having inadequate capacity and capabilities to effectively withstand cybersecurity threats and cyber-attacks.

The evolution of the Internet has led to a significant growth of cyber-attacks and cyber-incidents, often with consequences that were disastrous. Despite the improvement in cybersecurity, precautions and cybersecurity threat mitigation techniques such as web browsing content intelligence, cybersecurity analytics, behavioural threat intelligence and network policy control, cybercriminals have developed sophisticated ways to disrupt business and steal information in organisations.

1.2 Research problem statement

There is a gap in knowledge concerning promoting cybersecurity in sub-national governments (provincial government and local government) through a better understanding of vulnerabilities, needs and historical responses in order to offer relevant future responses in government. The provincial government needs to prepare for the inevitable cyber threats by understanding and considering what cyber threats apply to government departments. Alignment and coordination across government are needed to implement the National Cybersecurity Policy Framework. It is uncertain how government departments have incorporated cybersecurity in their strategic planning processes, policies and operations to promote organisational and operational resilience. The government stores a significant amount of data and often uses legacy systems vulnerable to complex cyber threats and attacks. Vulnerabilities mitigated through cybersecurity frameworks, standards, people management and backed up by good vulnerability intelligence can provide an understanding of how and why threat actors are targeting particular vulnerabilities (Pretorius & Ngejane, 2019). Through cybersecurity frameworks, organisations have the ability to facilitate the identification of critical systems and protect the critical systems from evolving cyber threats that can disrupt business operations (Krumay, Bernroider & Walser, 2018). People are the greatest vulnerability in any organisation, and people management is therefore, critical to ensure a cyber-secure culture that can mitigate overall cyber-related business risks. In cybersecurity, people are seen as victims, the weakest link in the system, a direct threat to the business's security and operation (Dalal, et al., 2021). Responding to cyber incidents through the implementation of frameworks, standards and people management can ensure operational resilience in the organisation.

1.3 Research purpose statement

The purpose of this research is to investigate threats and vulnerabilities in cybersecurity and determine if there is a need to mitigate cybersecurity using frameworks and standards. Through investigating the alignment of cybersecurity with frameworks and standards, the current threats and vulnerabilities can be identified and addressed that impact government information systems. The research will then look at what is needed for the government to respond to a cyber incident and what government needs to do to become cyber resilient. The research will take the form of a case study investigation of vulnerabilities, needs and current responses in fourteen departments and entities in the Provincial Government. The investigation will focus narrowly on frameworks, related standards and people management because, in order to offer relevant future cybersecurity responses to ensure operational resilience in government, a better understanding of current vulnerabilities, needs and historical responses are required (technical vulnerabilities excluded).

1.4 Research questions

Main research question for this review is:

How can provincial government departments improve operational resilience through effective cybersecurity?

The research sub-questions are:

1. What are the current cyber vulnerabilities (technical vulnerabilities excluded) of government information systems to external threats?
2. How do government departments currently respond to cybersecurity incidents?
3. How should provincial government departments mitigate cybersecurity vulnerabilities (technical vulnerabilities are excluded)?

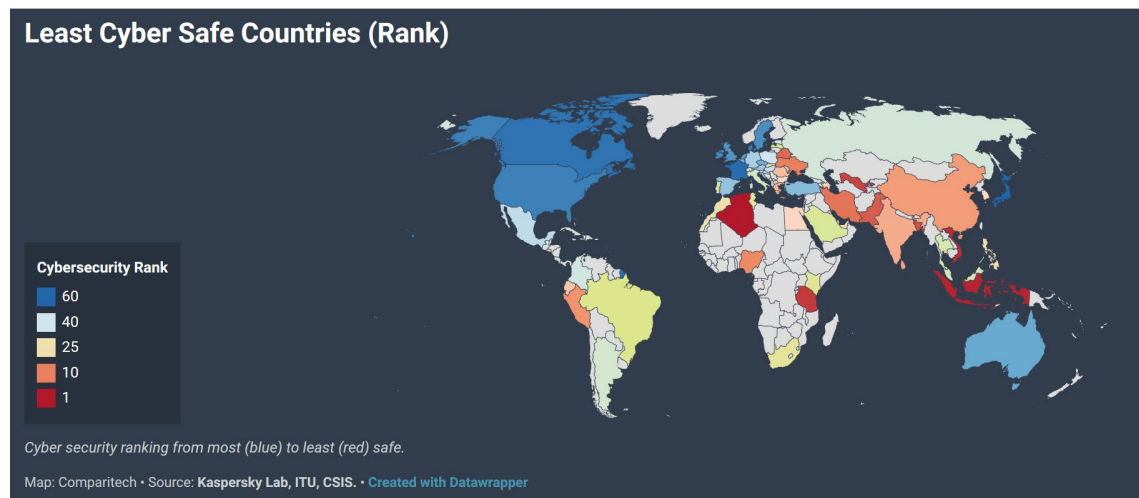
1.5 Background discussion: Facts and figures about the state of cybersecurity in government in South Africa

1.5.1 Cybersecurity Globally

The digital transformation of the world has increased due to the increase in smart devices, networked systems, and the Internet of Things (IoT). The rise in the use of network smart devices is leading to a growing cybersecurity threat environment. The exact effect and costs of cyber incidents is a debated topic, but year by year, the cost increases considerably (McAfee, 2018; Verizon, 2019).

Cybersecurity is a concern for all countries, threats and impacts in their nature differ from country to country. Therefore, there is a need to assess the impacts and threats specific to a country. The global concern fuelled by data breaches and lack of skilled cybersecurity professionals has required research institutes to survey and report on cybersecurity to promote cybersecurity initiatives through comparison (ITU, 2018a). The Global Cybersecurity Index (GCI) ranks countries from least safe to most safe. For the year 2018, 60 countries were surveyed and split into three main categories, whereby the top 6 countries under each category are listed in the table below.

Figure 1: Global Cybersecurity ranking



Source: ITU (2018a)

Table 1: Comparison of GCI rankings 2018

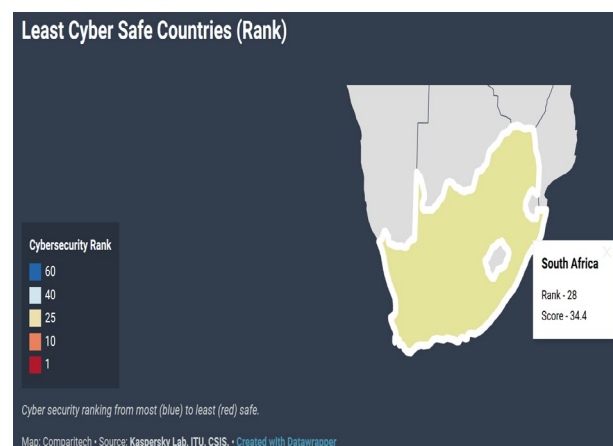
Global Cybersecurity Index rankings 2018

Top 6 Countries with worst cybersecurity	Top 6 Countries with cybersecurity commitment	Top 6 Countries with the best cybersecurity
Gabon	Uzbekistan	United Kingdom
State of Palestine	Moldova	United States of America
Senegal	Ukraine	France
Sudan	Azerbaijan	Lithuania
Gambia	Cyprus	Estonia
Ethiopia	South Africa	Singapore

Source: ITU (2018a)

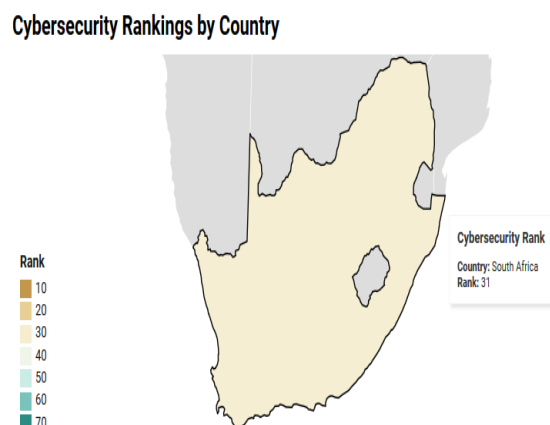
The Global Cybersecurity Index (GCI) reports on the commitment of countries to cybersecurity at a global level, the GCI looked at 60 countries in 2018 and found considerable differences in a number of categories, from malware rates to cybersecurity-related legislation. South Africa ranked 28 out of 60 countries as least cyber safe. In 2019, looking at the GCI 2018 report and Kaspersky 2019 report on security statistics South Africa, improved and was ranked 31 out of 76 countries, 16 new countries added to 2019. The Global Cybersecurity Index (GCI) is busy compiling the 2019/2020 report and has been delayed by the COVID-19 Pandemic.

Figure 2: Cybersecurity Ranking 2018



Source: ITU (2018a)

Figure 3: Cybersecurity Ranking 2019



Source: Kaspersky (2019)

1.5.2 Cybersecurity incidents in the South African Government

Government departments are dependent on evolving information systems. Information systems are critical for e-government and play an important role in the government department's business process's success and ability to deliver the departments mandate. To achieve the department's strategic objectives effectively, these information systems need to stay relevant and technologically driven, in other words, digitally-enabled operations need to be efficient, increase performance, improve service delivery speed and reduce cost. Cyber risks have a capacity to disrupt information systems and are increasing continuously. Cybersecurity survey reports (ITU, 2018a; Kaspersky, 2019; Verizon, 2019) rank South Africa in the top 20 for most vulnerable to cyber-attacks. An examples of recent cyber incidents that impacted the South African government negatively are listed in Table 2 below:

Table 2: Cyber incidents in South Africa

Year	Information about the incident	Type of cyber incident
2018	Department of Labour experienced an unsuccessful attack on one of its external-facing servers. A DDOS attack is when multiple systems flood the bandwidth or resources of a website, making it unavailable. Level of Incident: Low (No servers, systems or client's information was compromised)	Distributed Denial of Service (DDoS)
2018	Websites of the Presidency, Department of Environmental Affairs and Department of Home Affairs, were disabled by the hacking group "Black Team". A website defaced and replaced with the hacker group emblem and message. The website is then disabled for repair.	Hack

	Level of Incident: Medium (Servers, systems or client's information was compromised)	
2018	A contractor of municipalities discovered a data breach of personal records. Over 900k records of South African's stolen in data breach. Level of Incident: Medium (Servers, systems or client's information was compromised)	Data Theft
2019	Lazarus group targeting banks and other financial companies around the globe Cybercrimes across digital banking platforms increase yearly - resulting in losses of over R262m, no loss reported in this incident. Level of Incident: Medium (Servers, systems or client's information was compromised)	cyber-espionage and cyber-sabotage
2019	City of Johannesburg had a breach on its network, bitcoin ransom notes from a group called the Shadow Kill Hackers Bitcoins of the value of \$30k demanded by hackers. The Call Centre and digital platforms were taken offline for recovery. Level of Incident: High (Servers, systems or client's information was compromised)	Ransomware
2019	Provincial Treasury Northern Cape departmental website defaced. External facing digital platforms were taken offline for recovery. Level of Incident: Medium (Servers, systems or client's information was compromised)	Hack
2019	Organisations are facing malware attacks caused by employees making inappropriate use of company property. Malware attacks in South Africa increased by 22% in the first quarter of 2019. Level of Incident: Medium (Servers, systems or client's information was compromised)	Malware
2020	A perpetrator hacked one of the servers of the Department of Employment & Labour Hacker hacked over 300 staff credentials for the purpose of fraud and corruption. Level of Incident: High (Servers, systems or client's information was compromised)	Hack

Sources: Breakfast, 2018; Department of Labour, 2018; Etheridge, 2018; Paton, 2019; Smith, 2019a; Smith, 2019b; Department of Employment & Labour, 2020

Cybersecurity has been severely compromised in the area of digital banking, with South Africa listed as having the third-highest number of cybercrimes in this area and yet lacking a comprehensive cybercrime legal framework (Didenko, 2018).

South African government departments need to move from the commitment to actual cybersecurity practice. By understanding the current threats and challenges that government departments face will enable them to manage cybersecurity risk more effectively and provide a view of the current cybersecurity risks and gaps (Kaspersky, 2019).

The NIST cybersecurity framework ensures that the cybersecurity vulnerabilities, needs and responses are identified under categories (Access Control, etc.), and subcategories function referenced to existing standards such as the International Organisation for Standardisation (ISO) and International Electrotechnical Commission (IEC) 27001 and Control Objectives for Information and Related Technologies (COBIT) and etc (National Institute of Standards and Technology, 2018) to ensure operational resilience in government. The South African government's response to the issue of cybersecurity has been the implementation of the National Cybersecurity Policy Framework (NCPF). This policy framework is aimed at a coherent and integrated cybersecurity approach to address cybersecurity threats. Given the cyber-crime occurrence globally, the public and private sectors have taken cybersecurity precautions to strengthen and mitigate these risks (SSA, 2015). The NCPF for South Africa defines cyber-espionage as an act or practice to obtain secrets without the permission of the owner of the information (personal, sensitive, proprietary or of classified nature) from individuals, competitors, governments and enemies for personal, economic, political advantage. The NIST CSF can complement the National Cybersecurity Policy Framework (NCPF) as a scorecard through core functions that deliver a high-level strategic view of an organisations management of cybersecurity risks (Identify, Protect, Detect, Respond, and Recover).

One of the well-known cybersecurity frameworks is the NIST Cybersecurity framework (CSF), the NIST CSF developed by the National Institute of Standards and Technology in 2013 (NIST, 2018). Although mainly used to assess critical infrastructure, the CSF has a list of security controls from several sources that have been combined. The CSF divided into several core functions that provide a high-level strategic view of organisations management of cybersecurity risks (Identify, Protect, Detect, Respond, and Recover) through the lifecycle approach. The NIST CSF has categories (Access Control, etc.) and subcategories for each function referenced to existing standards utilised in the NCPF (ISO/IEC 27001, COBIT, etc.) (National Institute of Standards and Technology, 2018).

The National Cybersecurity Policy Framework utilising existing standards and measured using the NIST Cybersecurity framework ensures that the cybersecurity vulnerabilities in government get identified. Needs to mitigate cybersecurity risks are categorised, and weakness in cybersecurity controls responded accordingly to ensure operational resilience in government. Implementing a policy approach, frameworks can be reinforced as policies are expected to facilitate rather than regulate.

1.5.3 Case study of the Provincial Government

The Provincial Government Information Technology Officer Council (PGITOC), which was created to serve as an ICT coordination and consolidation vehicle in government, looks at strategic partnerships with government agencies, the business sector and any other bodies related to the ICT sector in order to help it meet its objectives. The Council, which is involved in the investigation, formulation and development of ICT security policies, e-government and strategy, and ICT procurement, has key objectives which focus on the alignment of ICT and ICT Security (Cybersecurity) in the province with government business objectives. The PGITOC resolutions filters to departments via departmental

Government Information Technology Officer's (GITO's) and their respective department ICT Strategic committees, ICT Steering committees and ICT operational committees.

The case study was chosen as it was considered highly suitable for the research setting and will provide a government department view. Focusing narrowly on frameworks, related standards and people management in order to offer relevant future cybersecurity responses by understanding current vulnerabilities, needs and historical responses to ensure operational resilience.

The research is conducted from the assumption that government departments promote cybersecurity and foresee the importance of cybersecurity. Therefore, the research design aims to ensure that:

- All provincial government departments will be requested to participate in the research study.
- All targeted participants will be willing to participate.
- The research should provide sufficient data for analysis.

1.6 Research benefits and limitations

To my knowledge, there is inadequate data available on the state of cybersecurity readiness in provincial government departments. The research will benefit the provincial government by identifying cybersecurity risks and establishing a cybersecurity risk management approach through strategies, policies, and good cybersecurity practices.

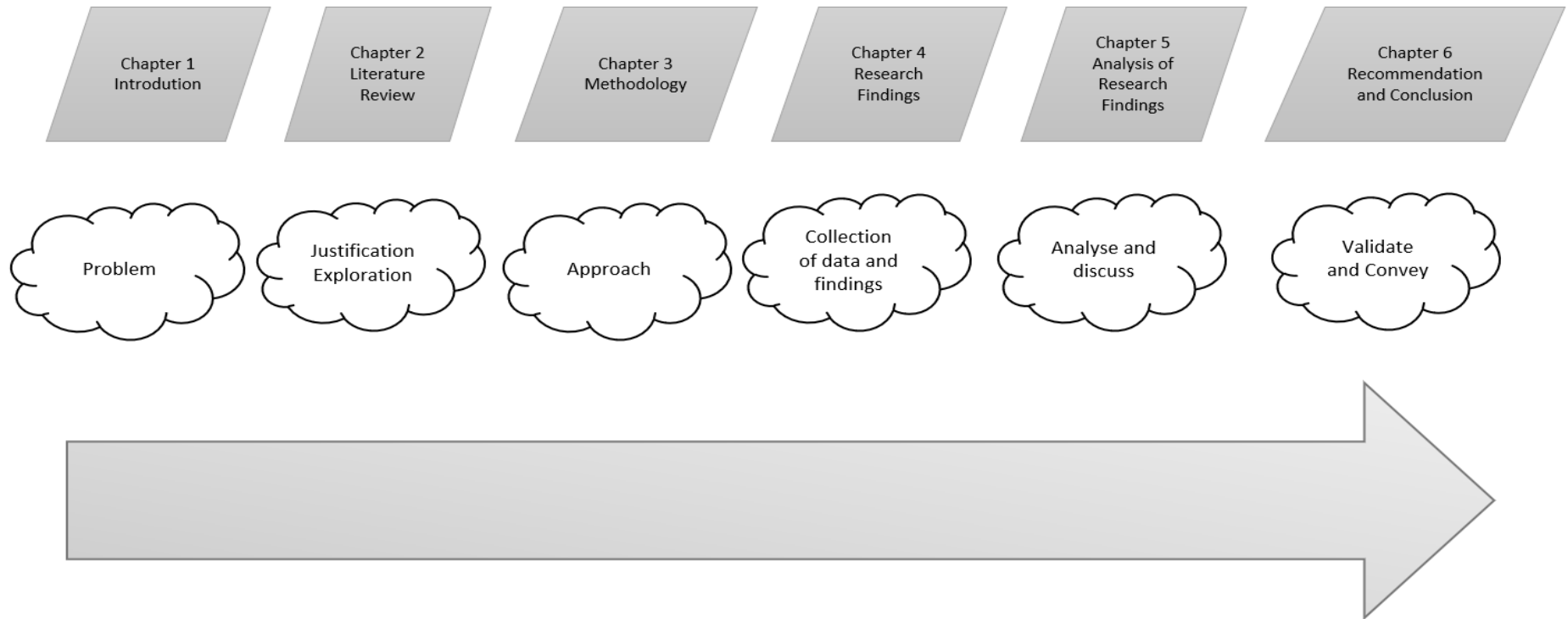
The research will give insight into the identification of factors that influence or affect cybersecurity effectiveness in government departments. While this study is limited in scope to government departments, the results may easily be applied to government entities, and private sector organisations as the cybersecurity effectiveness of government departments are critical to the maintenance of services to the public.

The research is limited to the target organisation and describes factors in this narrowed scope. Therefore, the scope is narrowed to provincial government departments and their service provider SITA. The targeted participants are at least two participants per department that are involved in the following fields: Information Technology, Information Security, Cybersecurity, Information Technology Security and Risk.

1.7 Research chapter outline

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

Figure 4: Research Chapters outline



Chapter one: Closing the gap in cybersecurity to achieve operational resilience

Chapter one sets out the research focus and research problem and specifies the study's significance giving the research context. The chapter explains the need for cybersecurity research in South Africa by identifying cybersecurity risks and establishing a cybersecurity risk management approach through strategies, policies, and acceptable cybersecurity practices. This chapter also explains the context for understanding cybersecurity in the provincial government in South Africa.

Chapter two: Promoting cybersecurity through better understanding vulnerabilities, needs and responses

The chapter explores the nature of cybersecurity vulnerabilities in provincial government and what is needed to respond to cybersecurity through frameworks, standards, and people management. The chapter explores the different types of vulnerabilities affecting the provincial government and the different cyber threats categories. The chapter further explores operational and cybersecurity resilience in the provincial government and the alignment between these cybersecurity, frameworks, and government standards.

Chapter three: Research methodology: Qualitative constructivist and systematic mapping methodology

Chapter three outlines the research methodology and appropriate methods which the researcher applied to address the research purpose and research questions. Methods of research design are examined in relation to the research diagram. The previous chapters considered the literature as a baseline to address the research questions, and this chapter explains why specific research methods were chosen.

Chapter four: Inside the government cybersecurity landscape

Chapter four presents in detail the findings of the research data collected in provincial government departments. The chapter introduces the research findings from the interviews and aims to contextualise cybersecurity in the provincial government. The research questions and objectives directed qualitative content analysis of research findings.

Main research objective: To identify why and how provincial government departments can improve operational resilience through effective cybersecurity.

- Research objective (i): To identify the current cyber vulnerabilities of government information systems to external threats.
- Research objective (ii): To identify how provincial government departments currently respond to cybersecurity incidents.
- Research objective (iii): To identify the need for provincial government departments to mitigate cybersecurity vulnerabilities.

Chapter five: Discussion on findings

The Chapter discusses the research findings that were conducted in the provincial government. The purpose of the research study was to investigate threats and vulnerabilities in cybersecurity and determine if there is a need to mitigate cybersecurity using frameworks and standards. By investigating cybersecurity alignment with frameworks and standards, the current threats and vulnerabilities can be identified and addressed that impact government information systems. Further, this chapter discusses what is needed for the provincial government to respond to a cyber incident and what government needs to do to become cyber resilient.

Chapter six: Research Summary, recommendations and conclusion

Chapter six concludes the research by summarising the research emphasising a combination of the research findings interpreted and discussed from the analysis of data collected from the interviews and document review and provides evidence of how the research aims have been fulfilled. This chapter further identifies the research limitations and recommendations for future research. The chapter concludes with an explanation of how provincial departments in the South African government can improve cybersecurity.

CHAPTER 2: PROMOTING CYBERSECURITY THROUGH BETTER UNDERSTANDING VULNERABILITIES, NEEDS AND RESPONSES

The literature covering cybersecurity fails to clearly define the concept of cybersecurity. The meaning of cybersecurity varies from the security of unauthorised access to the management function designed to protect the organisation (Brookson, et al., 2015). Cybersecurity, defined with many definitions, has caused it to be a poorly understood term in our time (Urgessa, 2019). For the purpose of this research, cybersecurity will be defined as the protection of Cyberspace, the term expressed by authors (Brookson, et al., 2015, page 7):

Cybersecurity shall refer to security of Cyberspace, where Cyberspace itself refers to the set of links and relationships between objects that are accessible through a generalised telecommunications network, and to the set of objects themselves where they present interfaces allowing them remote control, remote access to data, or their participation in control actions within that Cyberspace.

2.1 Nature of vulnerabilities in public sector information systems

Many countries across the globe are embracing emerging trends in Cyberspace, concerns over cybersecurity are accumulating due to reports of increased breaches and attacks (Fearn, 2017; van Niekerk, 2017; SABC News, 2017). Common in most literature, cybersecurity importance has grown considerably in the last few years. Many countries are starting to establish a set of frameworks, policies, tools and security measures in order to prepare their environments for cybersecurity threats and vulnerabilities. Cybersecurity risks are getting worse every day due to newly implemented IT systems with computer systems that are getting weaker, even more vulnerable than traditional computer systems, and contribute to the rising cybersecurity vulnerability level.

2.1.1 Cyber threats and vulnerabilities in government

From the literature, the risk to government information systems can be defined as a potentially damaging consequence due to a cyber-attack or cyber threat that comprises the confidentiality, integrity, and availability of government information systems. Government websites, financial systems, infrastructure systems and government to citizen service platforms are the primary targets for cyber-attacks. These attacks range from identity theft, intellectual property theft and financial theft and critical infrastructure attacks. A cybersecurity vulnerability is a flaw or weakness in information systems and their weak or poorly implemented security controls that can be exploited (Alshayeb et al., 2020). Government is affected by the following vulnerabilities:

Web vulnerabilities

The top five most common categories of web attacks are malware, DDoS (Distributed Denial of Service), website defacement, SQLi (SQL Injection) and account Hijacking. Cyber-attacks continue to infect web sites and web applications, allowing attackers to access sensitive data and exploiting legitimate web sites (ENISA, 2019; Parsons, 2019). Government Websites were hacked and defaced in 2018 – 2020, cyber-attacks are continuously increasing and targeting web vulnerabilities (Breakfast, 2018; Smith, 2019a; Smith, 2019b).

Software / System vulnerabilities

Diesch, Pfaff and Krcmar (2020) research emphasise that system vulnerabilities are the gaps or weaknesses that make threats possible and entices threat actors to exploit these vulnerabilities. A weakness in system security procedures, internal controls and implementation design is a few examples (ENISA, 2019). Governments e-government services and government Information systems are vulnerable, the city of Johannesburg ransomware incident that took place in 2019 shows how vulnerable government systems are to cyber-attacks (Paton, 2019).

Security vulnerabilities

ICT systems deal with an enormous amount of sensitive data, such as personal files, company records, government files, etc. ICT systems are also often in control centres of critical infrastructure. Critical infrastructure may be subject to cyber-attacks and requires additional cybersecurity measures to protect against Information leakage/loss, prevent unauthorised access, and secure all communication in and out (ENISA, 2019; Williams, et al., 2020).

Access rights management is important for both the physical and the cyber domains and allows for granular management of all authorised personnel, with the ability to restrict access. Access Management in government systems can be compromised, as identified in the incident that took place at the Department of Employment and Labour in which over 300 staff credentials were compromised (Department of Employment & Labour, 2020).

For the government to prepare for the inevitable cyber threats, the government needs to understand and consider what cyber threats apply to departments (ITU, 2018b). The National Cybersecurity Policy Framework (NCPF) acknowledges the following cyber threats categories: cybercrime, cyber espionage, cyber warfare and cyber-terrorism.

Table 3: Comparison of NCPF cyber threats categories

	Target	Method	Motivation
Cybercrime	Individuals	Distributed denial of service	
	Private Companies	Identity theft	Economic gain
	Government	Malware	
Cyber espionage	Individuals	Different techniques and	Political gain
	Private Companies	methods (attacking	Economic gain
	Government	organisation gateway)	
Cyberwarfare	Infrastructure	Different techniques and	
	Information Technology	methods for disruption	Political gain
	(Private and Public)	(virus attack, DOS attack)	
Cyber terrorism	Public Sector	A range of methods	Political gain
	Private Sector	(hacking into the hospital)	Revenge

Cybercrime, cyber espionage, cyber terrorism, cyberwarfare

The term cybercrime broadly accepted in literature and defined in this study as criminal acts using information and communication technology (Jaccard & Nepal, 2014; Azmi, Tibben & Win, 2018).

Based on this definition, cybercrimes can be distinguished as the following:

- Targeted cybercrimes: crimes in which a computer or workstation is the target of the offence; and
- Cybercrimes Tools: crimes in which a computer or workstation is used to facilitate a traditional crime.

In a way, the NCPF is securitising the cybercrime issue (identity theft, fraud and phishing) as a matter of state security.

An action taken by a nation to penetrate another nation's ICT infrastructure for the purpose of disrupting or causing damage can be deemed as cyberwarfare. Cyberwarfare can either be offensive or defensive. The offensive form gathers intelligence about the cyber capabilities, configuration, and operations of a country that is regularly collected and used against them to disrupt, destabilise and degrade their cyber defence. Defensive cyberwarfare is mainly about countries strengthening their national cyber defence capabilities to proactively detect, analyse and mitigate against threats (Mbanaso, 2016).

Internet-based attacks by individuals, groups, terrorists to disrupt devices connected to the internet is cyber terrorism (Tehrani, Manap & Taji, 2013). Cyber terrorists use cyberspace to disrupt computer or telecommunications services to illicit widespread disruptions and loss of public confidence in the ability of government to function effectively.

From past cyber incidents, the following threats in government can be identified: Hackers exploiting coronavirus fear by spreading malware and e-mail viruses to carry out the malicious activity and spread computer viruses, Ransomware encrypts files then the criminals will then get in contact and offer to send the encryption key for a fee, data breaches such as third-party service providers information systems getting compromised, Hacktivism is now considered more sophisticated than ever before. It no longer only focuses on the social and political protest but includes politicised attacks, essential service disruption, espionage and cyber warfare (Breakfast, 2018; Department of Labour, 2018; Department of Employment & Labour, 2020; Dyess, 2020; Etheridge, 2018; Paton, 2019; Smith, 2019a; Smith, 2019b).

COVID-19 pandemic and cybersecurity

An emerging theme identified through the participant observation in the National GITOC - information security meeting is ICT Security trends and threats during Covid-19. The current pandemic due to COVID-19 is a very challenging issue for the government. The government needs to provide accurate and timely information to the public and sister departments. With the advancement of technology and cybersecurity challenges, it is common for hackers and attackers to take advantage of times when there are emergencies. The online video conferencing apps such as Microsoft Teams, Zoom, and Google meet usage have increased during the pandemic, bringing on more issues and threats in terms of cybersecurity (Alshayeb et al., 2020). The government will have to deal with the growing security demands emerging from the increased risk of cyberattacks.

The recent outbreak of the coronavirus pandemic has seen a considerable increase in the number of user or officials interacting with each other working online. Taking advantage of this situation, bad

actors in cybersecurity have become more active by hacking and attacking for financial gain and other interests. Government is vulnerable to cyber threats such as phishing and malware or ransomware attacks (Broh et al., 2018; Brohi & Dion, 2020). The following top cybersecurity threats amid COVID-19 are:

DDoS attack

Government departments have seen an increase in Distributed Denial of Service (DDoS) in the current pandemic due to COVID-19. Hackers are flooding the government departments websites or systems by attacking the communication channel, crashing the relevant website or government system (Chigada & Madzinga, 2021). The DDoS purpose is to attack network traffic rendering a computer resource or network unavailable. By targeting organisations computers and their network connection, the organisation's operations, reputation, and trustworthiness can be damaged (Arabo & Pranggono, 2021). The majority of DDoS attacks focus on targeting the transport and network layers to overwhelm the target machine, rendering the system resources inefficient until the server or system goes offline. These attacks can also saturate the entire network with malicious traffic, causing the entire network to be temporarily unusable.

Malware

Malware, spyware and trojans spread by cybercriminals in the current pandemic are taking advantage of the situation. Malware, spyware and trojans embedded in coronavirus maps and websites infect individuals, organisations and government by luring the targets to follow a link in an email or downloading malware to their computers or mobile devices (Chigada & Madzinga, 2021; Arabo & Pranggono, 2021). 94% of computers corrupted by malware during the pandemic were infected by an email. Malware, defined as a dangerous application, can lead to data leakage of government information and cause government departments systems to malfunction and interrupting the department's operations. Cybercriminals are targeting the government through phishing emails and hyperlink attachments. Workstations can be infected by malware at any given time if the device is connected to the organisation network.

Ransomware

Ransomware attacks targeting government institutions by cybercriminals rely on the government, which cannot afford to be locked out of their systems during this highly critical time, forcing them to pay the ransom (Chigada & Madzinga, 2021). Ransomware infects systems via email attachments, links and already exploited employee workstations that are vulnerable (Arabo & Pranggono, 2021). A malicious program Ransomware that was designed to facilitate a broad range of despicable activities. It prevents access to people or organisations data unless a ransom is paid (typically using some cryptocurrency, such as bitcoin). An example of ransomware deployed during covid is CovidLock, developed to monitor statistics on COVID-19. Users installing this application have to grant permissions on the users' mobile device. Once the application is installed, it blocks user contacts, pictures, videos, and social media accounts access. To regain access, the victim has to pay the ransom using bitcoins. If the attacker does not receive the bitcoins, the infected data will either be published or erased.

Spam emails

Spam emails using coronavirus themed emails with malicious attachments have increased during the pandemic. A common way to spread malware is via email. Cybercriminals use the pandemic to entice people to click, primarily by hiding the executable in archive files. During the COVID-19 pandemic, Phishing was observed as a common threat. Attacks via spam e-mails containing the word "corona" or "covid" have been reported. Attackers impersonated the World Health Organization (WHO), and the infected e-mails often contained subject lines such as "COVID-19 updates" or "COVID-19 tracker of your city". Malicious actors use existing, genuine covid materials as bait to click or open an attachment.

Malicious URL's

Dixon and Balson (2020) state that cybercriminals are taking advantage of the COVID-19 pandemic by creating malicious URL's. These URL's relating to the coronavirus attract unsuspecting users looking for COVID-19 information or statistics. Threat actors gain access to sensitive information from their victims that believe they have connected to legitimate COVID-19 URL's. Websites that claim to be applications to protect against covid-19 lure individual targets and then proceeds to request the user to either enter their credit cards details or install malware.

2.2 Approach to the alignment of cybersecurity responses with vulnerabilities and needs in government departments

2.2.1 Cybersecurity frameworks

Today's organisations need to comply with industry specific regulations, policies and standards (Gourisetti & Patangia, 2020). There are a number of cybersecurity standards and frameworks available. Researchers Azmi, et al. (2018) emphasise there are many cybersecurity frameworks and they share the same concepts. Organisations can benefit by adapting either a single cybersecurity framework or a combination of frameworks as there is no one size fits all for the public and private sector. Cybersecurity frameworks assist those charged with cyber governance at the organisation to mitigate the risks associated with the adoption and deployment of cybersecurity. The benefits of frameworks are that it assists public and private organisations in achieving their objectives for the governance and management of cybersecurity. In the private sector, adopting frameworks can aid in creating a defined structure within which to work. As technology has continued to evolve, the frameworks in cybersecurity have also done so over time. Frameworks have also been known to assist in bringing down costs, improving efficiency and security, and increasing productivity within business operations (Weber & Rudman, 2018). Organisations are not limited to a single framework or standard and can use a combination to achieve cybersecurity for their organisational needs (ITU, 2018b).

The National Cybersecurity Policy Framework (NCPF) requires that there be alignment and coordination across government. According to Gcaza and von Solms (2017), the analysis of the government environment, NCPF stipulates and accepts that a culture of cybersecurity is an imperative. However, Sutherland (2017) has expressed the lack of priority placed on cybersecurity as the timeframe it took to adopt the National Cybersecurity Policy Framework and how slow the framework's implementation has taken. The NCPF is deemed sufficient, according to Gcaza and von Solms (2017), to provide the strategic direction of SA concerning a cybersecurity culture. As to the

literature, government departments will need to look at their approved frameworks such as the Corporate Governance Information Communication Technology Policy and the National Cybersecurity Policy Framework (NCPF) and assess if the department's strategic plans are aligned to ensure cybersecurity.

2.2.2 Cybersecurity standards

Research has shown that government needs a cybersecurity strategy that protects its information systems from emerging cyber threats and cyber-attacks and is aligned to governments business that will incorporate standards, frameworks, and best practices (Pretorius & Ngejane, 2019). Tambo and Adama (2017) research suggest that to ensure resilient and reliable public and financial institutions security, national and international standards are required to promote reliability, integrity and availability of critical data and information through collaborative and coordinated cybersecurity. Through the application of cybersecurity standards to government and public organisations, tangible benefits that justify the time and financial resources can be witnessed. Leveraging on cyberspace standards, telecommunication standards, and electronic infrastructure is crucial to cope with technological developments to mitigate hackers. The organisation's data and information security, awareness and risk are boosted, and potential inside and outside vulnerabilities or attacks are mitigated through standards. Mbanaso, Abrahams and Apene (2019) research further support cybersecurity standards promote effective management for cybersecurity risks in organisations. Standards with specific reference to alignment are non-existent as standards are generally generic and can be easily implemented and adapted for most industries. The International Organization for Standardization (ISO) and the National Institute of Standards and Technology (NIST) are involved in mitigating the impact of cyberattacks. Through developing cybersecurity frameworks, security protocols, and guidelines, cyberattacks are minimised.

Some of the following standards utilised in the NCPF (*Mshunqane, Z. (2017)*):

ISO/IEC 27001 & ISO/IEC 27002

The International Organisation for Standards (ISO) 27001 and 27002 regarded as a framework for security controls that provides generic requirements for assessing and treating information security risks. These standards can be tailored to the organisation's needs and applied to all organisations regardless of the type, size or nature. ISO/IEC 27001 focuses on the requirements for establishing, implementing, maintaining and continually improving information security management. ISO/IEC 27001 is based on the old approach of information security that focuses on security information and system security, whereas cybersecurity focuses on more than information or system security.

For cybersecurity, ISO/IEC 27001 and 27002 are generally followed for information and system security. The 27001 focuses on information security management systems, and 27002 on code of practice for information security controls, however, it maps directly to additional national standards of South Africa (ISO, 2018).

COBIT

Control objectives for information and related technologies (COBIT) are commonly used in enterprise governance and the management of information and technology frameworks. It provides

documentation to build and maintain through a set of controls for the governance of information technology. COBIT as such is not a framework for cybersecurity but rather a risk-based control and governance framework. In the COBIT framework, cybersecurity is linked via other information security and cybersecurity frameworks (ISACA, 2018).

NIST Cybersecurity framework

The NIST Cybersecurity framework has been developed utilising recognised standards such as the Control Objectives for Information and Related Technologies (COBIT), International Organisation for Standardisation (ISO) and International Electrotechnical Commission (IEC). According to the National Institute of Standards and Technology (NIST, 2018), the NIST Cybersecurity framework is has been developed to reduce cybersecurity risk and improve cybersecurity to critical infrastructure. NIST Cybersecurity Framework, a framework that integrates industry standards and best practices to help organisations manage their cybersecurity risks. The NIST Cybersecurity Framework enables a common language that allows staff at all levels within an organisation to develop a shared understanding of their cybersecurity risks. The NIST Cybersecurity framework provides a reference model that allows an organisation to implement effective cybersecurity by continuously applying cybersecurity risk management to improve the resilience of information systems and critical infrastructure and complements the National Cybersecurity Policy Framework (NCPF) as a scorecard (Krumay, Bernroider & Walser, 2018).

2.2.3 People management for improved cybersecurity

By their very nature, humans are central to the state and, because of this, central to security. The growing sophistication in information technologies, associated attacks, and crime calls for a corresponding level and amount of skills to meet such challenges. Organisations have become concerned about security trends that threaten their business and operations due to increased cyber-attacks. Cyber-attacks have effectively beaten security solutions by exploiting the human-factor limitations in knowledge and skills. These attack patterns have manipulated human elements into unintentionally conveying access to critical government systems. Awareness training focuses on providing users with the knowledge of the most common issues. Security software will never replace the people using the machines and is there to aid the users and not act on their own and serve as a means of defence. As such, organisations that seek to be up the curve of cyber, need to train and have a pool of highly skilled individuals. Cyber-attacks have effectively beaten technological security solutions through exploiting human-factor limitations in knowledge and skills (Chandarman & Van Niekerk, 2017; Craig, 2018).

As often repeated in literature, the weakest point in the security chain seems to be the human. The main issue, the human factor, is impossible to fix completely, this raises the importance of management and planning (Dalal, et al., 2021). From the people management viewpoint, it is achieved foremost by informing employees of the importance of cybersecurity. Cybersecurity knowledge attributes towards workforce security capability, which is invaluable to achieve a secure environment. Effective implementation of security knowledge and skills should be built on a clear understanding of existing capability and the identification of cybersecurity capability shortfalls that reveal vulnerabilities. This is achieved by training and including employees in the securing activities and is

essential for building a cybersecurity culture (Tambo & Adama, 2017; Craig, 2018). Cyber-attacks on government employees become effective due to a couple of reasons, weak or lack of sufficient cybersecurity knowledge and skills, negligence, misinformation (Dalal, et al., 2021).

NCPF needs more work, for example, there is a need for specific detail about how the cyber human resource will be trained and what the timelines are. A commendable component of the NCPF is the way it targets awareness and education as critical pillars to cybersecurity due to the human factor. One way to reduce organisation cybersecurity vulnerabilities or risk potential is to enhance the department's cybersecurity capabilities through improving cybersecurity awareness and training. Humans will always be involved directly or indirectly will play a major role towards achieving cybersecurity objectives (Marble, et al., 2015). Cyber resilience, often regarded as a sub-discipline of resilience, is about returning to normal in the event of a disruption on (digital) information systems. On the other hand, it is also about preventing disruptions from significantly affecting the government department business processes' continuation. Cybercriminals are increasingly choosing attacks that do not focus on just technical weaknesses and include the human factor.

2.3 Responding to improve cyber resilience

Research has shown that departments need to have cyber resilience that can mitigate cyber risks for the government to respond to cyber incidents. Frameworks can support the provincial government departments risk governance processes and procedures by exerting emphasis on strategic responsibility and leadership, focusing on opportunities, making risk-informed decisions, and contribute to the achievement of operational resilience against organisational risks and cybersecurity risks. Cybersecurity resilience refers to the ability to continue with business operation despite adverse cyber events taken place. Cybersecurity's general objective is to protect networked IT and information systems, and cyber resilience is focused on a higher-level objective of delivering the governments departments strategic and operational objectives (Von Solms, 2018). Information systems can be said to be resilient only when they continuously deliver business value. Even in the face of adverse cybersecurity events, the provincial government departments must focus on the business operations resilience as its starting point rather than information technology when implementing cybersecurity resilience.

Cyber resilience is not only about technology, and it covers people and processes. Cyber resilience cannot exist in isolation and needs to be integrated and aligned in the organisation. Cyber resilience is about being proactive and not reactive (Carew, 2019). If cybersecurity is not adequately addressed, the cost will be perceived as being to be high, and risks are likely to increase with emerging cyber threats and the adoption of the fourth industrial revolution (Lees, Crawford, & Jansen, 2018). However, cybersecurity resilience is not easy to implement and operationalise. Cybersecurity resilience is a multi-dimensional conception that involves governance, awareness training, and business continuity management. Some authors consider cyber resilience a part of cybersecurity-focused on responding to a cyber incident; other authors consider cyber resilience a more holistic concept that includes the whole lifecycle and the strategic and human processes into cybersecurity (Schneier, 2014; Cybenko, 2016). The government needs to develop comprehensive cybersecurity and

data resilience strategies. While cybersecurity defences are essential to prevent attacks, they are no longer sufficient in isolation.

The pervasiveness of cybercrime means that the real challenge for the government is being prepared for a cyber-attack. Critical government systems need to be identified and adequate protection applied, departments need to be able to detect cyber-attacks quickly and then contain and recover their systems as fast as possible. Tying all of this together is the need for a strong governance framework that outlines a cyber resilience strategy and create accountability and alignment with government frameworks, policies and standards (Von Solms, 2018).

2.3.1 Cybersecurity alignment

Alignment has become an organisations' necessity to bring about risk management, effectiveness, resilience, mitigation and compliance (Bohnert, Gatzert, Hoyt, & Lechner, 2019). Establishing government-wide risk governance is complex and requires multiple risk functions. Managing departmental risks with cybersecurity risks and aligning to business is a problem whereby this alignment is missing or is not established (Chigada & Kyobe, 2018). Risk governance proficiency has improved over time; however, the benefits derived from cybersecurity and risk management have not been fully gained, which can be construed as mismanagement of risks. Meaning that without the alignment of cybersecurity and risk, resilience cannot be improved in departments, as cybersecurity risks are considered one of the most important factors for digital transformation and e-government services (ITU, 2018b).

IT governance two primary purposes are the alignment between IT activities and organisational goals and the generation of value from IT. The alignment should be based on the defining role of the government in cybersecurity. A better understanding of NIST CSF adoption may also assist information security and align with cybersecurity strategy and frameworks. Héroux and Fortin (2017) emphasise that there is a high potential risk of misalignment between IT governance and corporate governance. The integration between business and IT is critical as it embraces the constraints and dependencies inherent to the government department and focuses on the activities that management in the department perform to achieve interconnected goals. IT governance is an integral and important part of corporate governance (Héroux & Fortin, 2017).

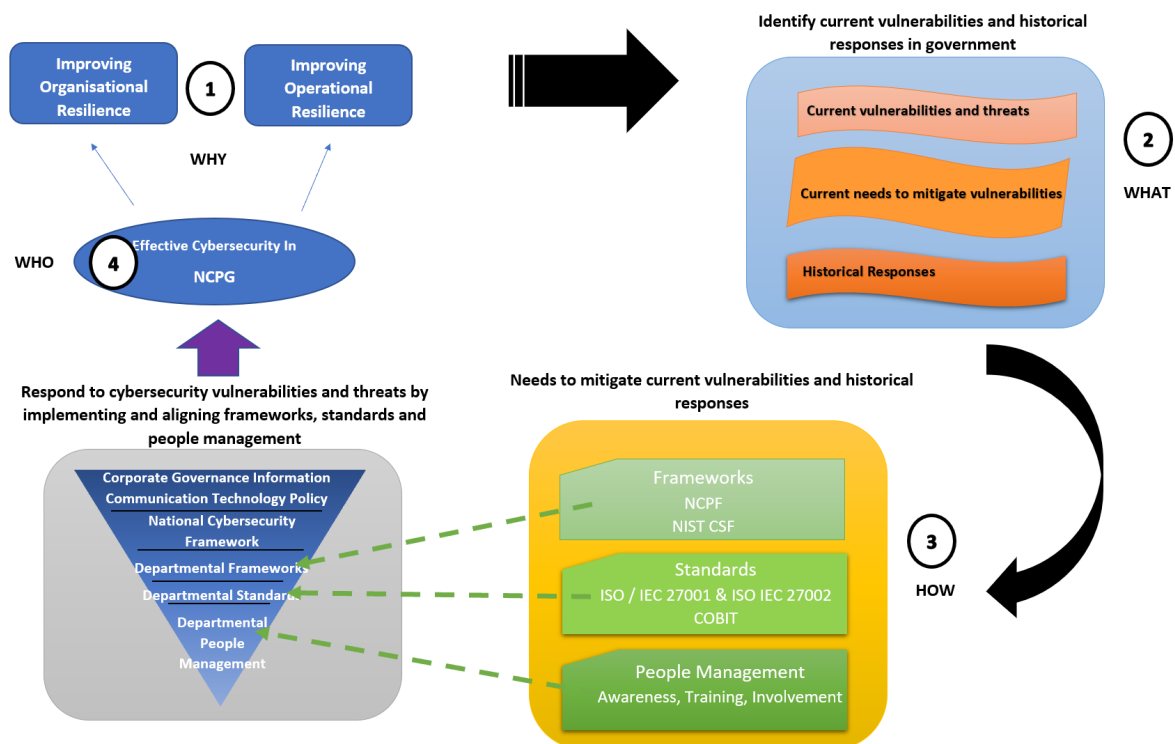
2.4 Analytical framework

Global technological advancement has influenced the public sector in South Africa, and this technological advancement has brought about an environment whereby cybersecurity has become a necessity. An analytical framework for aligning cybersecurity vulnerabilities, needs and responses in government is expressed as the requirement of improving organisational and operational resilience (why) to prepare for inevitable cyber threats. For the government to prepare for these threats, it needs to understand and consider what current cyber vulnerabilities impact government departments and the needs to mitigate these vulnerabilities are and how departments historically responded (What). Through the implementation of frameworks, standards and people management, to mitigate

the identified cybersecurity needs (How), the Provincial Government (Who) can respond to cyber-attacks and ensure operational resilience for future events.

The analytical framework is based on the literature review using a systematic approach, as described in section 3.2.2.2. The literature background is based on what government departments require for the alignment of frameworks, standards, and people management to mitigate cybersecurity risks in response to cyber-attacks and ensure operational resilience. This framework is used to guide the collection of qualitative and quantitative content and analyse each of the three themes selected for effective alignment to improve government departments' organisational and operational resilience.

Figure 5: Research Analytical Framework (own diagram)



Source: Harris, 2020

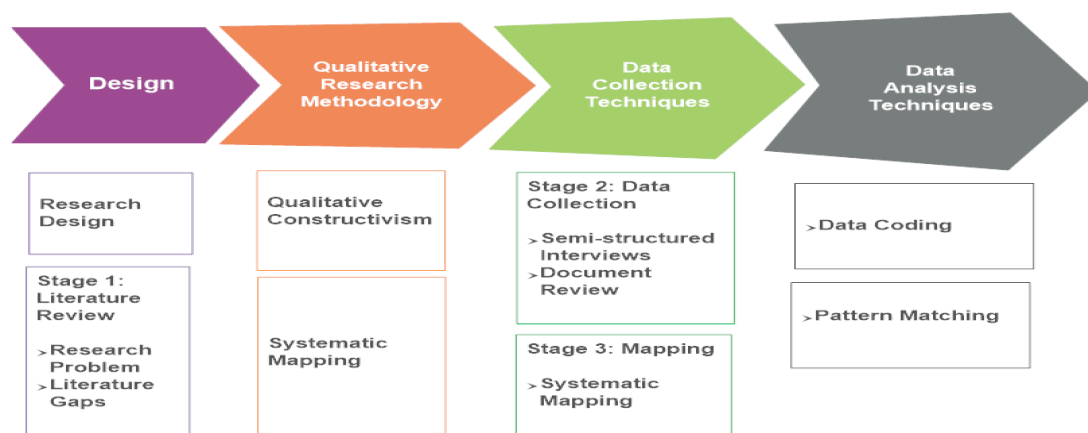
This analytical framework informs the data collection and analysis of this research. This was done by identifying cybersecurity vulnerabilities and the needs to respond through implementing and aligning frameworks, standards and people management in the provincial government.

CHAPTER 3: RESEARCH METHODOLOGY: QUALITATIVE CONSTRUCTIVIST AND SYSTEMATIC MAPPING METHODOLOGY

3.1 Introduction

This section outlines the research methodology and identifies the appropriate methods which the researcher applied to address the research purpose and research questions. Methods of research design are examined in relation to the research diagram. The previous chapters have considered the literature as a baseline to address the research questions. This section is subdivided into sections that explain why specific research methods were chosen.

Figure 6: Research Methodology diagram



Author, 2020

3.2. Research design: Steps to collect and analyse data towards the research goal

The research design was broken into components such as purpose, approach, research methods and techniques (Abutabanjah & Jaradat, (2018). The research methods and how the research study analysis took place was captured in the research design. The research design further outlines the steps that need to be planned to reach the research goal (Hammarberg, Kirkman & de Lacey, 2016). Through the adoption of qualitative constructivism (chosen for its ability to map the participant's views and perceptions in a case when there is a lack of knowledge) and systematic mapping (chosen for its ability to identify limitations and gaps in research) that intends to capture responses and promote in-depth answer and meanings from analysing the data collected. Keeping this scope in mind the following data, tools and techniques have been selected (Primary data – interview and document review, secondary data – systematic mapping). Both primary and secondary data analysis rely on constructivist research philosophy and driven by the research questions.

3.3. Research methodology: Qualitative constructivism and systematic mapping

When considering the limited published research regarding the South African government information systems, cybersecurity, alignment and needs the researcher examined different research methodologies to select an effective research methodology. A qualitative constructivism method research approach will allow the researcher to comprehend the government's cybersecurity challenges. Since this is an academic research study, the researcher sought approval and clearance to carry out research from the school of literature, language and media research ethics committee of the University of the Witwatersrand in South Africa before any data was collected. Approval was granted by the school of literature, language and media research ethics committee by means of an application requesting permission to conduct the research. The clearance certificate, an officially authenticated document from the University of the Witwatersrand, was approved, clearance certificate number: SLLM-M20-01 (Appendix C). Additionally, in keeping with ethical standards, the researcher applied the general rules, guidelines and standards for conducting research. The researcher's limitations were further acknowledged, and the research findings shall be made available for academic reference.

Further a case study on the provincial government was used to allow the researcher to gather information for the research study. As Yin (2009) states, "case studies are suitable for situations that emphasise thorough understanding in an individual setting, that focuses on current events." Case study evidence using multiple sources allows a researcher to report on a broader range. Case study research can be singular or include multiple case studies. There is a common concern that case studies provide little basis for generalisation, but Yin (2009) states that case studies can be generalised to the limits of their theoretical proportions.

3.3.1 Qualitative constructivism

Based on the constructivist design, the constructivist researcher chooses to utilise qualitative data collection methods and analysis. Alternatively, the constructivist researcher can utilise a combination of both qualitative and quantitative methods (mixed) (Chow, 2014). The qualitative constructivist research theory method was chosen to determine the nature of cybersecurity and to better understand other aspects of the research. The research problem, the research question, and the research objectives unknown aspects could be better explored, understood and explained by applying the research theory method. "Not everything that can be counted counts, and not everything that counts can be counted" (attributed to Albert Einstein; Patton & Cochran, 2002).

Constructivists believe that knowledge is essentially subjective in the environment, constructed from our observations and mutually decided upon agreements (Gash, 2014). As to this view, constructivism was selected as new knowledge that needed to be collected rather than merely acquiring it via memory or solely communication from those who know to those who do not know about cybersecurity in the provincial government. Constructivists believe that meaning or understanding is achieved by integrating the information with existing knowledge and then analysing the new information or knowledge (Gash, 2014). With the limited knowledge available, a constructivist approach will assist in mapping the participant's views and perceptions relating to the research questions and provide a means to explore the issues and lack of knowledge in the case study.

The qualitative method helps the researcher to understand the research problem, the elements and interdependencies that are unknown. As part of the mixed-method, the qualitative evidence formulated via academic journals, publications and unpublished documents and reports for a more

comprehensive understanding. According to Chow (2014), qualitative research has both strengths and limitations; however, it offers a vital way to engage and explore issues that cannot be quantifiable.

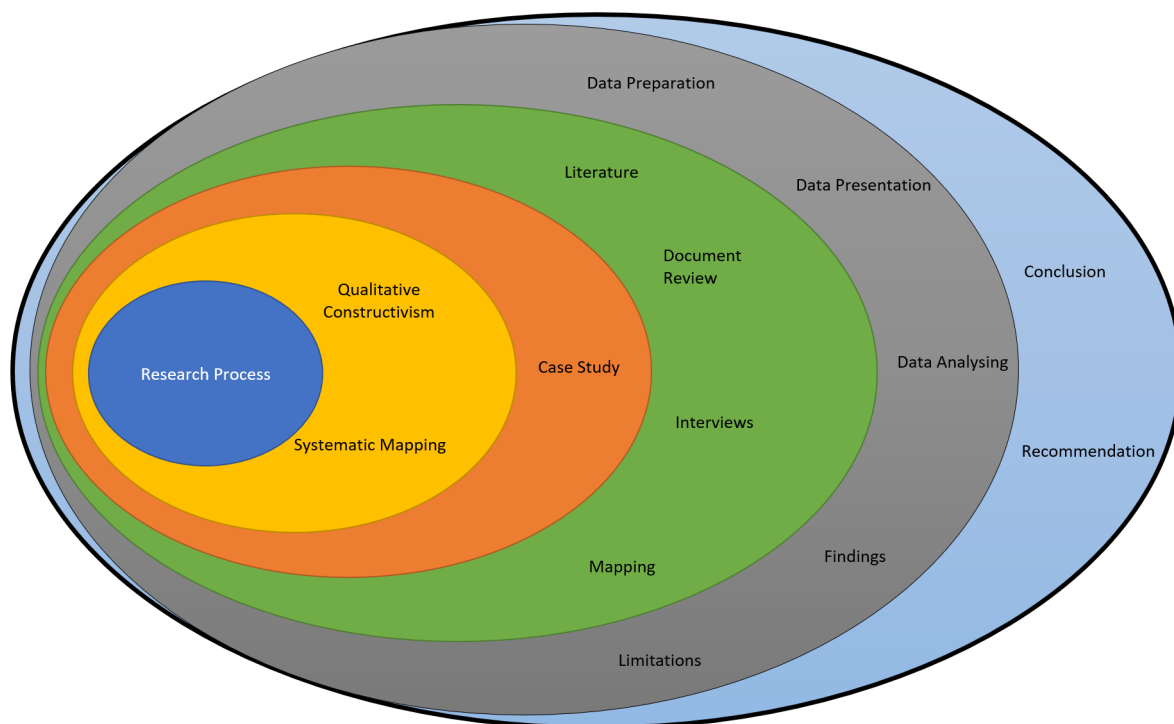
Figure 7: Qualitative Constructivism

Qualitative Constructivism
Method
Text or Image data
Open-ended questions
Emerging approaches
Research Practices
Focuses on a single phenomenon
Adds personal values in to the study
Studies context
Validates the accuracy
Interprets the data
Collaborates with participants

3.4 Research approach: Data collection and data analysis

A research approach represents the plan and steps upon which the researcher followed to assist in collecting, analysing, and interpreting data (Creswell, 2018). The research approach consists of three stages; the first stage consists of a literature review based on a manual selection of academic research papers, where the topic of cybersecurity is broadly searched and researched, the documents were then reviewed and allocated to a theme (e.g. cyber threats, vulnerabilities, frameworks, standards, alignment). This stage provides a broad view of what knowledge on the cybersecurity topic is available and if there is a need for further research. The second stage is to investigate further the literature review with a systematic focus on mapping the principal elements and assessing the findings to determine various dimensions of the research problem. The third stage was focused on collecting primary data from interviews, documents, questionnaires and surveys from the case study.

Figure 8: Research Process



Author, 2020

3.4.1 Primary Data

3.4.1.1 Interviews

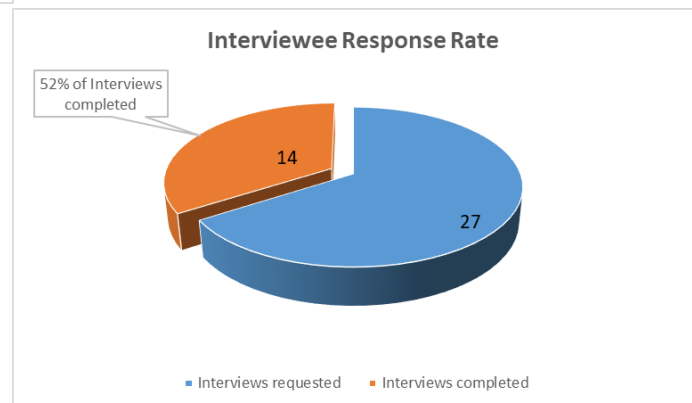
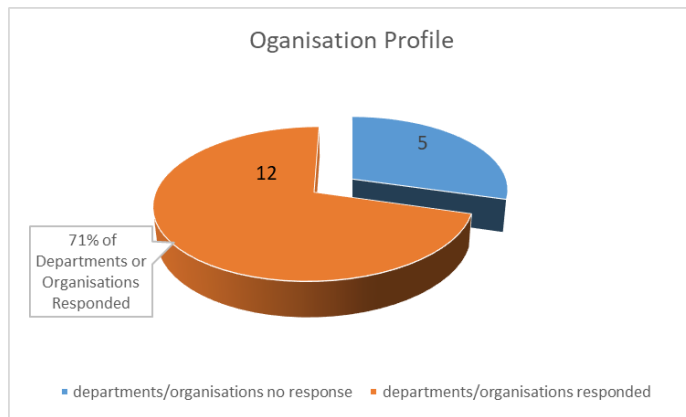
The researcher utilised interviews as a research tool to get responses in a shape that allowed the respondents to have discussions and with the researcher in a singular or combination of selected participants (Stoneman & Gilbert, 2016). Interviews provide the researcher with an advantage in collecting in-depth information from different respondents. A further advantage is of interviews allows for follow-ups if the information collected needs clarity and allows for respondents of different positions and locations to be interviewed. The design of interviews can be unstructured, structured and semi-structured. The semi-structured interview seems most suitable to use for this research as a semi-structured, face-to-face interview (traditional or electronically due to COVID pandemic) can stimulate opinions and elaborations from the respondents, and its principal characteristic is its flexibility and versatility in gathering responses (Myers, 2013) (Stoneman & Gilbert, 2016).

Background information on organisation and interviewees

Seventeen departments or organisations that included twenty-seven individuals were requested to participate in the research. The names of the departments/organisations and participants have not been declared as the research topic was considered sensitive, and therefore the research was conducted as an anonymous study. Approval from the overlapping organisation stipulated that information regarding departments and individuals was to be kept confidential.

Figure 09: Organisation Response Rate

Figure 10: Interviewee Response Rate



Source: Harris, 2021

Source: Harris, 2021

The primary interview data is from fourteen interviews conducted from twelve departments or organisations in the province.

3.4.1.2 Participant observation: MS Teams Virtual Meetings

Participant observation: By observing the discussions and noting down the key issues discussed regarding cybersecurity matters, that can be used as data. Participant observation is a qualitative research methodology and involves active participation and observation of a defined group of people in their environment, such as the provincial government. The objective is for the researcher to collect data utilising participant observation to provide depth and context to observations and help minimise mistaken assumptions. What sets participant observation apart from other ways of doing research, the researcher is embodied, participating in the environment of the research subject.

3.4.2 Secondary Data

3.4.2.1 Document review

A document review of existing unpublished documents (MPAT, Audit General, Internal Audit and departmental ICT), reports being conducted to ascertain relevant data (Myers, 2013). Relevant documents and reports are reviewed and analysed according to the themes: vulnerabilities, needs and responding for cybersecurity.

3.4.2.2 Systematic Mapping

The systematic mapping study must not get confused with a systematic literature review methodology, the systematic mapping is a mapping of the provincial government data and is a lighter

form of the systematic mapping methodology. The lighter systematic mapping method was chosen as a more comprehensive systematic literature review was not required at this research level. Using systematic mapping, existing research on cybersecurity can be better understood by identifying the limitations and gaps of current research. By using a systematic mapping methodology (Nguyen, Ali, & Yue, 2017), existing research on cybersecurity was used to contribute to this research by identifying those categories of cybersecurity data that needed to be investigated in the study context. In order to select the cybersecurity data categories, a set of variables were identified focused on the publication and bibliographic data. Data was then extracted into Microsoft excel to formulate the data visualisations.

From the research completed through a systematic mapping, the following limitations or gaps were identified: Research published from 2016 till today has limited research with regard to South Africa and cybersecurity. When you further extend the search criteria to include the government, the data presents a very small percentage for the South Africa government and cybersecurity. A further potential source of limitations and gaps in the research can be the fact that only research published in the English language has been selected. This decision may result in a possible threat to rationality because potentially important research published in other languages may not have been selected. However, the English language is the most widely used language for scientific papers, so that this bias can be reasonably considered as minimal.

The mapping process involved performing five steps, where each step's outcome provides the next step's input. In step 1, research questions and objectives are defined to provide a general scope for the study. Step 2 the search strategy is defined to find the published studies from the available digital libraries. In step 3, relevant studies can be chosen using a screening process using inclusion and exclusion criteria. Step 4, the keywording enables classification and data extraction, and in the final step, step 5 data category extraction and mapping process was conducted.

Table 4: Five steps mapping process

Step 1	Step 2	Step 3	Step 4	Step 5
Definition of the research question	Search strategy defined	Screening process	Keywording	Data category extraction
Scope defined	All Papers searched	Relevant Papers chosen	Classification enabled	Systematic Map

This systematic mapping process was followed and is used to frame the data visualisations presented in Chapter 4. The data used in these visualisations were extracted from government documents and interviews. See diagram in section 4.2.

3.4.3 Data Collection Summary

Table 5: Collection Methods

Data Collection Methods			
Data Collection Method	Research Questions	Target Informants	Reason for gathering data from the informant in this manner
Traditional Literature review	All research questions broadly covered.	N/A	Broadly based review of existing academic literature and reports
Systematic Mapping	All research questions covered.	N/A	Mapping of existing academic literature and reports
Semi-structured Interviews	All research questions covered.	GITOC SITA Internal Audit	Collecting of in-depth information from different respondents
Document review	All research questions covered.	SITA Auditor General Internal Audit	Review of relevant documents and reports relating to cybersecurity.

3.4.3.1 Use of visualisations for data presentation

Data visualisation is crucial to helping people understand and make sense of collected data. In addition to computational and statistical approaches, visualisation techniques are needed to enable the interpretation of data and the communication of results. Researchers use illustrations of data for two purposes: first, to visualise and explore correlations and predictions among data sets; and second, to illustrate these data's interpretations clearly and concisely to an audience (Pettersson, 2010). This research mainly used MS Excel to analyse the relevant data in the field of cybersecurity in order to design visual presentations. The researcher captured all relevant data into MS Excel and created visual illustrations from the data to illustrate the analysed data. These visual presentations include the following types: Sunburst chart, selected for visualising data in rings broken into individual parts (executive management buy-in); Clustered bar chart, provided a method to visualise data over periods with quantities (Respondents experience); Column chart, visualising data in columns making it easier to identify quantity and differences (Cybersecurity Key Performance); Stacked column, providing more details, individual categorised data visible for easier interpretation (Types of cyber vulnerabilities most likely to affect information systems); Pie charts, allowed the research present the data in pieces with either quantities or percentages (Visibility of cybersecurity threats); Stacked bar, provided a method to visualise each respondents data (Improving operational resilience through effective cybersecurity).

3.4.4 Data analysis

The process to be used to analyse raw data collected from different sources, that is, interviews and document review as a primary source and systematic mapping as a secondary source to answer the research questions. Data analysis is a critical part of the research because it allows the researcher to reduce, convert and interpret data collected (Myers, 2013). Data analysis is an ongoing process; therefore, emerging data long the way will be considered. There is no single correct analysis method, and the process can be personalised and reviewed for each study (Auerbach & Silverstein, 2003).

Coding and organising data

3.4.4.1 Data coding

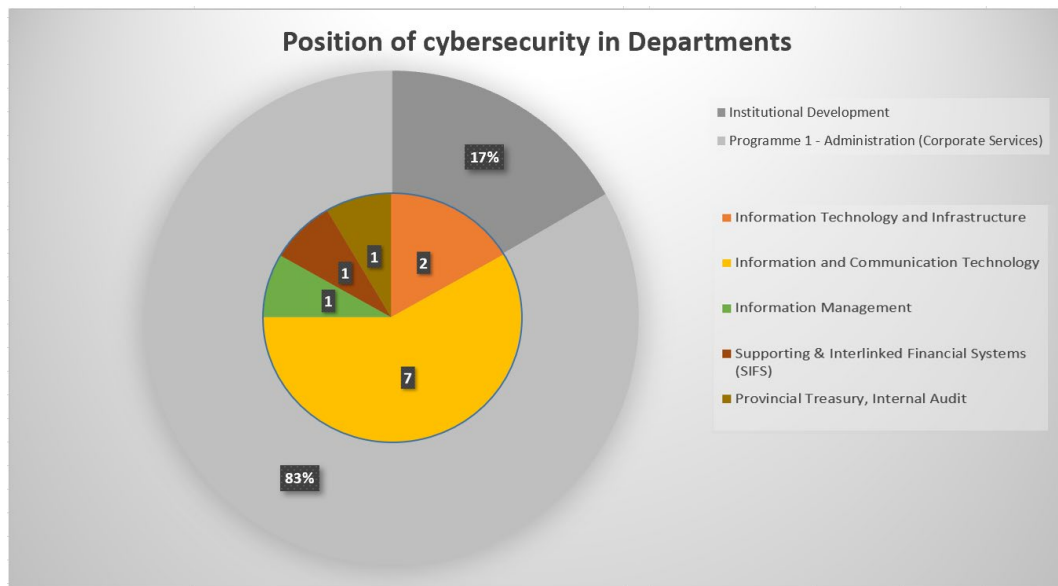
Qualitative data coding is a common method to identify the data collected by semi-structured interviews (Auerbach & Silverstein, 2003). The coding method was adopted to transform the interview with each individual into a script. Data coding is the result of collected data that has been analysed, abstracted and reassembled. Through data coding, the researcher can make meaning from the data gathered, and further conclusions are determined (Bazeley, 2009). The communications for gathering the qualitative data was through a phone call or video conferencing due to the COVID-19 Pandemic and a document review. An in-depth exploration of primary and secondary data comparing the interviews' findings, document review and any other qualitative data with the literature review findings and discussing differences between them. A pseudonym (false name) to represent data collected through an interview with participants was organised and recorded in the research report to ensure anonymity. The data collected from this research project was stored and will be encrypted for three years.

Table 6: Respondent Roles / Government Titles / Ranks

Overview of the respondent's roles in the provincial government.		Pseudonym
Respondent	Roles / Titles / Rank	
1	Government Information Technology Officer	GITO 1
2	Government Information Technology Officer	GITO 2
3	Government Information Technology Officer	GITO 3
4	IT/ICT Manager	ICT Manager 1
5	IT/ICT Manager	ICT Manager 2
6	Government Information Technology Officer	GITO 4
7	IT/ICT Manager	ICT Manager 3
8	Government Information Technology Officer	GITO 5
9	Senior Manager	Senior Manager 1
10	IT Technician	Technician 1
11	Audit Executive	Audit 1
12	IT/ICT Manager	ICT Manager 4
13	External: Audit Executive	Audit 2
14	External: IT/ICT Manager	ICT Manager 5

Aiming to understand in detail the provincial government departments nature as to where Information Communication Technology, ICT Security and Cybersecurity positions into the organisation. Clear from the data, it can be deduced that cybersecurity units or directorates mostly fall in the administration chief directorate in government departments. Programme 1 - administration is accountable and responsible for reporting and managing supporting directorates.

Figure 11: Position of Cybersecurity in departments (outer ring program, inner pie unit)



Source: Harris, 2021

Data collected went through a coding phase, and concepts, themes, and keywords from transcriptions were identified and labelled. Coding identified patterns and areas that needed focus in the data.

3.4.4.2 Pattern matching

Qualitative pattern matching is based on comparing theoretical patterns with observed patterns and can be especially useful for research (Sinkovics, 2018). The analysis will involve the deconstruction of the qualitative data into manageable patterns in accordance with the research aims. After the interviews, the interviewee responses were analysed for qualitative thematic trends and patterns and revealed factors of importance. Participant data were analysed to identify new themes or patterns meaningful to the research questions. The provincial government documents enabled the researcher to note patterns on how the departments enforce cybersecurity policies.

3.4.4.3 Atlas.ti for qualitative data analysis

The researcher will use computer software to store, retrieve, and analyse the collected data. Atlas.ti can help the researcher critically examine and analyse the data by sorting it, thereby allowing meaningful associations to emerge (Smit, 2014). The computer program was used to encode in-depth interviews and document analysis data to produce main themes and sub-topics. The coding technique involved a process of classifying and categorising text data partitions or a set of codes (concepts), categories (constructs), and relationships. Paulus et al. (2017) state that Atlas.ti codes and memo functions enrich and enhance the research findings through the addition of researcher interpretation and reflection. Atlas.ti also helped automate various processes in analysing qualitative content, such as cataloguing primary documents, organising codes, and code descriptions. In addition, Atlas.ti also allowed the researcher to organise and catalogue all data completely and efficiently. In addition to the strengths mentioned above, Atlas.ti also made possible connections (relations) between codes, themes and sub-themes. Different relationships, similarities and differences were identified by utilising Atlas.ti. Paulus et al. (2017) also underlined Atlas's importance in asserting that Atlas.ti

effectively manages search data by organising codes alphabetically, presenting code strength, and graphically representing data.

I used Atlas.ti to perform thematic analysis (a method for identifying, analysing, organising, describing, and reporting themes found within a data set) with keyword queries to group the data into categories based upon the coding to identify patterns in the data. Once all data had been uploaded to Atlas.ti, the researcher performed an exploratory review to familiarise himself with the data better. While coding did not occur during this exploratory review, memos and brainstorming maps were created to assist. The researcher identified patterns in the data by applying data analysis and aligning the data to the themes for cybersecurity research questions. The data included relevant sources such as semi-structured interviews, video recordings (MS Teams) and organisational documents. The interview transcripts and relevant documents were entered into the Atlas.ti analysis tool, resulting in identifying the major themes. Interview transcripts and the relevant document was converted from word or excel documents into a pdf so that Atlas.ti could import the data.

Figure 12: Clean Data Spreadsheet

Z	AA	AB
7. What cybersecurity frameworks / standards are there in the department?	8. What controls are in place to mitigate cybersecurity vulnerabilities in the environment?	9. What controls and measures are placed in the department to mitigate Cyber-attacks that exploit the human element?
ISO/IEC 27001 & ISO/IEC 27002 COBIT GTP only have a recovery plan for email, sure what the different departments have in place for their respective systems. For the transversal systems (BAS PERSAL and LOGS), SITA does have recovery systems in place and it is tested annually. ISO/IEC 27001 & ISO/IEC 27002 COBIT GTP only have a recovery / backup plan for email system groupwise. For the transversal systems (BAS PERSAL and LOGS), SITA does have recovery systems in place and it is tested annually.	Virus protection / Malware protection Patch management / Patch management Most departments firewalls has been removed due to it being old and outdated, so the only protection departments have is the anti-virus platform. However, some departments with adequate budget have implemented robust protection. I do however not have the details. Virus protection / Malware protection Patch management / Patch management Password policies / Risk Management Our firewalls are dysfunctional, so the only protection we have is our anti-virus platform. Firewall / Virus protection Patch management User access management / Password policies System Change Control / Risk Management Virus protection / Patch management / BC / DRP Project Management Not controlled. Only AV and WSUS Virus protection / Malware protection Risk Management / User awareness training We hope that our AV software will be sufficient Some attacks occur over the outdated Provincial Groupwise e-mail server Virus protection / Malware protection Patch management / Patch management User access management / Data encryption / Password policies System Change Control / Risk Management / Project Management User awareness training The department has an approved DRP (DRP tested bi-annually), however does not have a cybersecurity framework in place. The department has a cybersecurity framework in place. Risks are identified as to the framework.	User awareness training / Educational training In most departments, Cyber-security is just an addition to one of the technicians work. The province lacks people with relevant skills and expertise to do the work in the cyber-security environments. User awareness training / Educational training Cyber-security is just an addition to one of the technicians work. However, the person lacks skills as well as does not have the relevant qualifications. User awareness training / AWARENESS CAMPAIGNS User awareness training / Cybersecurity culture / Educational training The departmental teams role would be to remove/recovery from the threat. SITA identify infected nodes. GTP to prevent of another attack. User awareness training Department to identify risks and mitigate the risks. Departmental cybersecurity to be reported to the GTO Council. Provincial IT security team. SITA to provide solutions to mitigate cybersecurity. The problem SITA always wants to solve is to have a secure environment.

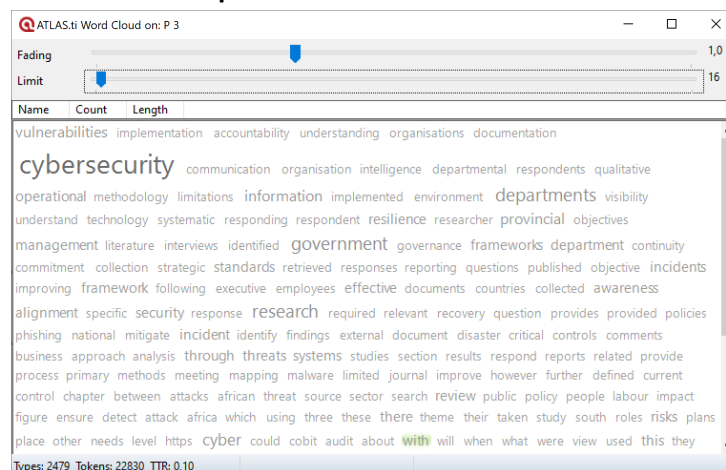
Source: Harris, 2020

The major themes revealed during the data analysis are linked back to the research conceptual framework and literature review. The process consisted of creating codes and categories, taking into account the themes, analysing the respondents' perceptions and experiences, and the existing literature review. Once the codes were added to the Atlas.ti project, the code was approached deductively and then linked to the data's important segments. As the data was coded deductively, the researcher had also come across new themes. Using the ATLAS.ti software, the code table was created within the "Code Manager" feature. A sample of the code table can be found below in table 7. The researcher used the code table to further review codes and determine how to develop the codes for analysis. Additionally, a detailed description was created for each of the codes, which ensured that the understanding of the code's purpose remained constant.

Table 7: Sample of Themes, Code Groups and Codes created.

<u>Questions (Q)</u>	<u>ANSWERS (A)</u>	<u>THEMES</u>	<u>CODE GROUPS</u>	<u>CODES</u>
What cybersecurity frameworks/standards are there in the department?	ISO/IEC 27001 & ISO/IEC 27002 COBIT	Frameworks Policies Standards Needs	Information Security Cybersecurity Frameworks	COBIT ISO 27001 ISO 27002 IEC 27001 IEC 27002 IASME Governance CIS COSA NIST Cybersecurity
What controls are in place to mitigate cybersecurity vulnerabilities in the environment?	Virus protection / Malware protection Patch management / DRP User access management/ Data encryption / Password policies System Change Control/ Risk Management / Project Management User awareness training	Controls Incidents vulnerabilities Responding	Protection Security Controls Risk Controls Encryption Mitigating controls	Virus Protection Anti-virus Malware Patch Management Disaster Recovery User access encryption Password policy Change Control Risk Awareness

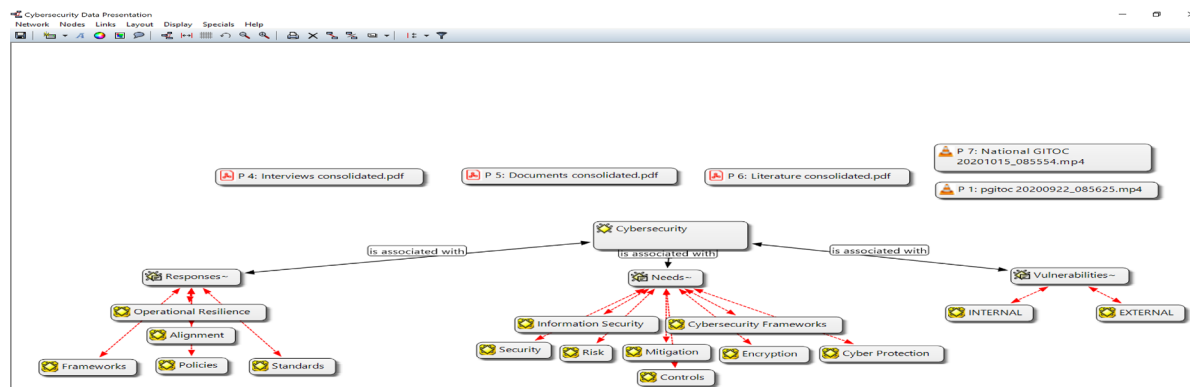
Figure 13: ATLAS.TI Word Cloud Sample



In analysing the primary data, all the interviews were digitally recorded, and their contents transcribed and analysed using the Atlas.ti version 7 qualitative research software. The consolidated interview transcripts, relevant consolidated documents and consolidated literature was converted from word or excel documents into a pdf so that Atlas.ti could import the data to be analysed. MS Teams video recordings were also included and imported into Atlas.ti to be analysed and notes linked to time-stamped captions.

Figure 14 presents how the data was imported to ATLAS.TI and how Atlas.ti created the possible connections (relations) between codes, themes and sub-themes. Family codes were generated and linked to the main themes. Codes are sub-categorised under the family codes.

Figure 14: Sample of ATLAS.TI Data Presentation



3.4.4.4 Inductive and deductive reasoning

Given this research's exploratory approach, an inductive reasoning approach was chosen. A representative of inductive research is that it is a theory-building approach that seeks to discover an understanding of the research study context. Data collection and analysis intends to explain patterns, facts, causes, and meanings in inductive reasoning (Hassad, 2020) rather than a deductive approach. The deductive approach using a hypothesis allows a causal understanding of the problem verified by testing. Researchers mainly use two types of analysis, quantitative and qualitative, when conducting research and gathering data; both methods are often seen as addressing the same question using different methods. The inductive reasoning approach ensures that the results are drawn based on discovering meanings instead of testing a hypothesis.

This approach to the research does not start with a hypothesis to test through deductive reasoning but instead creates a theory that can be used later in deductive reasoning-based research. This is an appropriate research method chosen for this research, given the limited research conducted in the provincial government on cybersecurity. Given the qualitative nature of the research, various vital terms, codes and phrases were extracted from the data. Semi-structured interviews (Hassad, 2020; Ravitch & Mittenfelner Carl, 2016) utilising inductive reasoning is adequate for small samples of interviewees to explore and gather data.

The researcher connected codes to create themes by constantly comparing one piece of data with another. Searching for patterns from the 'facts' or raw data allowed the researcher to find unanticipated themes and provided the capability to improve the data analysis during the coding process. Combining these approaches allowed the development of patterns from the unknown parts that may fall outside the predictive codes of deductive reasoning and allowed for a complete analysis. This step began with analysing prior codes, followed by a more inductive process of open coding. The overall step enabled the researcher to segment the data into small conceptual fragments and assigned data to categories and concepts. Inductive reasoning allowed the researcher to generalise the findings to all provincial government departments.

3.4.4.5 Synthesis

According to Rashid et al. (2019), when conducting a case study where evidence was gathered, one needs to systematically analyse and synthesise the data to allow ideas and patterns to emerge to build new theories or increase existing ones.

This process of combining the findings of multiple research studies to answer a question is often called 'synthesis.' Synthesis has been used to describe the process used to gather and collate evidence (ex:

systematic mapping) to answer a question. The data synthesis activity involves collating and summarising the data extracted from the research with the primary goal of understanding, analysing, and classifying the current research on cybersecurity. The researcher analysed the extracted data to find trends and collect information about each research question. Firstly, the researcher analysed each primary study individually to document it and tabulate its main features, then analysing the set of research as a whole to reason on potential patterns and trends.

After completing the data analysis, the researcher integrated the results in order to explain the qualitative results. In the following chapters, the results of the analysis of the extracted data will be presented. For the sake of clarity, the analysis results were organised according to the research questions. A notable finding from the synthesis is that there is scarce literature on cybersecurity in provincial government departments. The synthesis confirms that alignment is still young and not fully formed, and regulatory bodies have not focused enough to create alignment a priority in government. Chapter 6 provides a synthesis of the research findings to provide evidence of how the research aims have been fulfilled.

CHAPTER 4: INSIDE THE GOVERNMENT CYBERSECURITY LANDSCAPE

4.1 Introduction

This section presents in detail the findings of the research data collected in provincial government departments. The research methodology guide addresses the research objectives and determines if the objectives can be met. It introduces the research findings from the interviews and aims to contextualise cybersecurity in the provincial government. The data was collected by employing semi-structured interviews and document review as a primary collection instrument and the secondary source instrument systematic mapping to better understand the data limitations and gaps. It employs a qualitative content analysis of research findings directed by the research objectives:

Main research objective: To identify why and how provincial government departments can improve operational resilience through effective cybersecurity.

- Research objective (i): To identify the current cyber vulnerabilities of government information systems to external threats.
- Research objective (ii): To identify how provincial government departments currently respond to cybersecurity incidents.
- Research objective (iii): To identify the need for provincial government departments to mitigate cybersecurity vulnerabilities.

4.2 Primary data collection and analysis

Four themes emerged from the data, gathered through the interview guide and from the document review process, as presented below. The data collection through interviews and through document review yielded slightly different emphases, noting that the data from the two processes have now been integrated into the data presentation in the following sections.

Theme One: Current cyber vulnerabilities of government information systems to external threats

Theme Two: Identification of cybersecurity vulnerabilities in government departments

Theme Three: Needs with respect to improving operational resilience through effective cybersecurity

Theme Four: Government departments' responses to cybersecurity incidents

Primary data was gathered further using a document review guide prepared to obtain information about the research questions.

Theme One: Current cyber vulnerabilities of government information systems to external threats

Theme Two: Mitigation of cybersecurity vulnerabilities in government departments

Theme Three: Government departments' responses to cybersecurity incidents

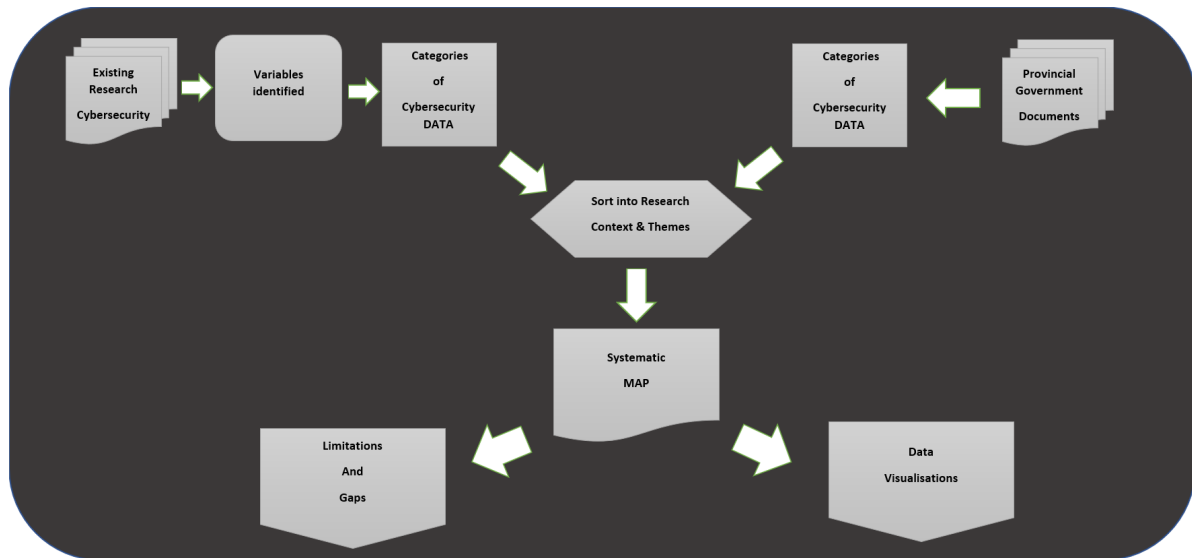
Theme Four: Improving operational resilience through effective cybersecurity

Data was extracted from the following documents, and the data extracted was then confirmed through a systematic mapping process as part of the secondary data collection:

- Departmental ICT frameworks / Cybersecurity frameworks / ICT security frameworks
- Departmental ICT policies relating to cybersecurity / ICT security

- Departmental IT strategic plans / IT plans
- Job descriptions of GITO's, IT Managers, ICT Specialists
- Auditor General and Internal Audit reports on ICT Security
- MPAT reports
- Departmental reports relating to IT Security and Cybersecurity

Diagram: Systematic mapping provincial government documents



Source: Harris, 2021

As cybersecurity is relatively new, the researcher chose to use existing research on cybersecurity to contribute to this study. Variables were identified, and abstract's of research papers were read looking for keywords and concepts. Categories were then identified that would contribute to the research paper. The provincial government documents were then examined against these defined categories (see a sample of data categories in the table 8 below). The data extracted were then sorted into the research themes and context, and a systematic map formulated. From the systematic map, limitations and gaps were identified and data visualisations formulated from the extracted data.

Table 8: Sample of data categories filtered to research theme - Vulnerabilities and threats

Research Type	Identified Categories from existing research	Electronic data sources	Number of relevant search results	Number of articles selected	Research Theme	Identified Categories from Provincial government documents	Research Type
Existing Research Cybersecurity	Web Vulnerabilities Malware Ransomware DDOS DOS Malicious URL SPAM Phishing SQL Injection attack Cross-Site Scripting Man in the middle attack Zero day exploit Cloud computing vulnerabilities Spear Phishing Insider Threats Scanning/Probing Remote Worker threats	Cambridge Sabinet Sage Science Direct Scientific Electronic Library Online (SciELO) SA	10 190 516 2303 6	2 13 6 9 6	Vulnerabilities & Threats	Malware Web Vulnerabilities Hackers Ransomware Social Engineering (phishing) Access Control Virus or Worm Trojan DoS Theft of devices	Provincial Government Documents

Categories from the existing research and categories from the provincial government documents allowed the researcher to identify gaps easily.

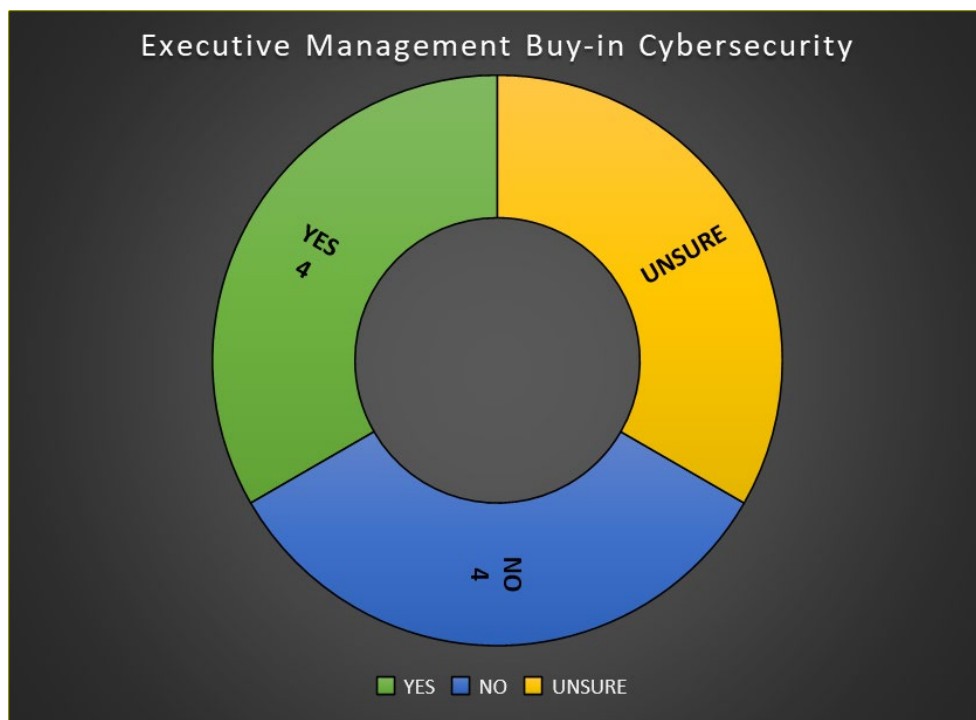
Data extracted and utilised in this chapter was found in the context of the larger systematic map of cyber vulnerabilities and presented as data visualisations. Unfortunately, the Auditor General's requested interviewees were not permitted to participate in the research; however, previous years departmental audit reports were available and provided by the premier's office.

Executive management buy-in and professional cybersecurity skills

The researcher sought to assess the respondent's opinion if executive management commits to the roles and relevant responsibilities to oversee the development and implementation of cybersecurity and security related matters. Following an assessment of executive management's commitment to cybersecurity, a holistic view of the respondent's accountability and limitations could be ascertained from the data.

Executive management has an understanding of the roles they need to play; however, there is very little to no commitment at all in the implementation of cybersecurity approaches (Respondent 10). In contrast, four of the fourteen respondents emphasise that executive management is fully committed and provides the resources for the implementation of cybersecurity and security related matters (Respondents 1, 2, 6 and 9). Four of the fourteen respondents argue that there is no commitment and the main focus of executive management is compliance due to the government being highly regulated and audited (Respondents 3, 4, 5 and 12).

Figure 15: Executive Management Buy-in



Source: Harris, 2021

To assess the respondent's position in the organisation, the respondent's experience in their current role, and how involved and responsible the respondent is for cybersecurity in their department, data

collected revealed that the respondent's accountability could be determined by the title or rank of the respondent. However, given the provincial government's nature, a clear separation of the respondent's roles was unfeasible because roles intertwined in some aspects of strategic and operational capabilities. Literature narrates the duplication or intertwinement of fields. The participants were mostly in senior or managerial positions in information communication technology (ICT) with ICT security responsibilities. Most of the respondents felt they have dual or triple roles, focusing on various aspects of Information Communication Technology. To acknowledge these variations of roles, two of the fourteen respondents focused on everything that is related to Information Technology across provincial government, from governance, strategy to operational and security (respondents 1 and 2).

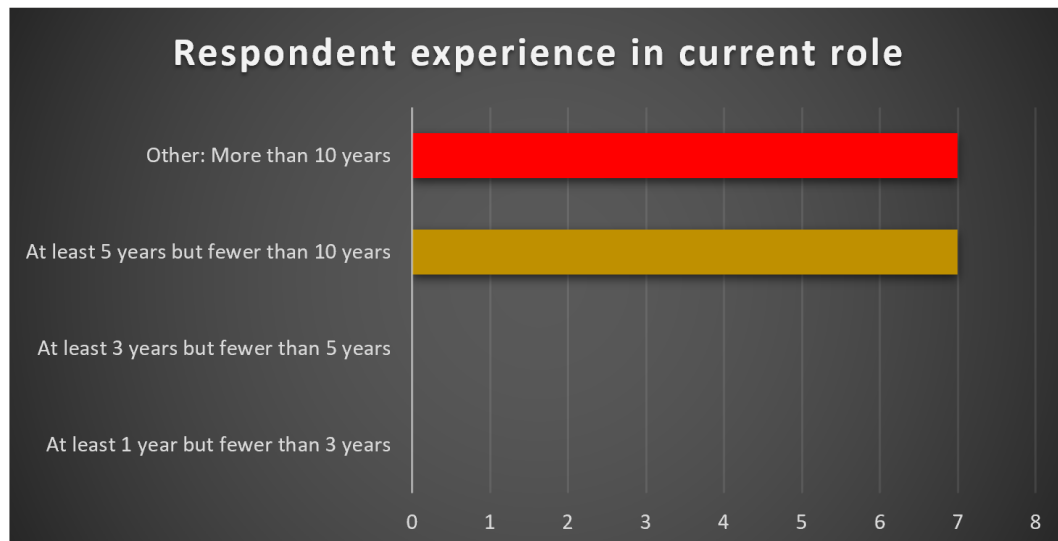
4.2 Digital and cybersecurity skills of the provincial government

In the departments of the provincial government, the GITO's, IT/ICT manager and security specialist are responsible for various roles across the organisation. Likewise, seven of the fourteen respondents agree and stresses a similar view.

"Their role titles do not necessarily reflect what they do, and often they also go around fixing things (operational)" (respondents 3, 4, 5, 6, 7, 8 and 12).

Respondents were further requested to disclose their experience in their current roles at the departments as part of the interview. The data in Figure 16 shows that the provincial government have experienced and expertise individuals (respondents 1 to 14).

Figure 16: Respondents Experience



Source: Harris, 2021

However, detail of their experience and qualifications was not included in the research. Respondent experience when it comes to cybersecurity paints a different picture; four of the fourteen respondents describe cybersecurity implementation as basic or minimal in their respective departments (respondents 1, 2, 7, 8, and 9):

"We have a Provincial Policy with Cyber related policy directives, albeit serious lack of provincial implementation."

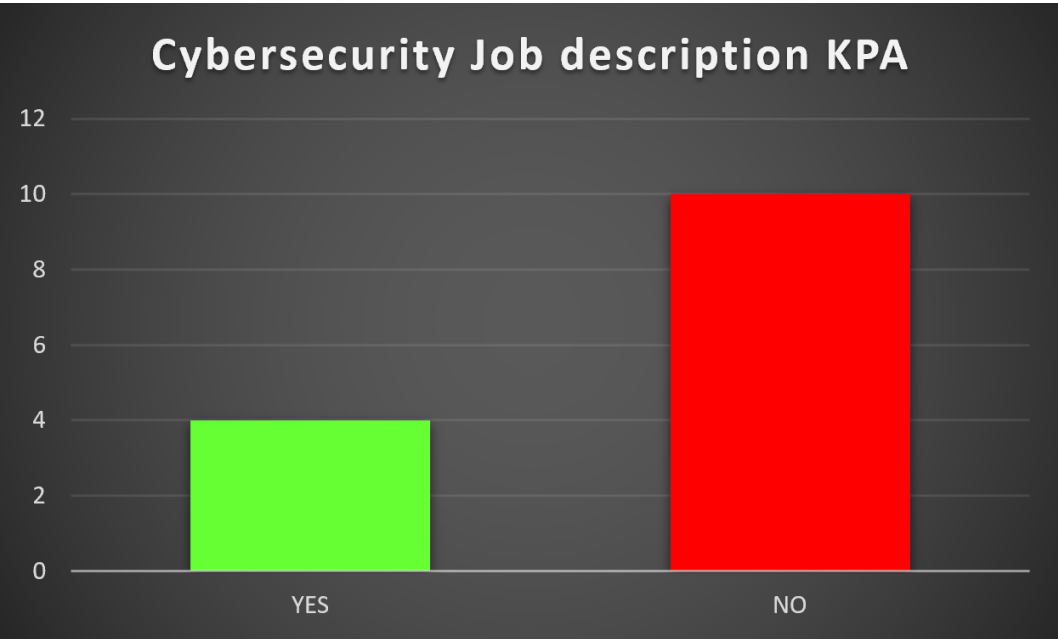
"There is very limited interaction with cybersecurity. Scenarios where cybersecurity incidents took place in the past, were discussed, such as the hack of the departmental website that took place..."

Some respondents support the consensus that cybersecurity is not implemented in their departments (respondents 3, 4, 5 and 13). However, one respondent exemplifies another side of the experience on cybersecurity:

"Policies and frameworks were developed suited to the environment of the department, with limited resources available. A cybersecurity program has been running for the past three years, and IT security has been implemented for longer than ten years" (respondent 6).

Data collected from the organisation and Interviewees profiling essentially define the respondent's accountability and limitations. Cybersecurity, as a key performance area stipulated in their job description, enforces accountability and reporting. The data presented in figure 17 presents only four of the respondents, including one respondent from an external organisation, who have included cybersecurity as a Key Performance Area in their job descriptions (respondents 3, 6, 12 and 14). This leads to the conclusion that there is low accountability and reporting when it comes to cybersecurity. Accountability instils transparency, trustworthiness, reliability and justice (Ince, 2018).

Figure 17: Cybersecurity Key Performance



Source: Harris, 2021

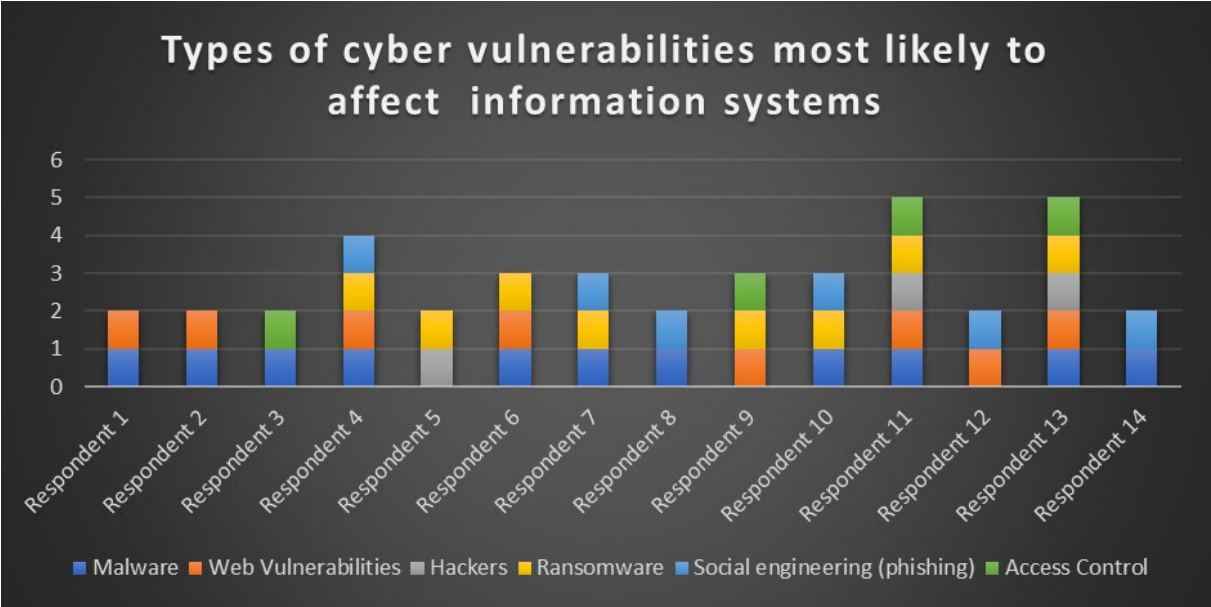
4.3 Government perception of cybersecurity vulnerabilities

This section seeks to determine the provincial government's vulnerabilities in cybersecurity. Aiming to establish the current external threats and cyber vulnerabilities to government information systems from data collected in the interviews and documents provided by the premier's departments and office. Clear from the data and a systematic mapping to link keywords such as malware, web vulnerabilities, hackers, ransomware, phishing and access control, the following cyber vulnerabilities that are most likely to affect the government information systems were identified. The participants' thoughts, ideas, and perceptions are the primary data of qualitative research, and respondents' responses do not necessarily provide a view of the reality in the provincial departments. Berg (2007) argues that a particular strength of this type of research is that participants may develop ideas, bring forward their own priorities and perspectives, and create theory grounded in the actual experience. The provincial government participants perception is based significantly on the daily and weekly alerts sent to cybersecurity professionals in the government departments by the Cybersecurity hub and their actual experience in their respective departments (respondents 1 to 14).

The participant's perception can indicate weaknesses in the research data as the participants believe they have a favourable perception of their current cybersecurity and their skills in this area. Lack of knowledge about cybersecurity and their perceptions practices allows for incorrect cyber vulnerabilities and threats to be identified and does not provide the reality of cybersecurity in the provincial government. Relying on entities such as the Cybersecurity hub and SITA can leave insider threats as unidentified or low-risk. Insiders have the knowledge of the internal workings of the government department and all the rights and privileges required to mount a cyber-attack that outsiders lack. Consequently, insiders can make their attacks look like normal operations.

The top three cyber vulnerabilities perceived most likely to affect government information systems were identified as malware, ransomware and web vulnerabilities. Eleven of the fourteen respondents' documents view malware as the highest cyber vulnerability, with ransomware and web vulnerabilities in second, with eight out of fourteen respondents' documents highlighting them. As illustrated in figure 18, malware is indicated as a vulnerability to most departments for information systems (respondents 1 to 14). Other information system vulnerabilities that the departments are facing are hackers, phishing and access control.

Figure 18: Types of cyber vulnerabilities most likely to affect information systems



Source: Harris, 2021

Data extracted from the respondent's documents revealed that the top cyber threats and risks documented by the departments were captured in a table to generate descriptive statistics. Using a screening process using inclusion and exclusion criteria and then searching for keywords, the respondent's documents that included the keywords were assigned a value of one. Six threats and vulnerabilities were identified that affect the departments. Table 9 shows the occurrence in each of the respondent's documents (respondents 1 to 14). Denial of services, trojans, ransomware, and devices' theft is considered low risk, phishing or malicious email medium risk and virus or worms as high risk.

Table 9: Top three cyber risks from relevant documents

	Top three cyber risks (threats and vulnerabilities) the relevant documents reveal					
	Virus or Worm	Theft of Devices	Phishing or Malicious emails	Ransomware	Trojan	Denial of services
Respondent 1	1	1	1	1		
Respondent 2	1	1	1	1		
Respondent 3		1	1	1		
Respondent 4	1	1	1	1	1	1
Respondent 5	1			1	1	1
Respondent 6	1		1	1		1
Respondent 7	1		1	1		
Respondent 8	1		1	1		
Respondent 9			1	1		
Respondent 10	1			1	1	
Respondent 11	1	1				1
Respondent 12			1	1	1	
Respondent 13	1	1		1		1
Respondent 14	1					
	11	6	9	9	5	4

Figure 19 highlights the top three risks identified and reported in the department's risks registers. Eleven of the fourteen respondents' extracted data show virus or worms as the top threat or vulnerability and phishing or malicious emails as the second, and theft of devices as the third and have been identified as risks.

Comparing to the data analysed in table 9, it is observed that two of the top three cyber risks correspond. Virus/worms and phishing/malicious emails recorded as high-risk and theft of devices as low risk to the departments (respondents 1 to 14).

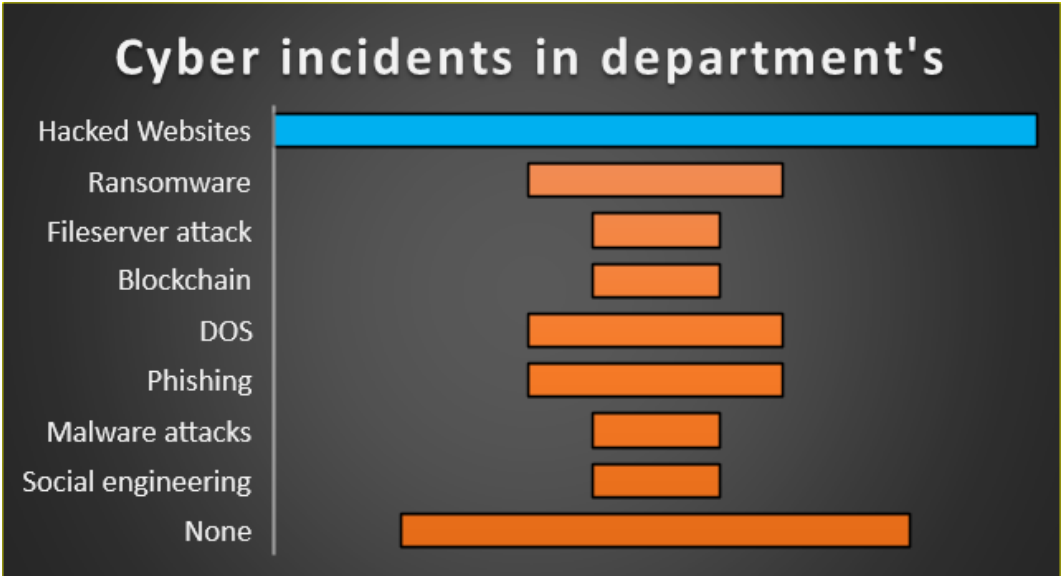
Figure 19: Top three cyber risks



Source: Harris, 2021

To verify the data extracted above, cyber incidents recorded in the departments that have taken place and the type of incident that took place was analysed. From the interview data, it was noted that the top cyber incident taken place at the provincial government departments is that the departmental websites had been hacked. Respondents stipulated the occurrence had taken place and at some departments more than once (respondent 1, 2, 5, 6, 9 and 11).

Figure 20: Department Cyber incidents environment



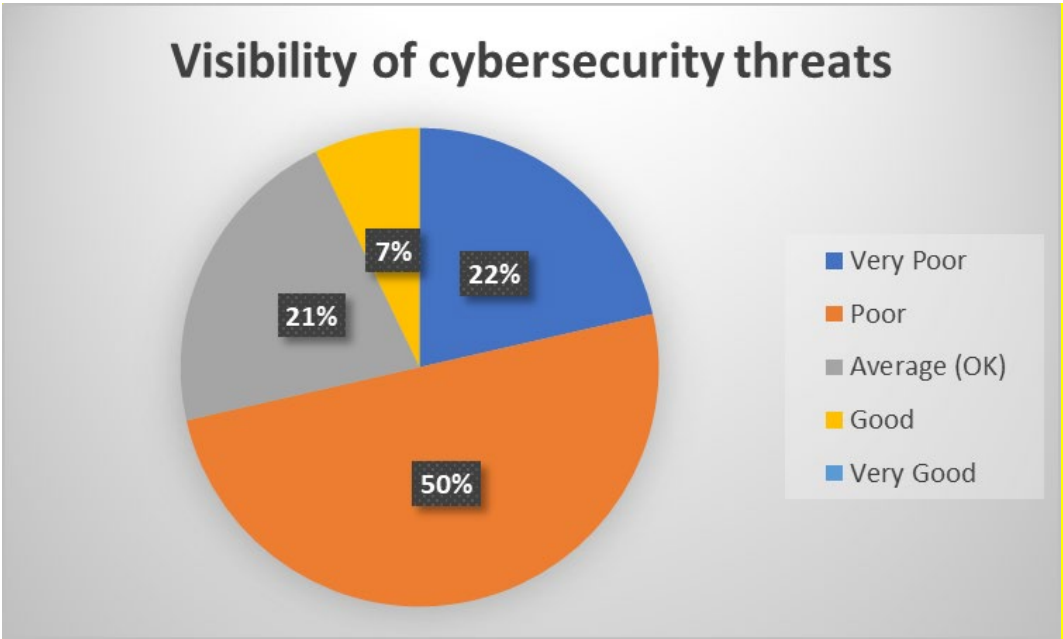
Source: Harris, 2021

Four of the fourteen respondents reported that there was no cyber incident at their department and could not confirm or deny if incidents could have taken place as they were unaware of them. The visibility of the vulnerabilities was analysed from the data collected to confirm some departments' validity having no cyber incidents reported (respondents 1 to 14).

“I need to be able to deal with bigger issues in the department and do not have the time to monitor cybersecurity incidents” (respondent 7).

The frequency of words identifying cybersecurity threats in the documents was determined to rate the level of visibility of cybersecurity threats. Using a scale from very poor to very good, respondents' documents can be analysed. Fifty percent of the respondent's documents revealed poor visibility for cybersecurity threats. Only one department's documents provided good visibility. Poor control measures and reporting demonstrate low governance maturity and create a barrier to identifying and mitigating cybersecurity vulnerabilities and threats. Diesch, Pfaff and Krcmar (2020) express that cybersecurity threats' visibility is very significant to mitigate cybersecurity risks.

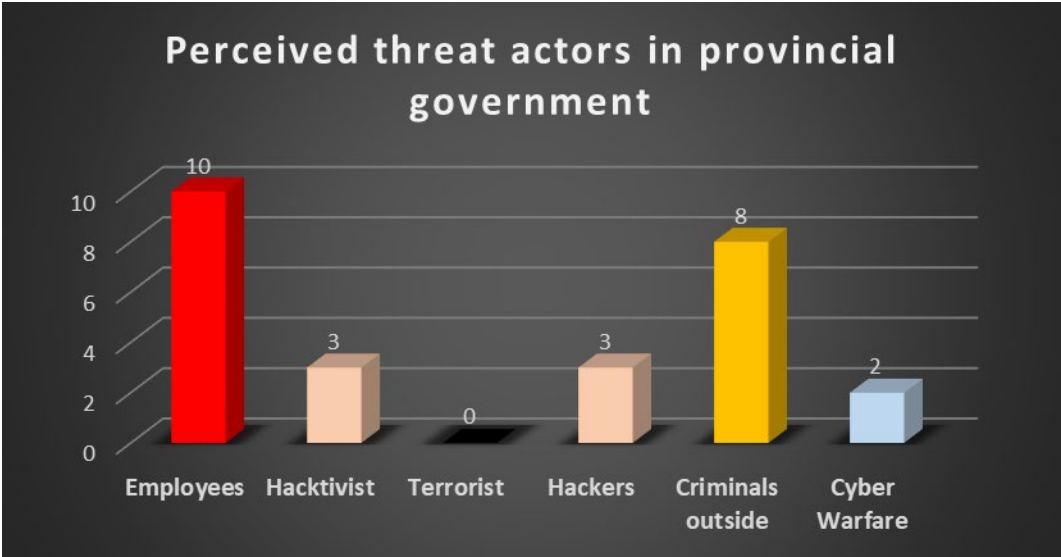
Figure 21: Visibility of cybersecurity threats



Source: Harris, 2021

The following threat actors were identified from the documentation. Regarding the top threat actors in departments, employees (internal) were indicated as the biggest threat for ten out of fourteen respondents' documentation (respondents 1 to 14). Secondly are criminals outside for eight out of fourteen respondents and then followed by hacktivist and hackers and then cyber warfare in the last place. See figure 22 below.

Figure 22: Perceived threat actors in the provincial government



Source: Harris, 2021

4.4 Improving operational resilience through effective cybersecurity

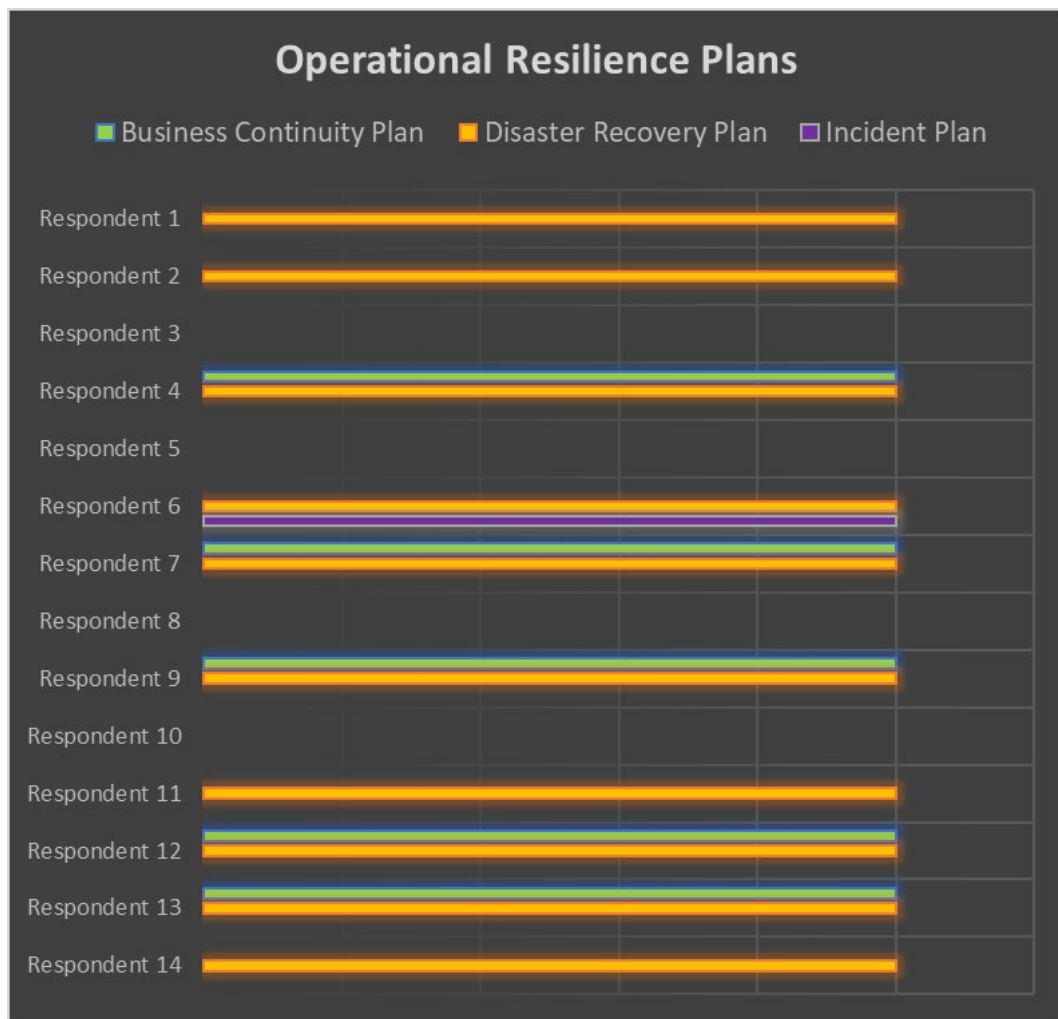
This section aims to appraise how the respondents in their department’s implement operational resilience and the significance of cyber awareness. Operational resilience requires that the appropriate activities and plans need to be implemented in the department's environment. Analysing the data assesses whether the department has or needs to implement a business continuity plan, disaster recovery plan and an incident recovery plan to ensure operational resilience. A Cybersecurity recovery plan incorporates these three plans and provides the department with the ability to timely restore systems to normal operations and an acceptable level.

The respondent's responses and document review are of great concern, as not a single respondent has identified that they have all the plans for a cybersecurity recovery plan (respondents 1 to 14). From the data in Figure 23, it is apparent that there is a need for these plans; Alignment can only be observed once these plans have been implemented or developed. Some of the respondent’s stated they have a business continuity plan or disaster recovery plan, however they believe the plans are not suitable and are unsure of the effectiveness of the plans or whether in the event that a recovery is entirely possible.

“In the process of review of BCP and DRP, the major problem resides with the institutional frameworks not being in place, for the transversal systems (BAS PERSAL and LOGIS), SITA does have recovery systems in place, and it is tested bi-annually” (respondent 12).

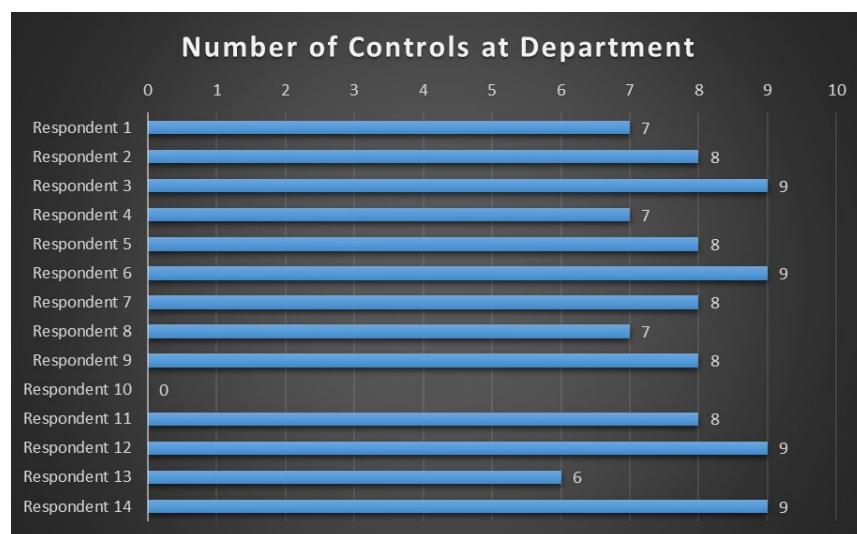
A cybersecurity recovery plan that incorporates business continuity, disaster recovery and incident is imperative for operational resilience in the organisation (NIST, 2018).

Figure 23: Operational resilience plans



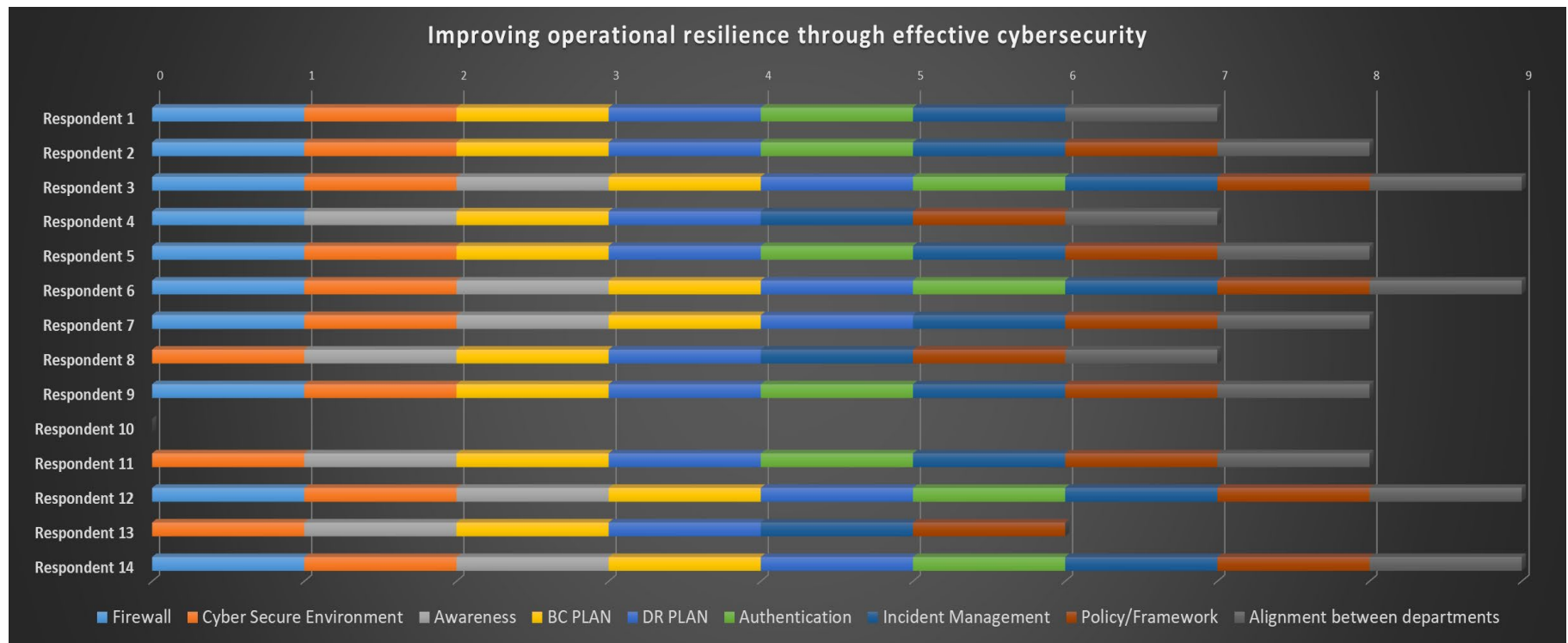
Source: Harris, 2021

Figure 24: Number of controls identified



Source: Harris, 2021

Figure 25: Improving operational resilience through effective cybersecurity

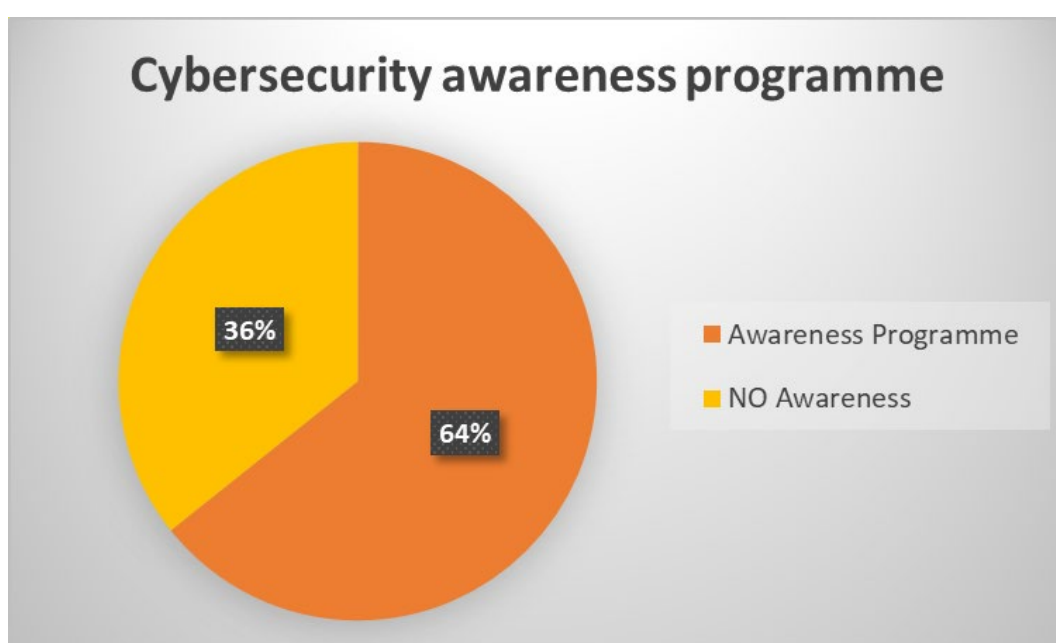


Source: Harris, 2021

The above findings in figure 25 suggest the respondent's view of what they consider to be required for operational resilience through effective cybersecurity (respondents 1 to 14). Overall, these results indicate that the departments have implemented cybersecurity for operational resilience; however, what is concerning is that cybersecurity awareness has been identified as important by only nine respondents out of the fourteen. Figure 25 indicates what the respondents believe improves operational resilience as the top 9 are identified. Figure 25 clearly allows you to identify what each respondent department has in place or easily does not have for operational resilience through cybersecurity. There is a clear misalignment in identified controls to mitigate risks to improve operational resilience through cybersecurity. The bottom three findings identified are awareness, authentication and firewalls. Mbanaso, Abrahams and Apene (2019) research further support cybersecurity standards, awareness and alignment to promote the mitigation of potential inside and outside vulnerabilities or attacks for effective operational resilience.

Effective operational resilience begins with a cybersecurity awareness programme, and cybersecurity awareness can make employees aware of cybersecurity risks. From the data, we can deduce if the respondents have a cybersecurity awareness programme in their departments.

Figure 26: Cybersecurity awareness programme



Source: Harris, 2021

Most of the respondent's responded that cybersecurity awareness is implemented in their departments. The respondent's that reported that there was no cybersecurity awareness in the departments commented the following below:

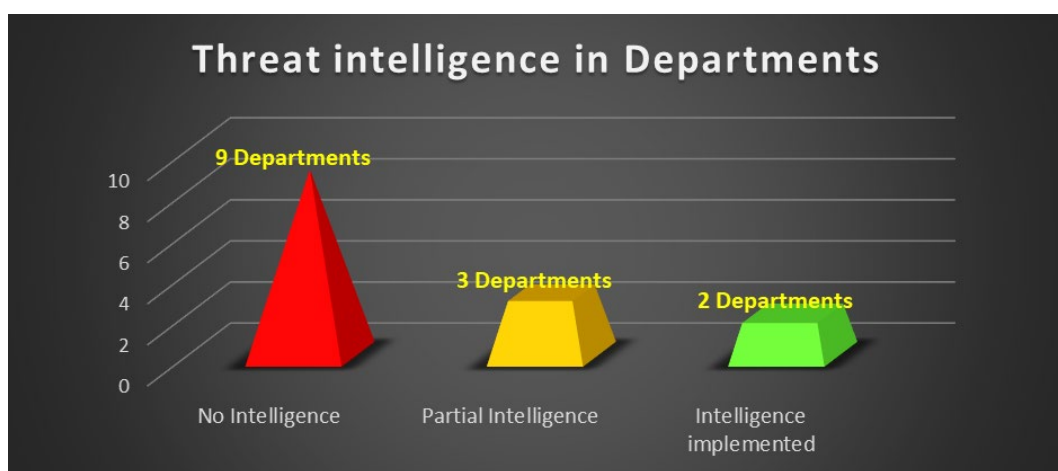
"The department does not have any such programs. Awareness is more aimed at managing disaster recovery with little emphasis on cybersecurity. Cybersecurity is currently seen as the responsibility of National and SITA "(respondent 9).

"No, our employees are not well informed. Seminars attendance is extremely low regarding policies and procedures" (respondent 7).

Awareness training and including employees in securing activities are essential for building a cybersecurity culture (Tambo & Adama, 2017; Craig, 2018).

Aiming to establish whether operational resilience in departments can or is improved by implementing effective cybersecurity and whether there is any alignment from the data collected. Key to cybersecurity is conducting cyber threat intelligence to identify, detect, and respond to cyber threats. Through a systematic mapping and data collection from the documents provided, figure 27 reports that nine of the fourteen respondents departments do not have any cyber threat intelligence in their respected departments (respondents 1 to 14). Cyber threat intelligence is of great importance to identify specific threats and can improve the understanding of cyber incidents targeting the government (Fachkha, 2015).

Figure 27: Threat intelligence in departments



Source: Harris, 2021

From the data collected and analysed, the respondents have a diverse view of understanding strategic alignment (respondents 1 to 14). The respondent's documents expressed strategic alignment as the need for all actors to be on the same page. From the data extracted, the data can be interpreted and presented as the following extractions from the respondent's documentation:

Strategic alignment is a golden thread, and all actors need to be on the same page. Business, Risk, HR, Finance, IT, Governance and the units implementing the departmental mandates all need to understand the importance of each other's role and responsibility (respondent 1 and 2).

Strategic alignment ensures that units priorities and employees are aligned to the department's priorities, a clear vision as to where and how to achieve department business initiatives (respondent 3 and 6).

Respondent 4 documentation states that alignment is the responsibility of senior management to ensure the unit's priorities are aligned.

Strategic alignment is very important and should be driven by the ICT Steering committee and Executive Management Committee (respondent 7).

IT strategic alignment is where the department's ICT objectives align with the department's strategic objectives to ensure that the objectives are achieved. It aims to ensure that cybersecurity

is an enabler and assistor to ensure the achievement of objectives. The strategic alignment is the responsibility of senior management and specifically the person charged with ICT (respondent 10).

Six of the fourteen respondents' documents provide a clear view of how the respondents department views strategic alignment. The other eight respondent's documentation view on strategic alignment data could not be extracted. Alignment is necessary to bring about risk management, effectiveness, resilience, mitigation and compliance (Bohnert, Gatzert, Hoyt, & Lechner, 2019).

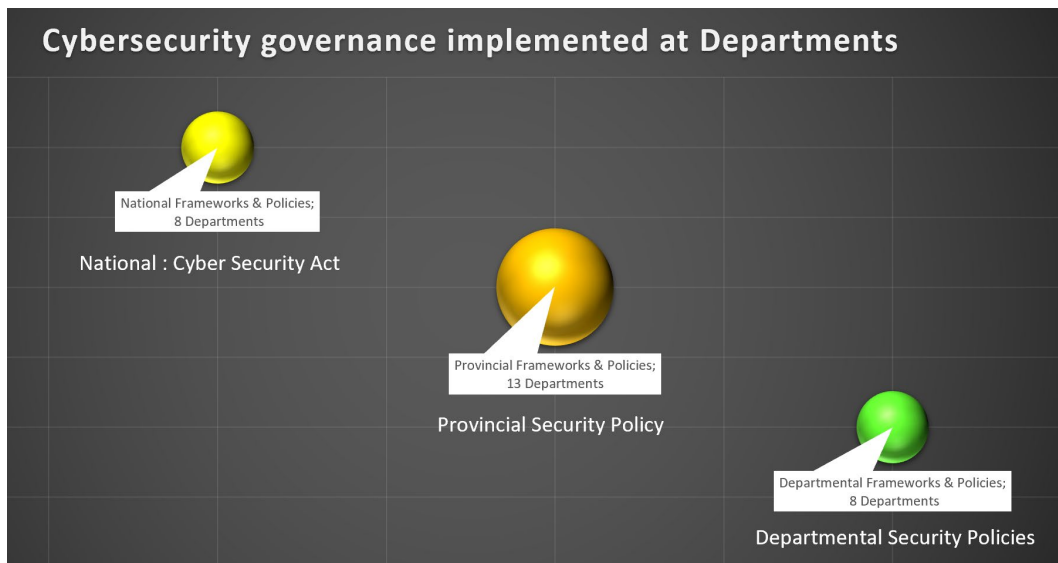
4.5 Mitigating cybersecurity vulnerabilities

We can deduce what cybersecurity governance is implemented in the departments to mitigate cybersecurity risks from the data extracted (respondents 1 to 14). Considering the broad spectrum of cybersecurity risks and cyber threats, respondents were asked about their department's position in mitigating cybersecurity risks. This allowed the researcher to comprehend what the respondents view as mitigation and what they view as cybersecurity risks. The purpose is to identify the respondent's opinion based on observation and experience to manage cybersecurity risk or cybersecurity incidents at a departmental or organisational level. Risk ownership is a critical aspect that enforces accountability (Lees, Crawford, & Jansen, 2018). Respondents have provided their views under the following three aspects:

1. Five of the fourteen respondents reported that cybersecurity is outsourced to the department's external entities such as SAPS cyber unit, SITA and external suppliers to provide a SOC solution for their department. There is no departmental preparation against cybersecurity risks. Five respondents believe that cybersecurity risk and preparedness are the responsibility of entities not residing in their departments (respondent 1, 2, 5, 10 and 12). This explains why there are gaps in the organisation regarding cybersecurity and cybersecurity risks, thus creating a bridge between departments and alignment.
2. Three respondents consider cybersecurity preparations as having an updated antivirus solution, desktop firewalls, and patch management. The disaster recovery plan's successful testing verifies that the department is prepared for cybersecurity risks (Respondents 4, 8 and 9).
3. Four of the fourteen respondents believe cybersecurity needs to be managed via a policy and framework that highlights cybersecurity as incident management, information security and security risk management linked to risk such as the NIST Cybersecurity framework (respondent 3, 6, 7 and 11). Departmental and organisational wide preparedness linked to risks identified.

From the data extracted, the researcher tried to establish if departments have implemented cybersecurity governance in their departments and at what level is the governance implemented (respondents 1 to 14). Aligning cybersecurity governance in the departments will help the provincial government manage their information systems and critical data so they can continue to be secured. They are illustrated in figure 28 below.

Figure 28: Cybersecurity governance implemented at departments



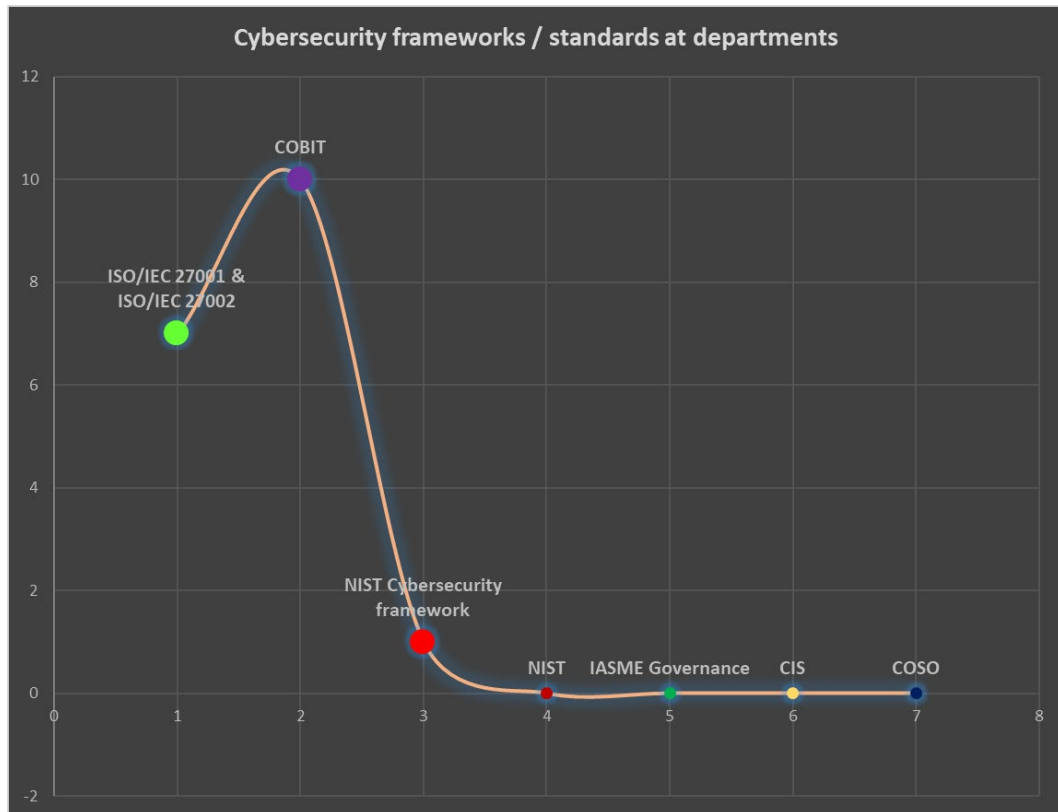
Source: Harris, 2021

Thirteen out of fourteen respondents' documentation presents that the provincial security policy is adopted in their departments; only eight of the fourteen departments have documented departmental security policies (respondents 1 to 14).

There is a concern that only eight of the respondent's documentation mentioned the national cybersecurity policy framework; this can imply an alignment issue between these frameworks and policies.

Through a systematic mapping process of cybersecurity frameworks and standards, the following frameworks/standards have been implemented in departments. Figure 29 presents the most common frameworks implemented in the departments is COBIT, and ISO/IEC 27001 and ISO/IEC 27002 follows closely in second. Only one respondent's documents mention the NIST Cybersecurity framework. Effective cybersecurity requires departments to be assessed against international standards, frameworks, methodologies and other best practices such as the NIST Cybersecurity framework. Such frameworks can assist in improving cyber risk and cybersecurity resilience. Government departments are not specifically assessing against the NIST Cybersecurity framework but against a combination of frameworks such as the ISO 27000 family and COBIT.

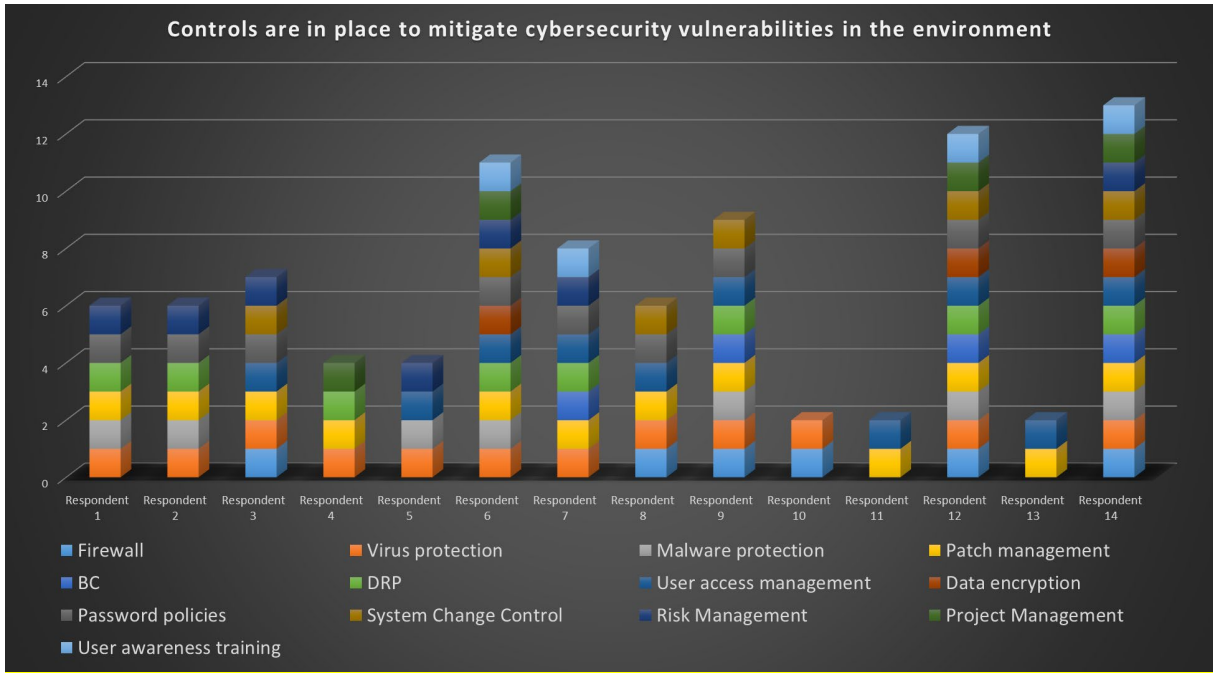
Figure 29: Cybersecurity frameworks/standards at departments



Source: Harris, 2021

Figure 30 shows the controls to mitigate cybersecurity vulnerabilities in the provincial government environment from the combination of data sources. In figure 23 the data presented a view that departments have aspects of BC, DRP and Incident management. Figure 30, taking a detailed approach of the data presented provides a different view and further supports the conclusion there is a need for business continuity, disaster recovery and incident management. Further both malware protection and user awareness controls scored in the bottom four, and this further supports data from the document review and interviews. A cybersecurity recovery plan incorporates the business continuity plan, disaster recovery plan and incident plan. From the data extracted from the document review and systematic mapping, this conclusion is verified as business continuity and disaster recovery plan both score in the bottom four lowest controls in place.

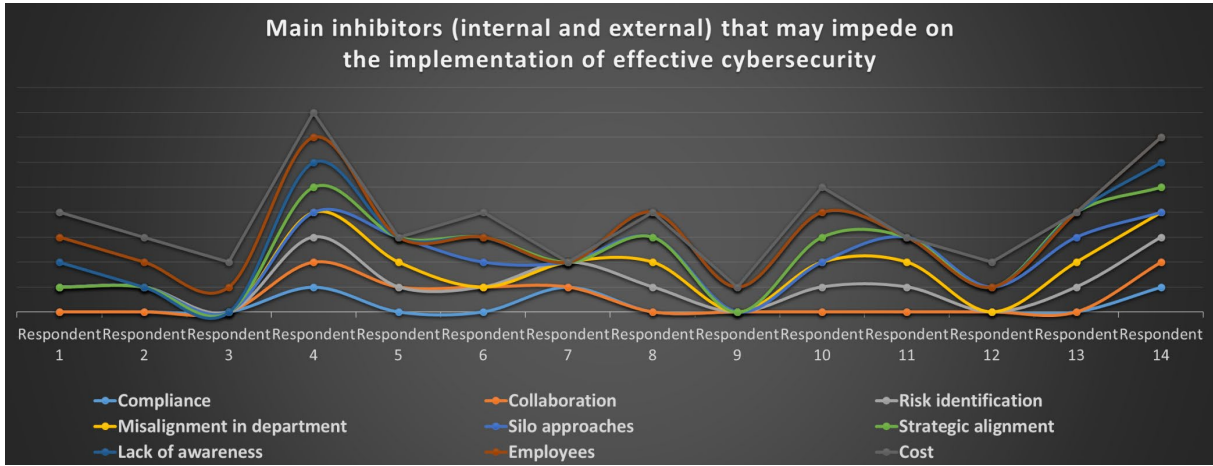
Figure 30: Controls are in place to mitigate cybersecurity vulnerabilities in the environment



Source: Harris, 2021

The main inhibitors (internal and external) that might impede effective cybersecurity implementation from the data revealed some challenges in government departments to implement effective cybersecurity. Challenges mentioned in the documentation, primarily reports from the internal audit and the Auditor General, have been identified in figure 31 below.

Figure 31: Main inhibitors that may impede on the implementation of effective cybersecurity



Source: Harris, 2021

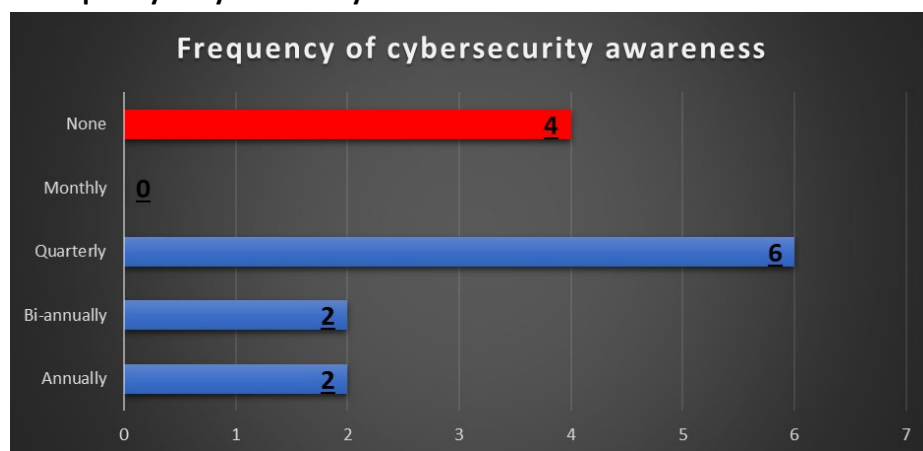
In figure 31, the diagram represents what inhibitors (internal and external) may impede the government department. The respondents identified the inhibitors they believe in impeding effective cybersecurity implementation (respondents 1 to 14). In the diagram, respondent 4 identifies eight of the nine main inhibitors that affect the respondent's department. Compliance was identified as one of the main inhibitors by the respondents. Many departments perform cybersecurity awareness only

because the auditor general requests a report on what awareness the departments have completed for the financial year. As a result, employees are reluctant to attend cybersecurity awareness.

The top three inhibitors identified are identifying cybersecurity risks, misalignment between departments, and lack of cybersecurity awareness. The top three inhibitors are fully supported in the previous data collected; these barriers need to be overcome to implement effective cybersecurity. Departments are obligated to provide ICT security awareness, ICT security awareness or cybersecurity awareness gets audited by internal audit and the Auditor General. The data extracted from the documents and interviews show that cybersecurity awareness needs to occur quarterly and reported in departmental ICT status reports the frequency and attendance of these awareness sessions. The data extracted only eleven out of fourteen respondents' documentation reports on ICT security awareness or cybersecurity awareness.

As discussed previously, cybersecurity awareness is documented and the frequency of the awareness was collected and reported in figure 32 below. The data revealed that six respondents provide cybersecurity awareness quarterly, two bi-annually and two annually. Four of the respondent's documentation made no mention of the frequency of cybersecurity awareness in their departments. The result shows that staff awareness is insufficient in relation to cybersecurity, and cybersecurity awareness is a challenge for some departments.

Figure 32: Frequency of cybersecurity awareness



Source: Harris, 2021

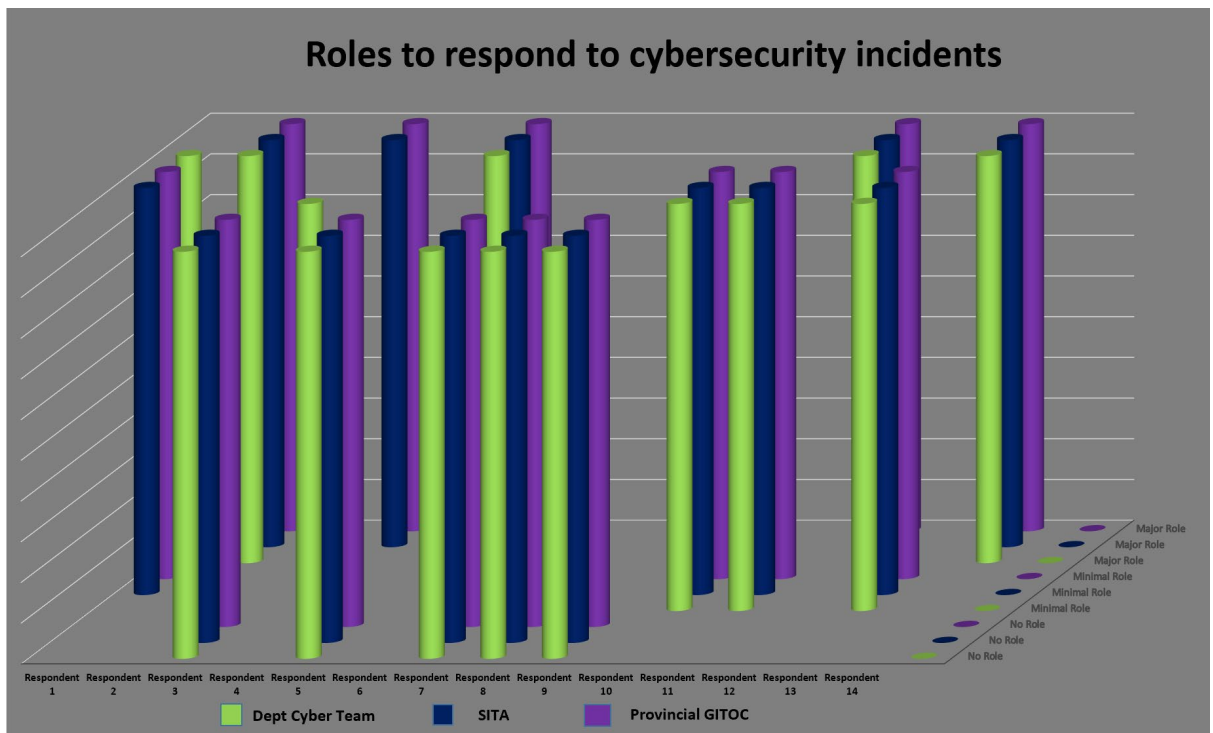
4.6 Government responding to Cybersecurity

Seeking to determine how the departments respond to cybersecurity incidents and the departmental cybersecurity team's role, SITA and the GITO Council in responding to cybersecurity incidents. From the data, the researcher can determine who in the provincial government is responsible for responding to cybersecurity incidents and if cybersecurity incidents get responded to at a departmental level, or organisational/provincial level or by external entities such as SITA. In figure 33, five of the fourteen respondents believe there is no role (respondent 3, 5, 7, 8 and 9). This supports the data collected in the interviews that there is no accountability when it comes to cybersecurity and executive management buy-in is essential for cybersecurity. Four of the fourteen

respondents believe the department, province and SITA play a significant role, and alignment is key to respond to cybersecurity incidents (respondents 2, 4, 6 and 12).

“Department to identify risks and mitigate the risks. Departmental cybersecurity to be reported to the GITO Council and provincial IT security team. SITA to provide solutions to mitigate cybersecurity” (respondent 6).

Figure 33: Roles to respond to cybersecurity incidents



Source: Harris, 2021

Table 10: Roles to respond to cybersecurity incidents

	Respondent 1	Respondent 2	Respondent 3	Respondent 4	Respondent 5	Respondent 6	Respondent 7	Respondent 8	Respondent 9	Respondent 10	Respondent 11	Respondent 12	Respondent 13	Respondent 14
No Role			Dept Cyber Team		Dept Cyber Team		Dept Cyber Team	Dept Cyber Team	Dept Cyber Team					No Role
No Role			SITA		SITA		SITA	SITA	SITA					No Role
No Role			GITOC		GITOC		GITOC	GITOC	GITOC					No Role
Minimal Role			Dept Cyber Team							Dept Cyber Team	Dept Cyber Team		Dept Cyber Team	Minimal Role
Minimal Role	SITA									SITA	SITA		SITA	Minimal Role
Minimal Role	GITOC									GITOC	GITOC		GITOC	Minimal Role
Major Role	Dept Cyber Team	Dept Cyber Team			Dept Cyber Team							Dept Cyber Team		Dept Cyber Team
Major Role		SITA		SITA	SITA							SITA		SITA
Major Role		GITOC		GITOC	GITOC							GITOC		GITOC
	Respondent 1	Respondent 2	Respondent 3	Respondent 4	Respondent 5	Respondent 6	Respondent 7	Respondent 8	Respondent 9	Respondent 10	Respondent 11	Respondent 12	Respondent 13	Respondent 14

Source: Harris, 2021

Critical to responding is to assess if the departments mitigate cyber risk and respond to cybersecurity incidents or use other role players. Just over a third of the respondents responded that their department identifies, controls and mitigates cybersecurity risks. Nine of the fourteen departments do not mitigate cybersecurity risks, and this data can be linked to the respondent's accountability and limitations. The conclusion is that there is low accountability and reporting when it comes to cybersecurity in the departments.

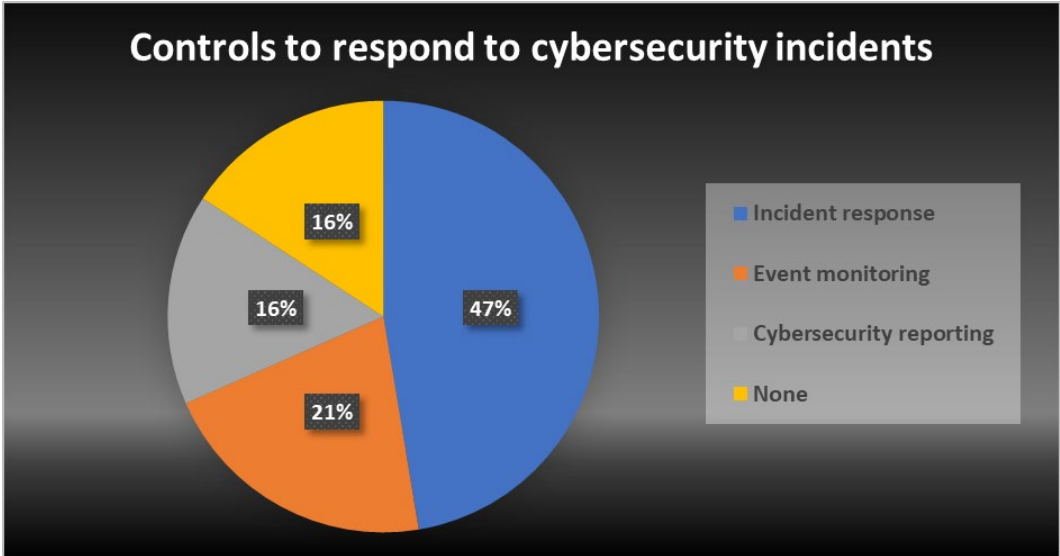
Figure 34: Cybersecurity Responses



Source: Harris, 2021

Aiming to establish how the departments detect and respond to cybersecurity incidents, the data shows whether the departments monitor, respond, and report cyber incidents. In Figure 35, three of the fourteen respondents' documents did not provide any data and were recorded as none (respondents 1, 9 and 10). Both event monitoring and cybersecurity reporting were identified as low, and nine respondents recorded only incident response in their documentation out of fourteen.

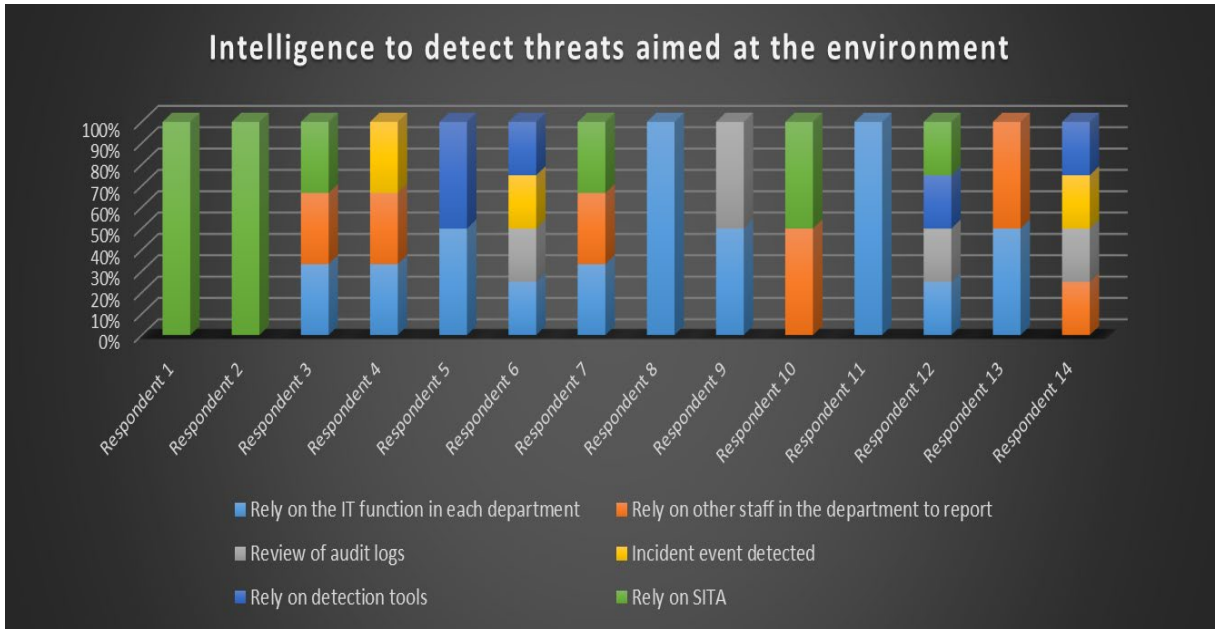
Figure 35: Controls to respond to cybersecurity incidents



Source: Harris, 2021

From the data collected and analysed, the following themes were identified to detect threats in the departments: (1) Rely on the IT function in each department, (2) rely on other staff in the department to report, (3) reviewing of audit logs in departmental information and security systems, (4) incidents that have occurred in the department environment (departmental website offline to website hacked), (5) tools implemented in the department to detect cyber threats and to (6) rely on SITA to protect departments from cyber threats.

Figure 36: Intelligence to detect threats aimed at the environment



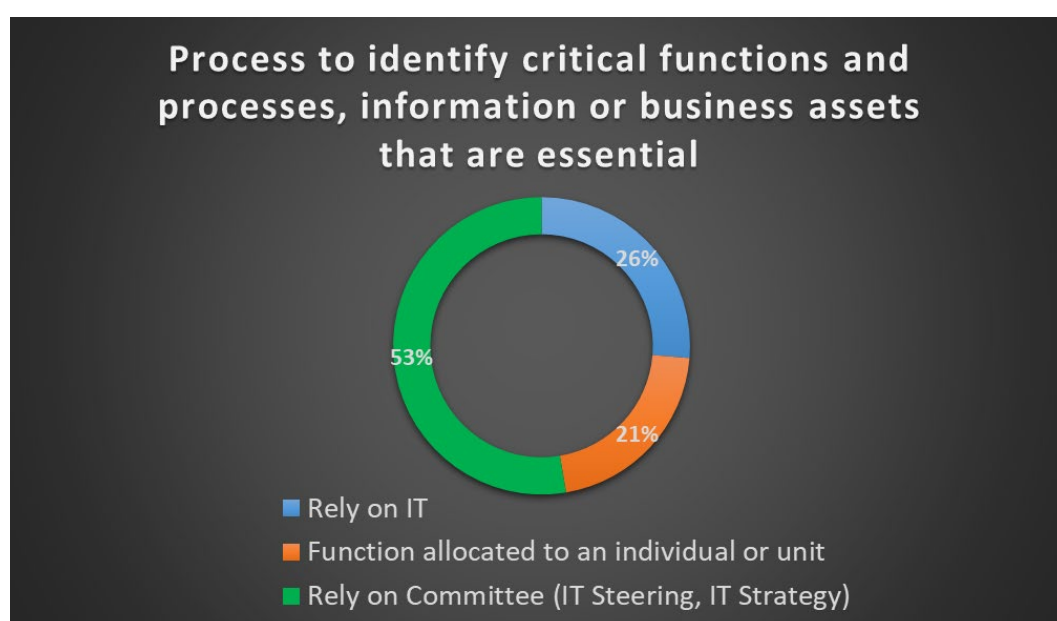
Source: Harris, 2021

Figure 36 data displays six of the fourteen respondents who rely on SITA. In contrast, ten of the fourteen respondents rely on IT in their respective departments and six of the fourteen respondents

rely on the departmental staff to detect threats. These three themes scored the highest and are ranked as the top three intelligence to detect threats in departments. A concern is that departments purely rely on the Information Technology unit in the fight against cybersecurity threats.

Data presented in figure 37 further supports the data that departments rely on IT and rely on the departments' IT governance committees. Departmental IT governance committees as to CGICTP framework incorporates both IT and management in the department and includes representatives such a risk. However, identifying critical functions (process, information and business assets) is the responsibility of a number of business functions in the department, such as risk or business continuity. In addition, the respondent's documentation reference to essential assets relates to information and technology, not people and facilities.

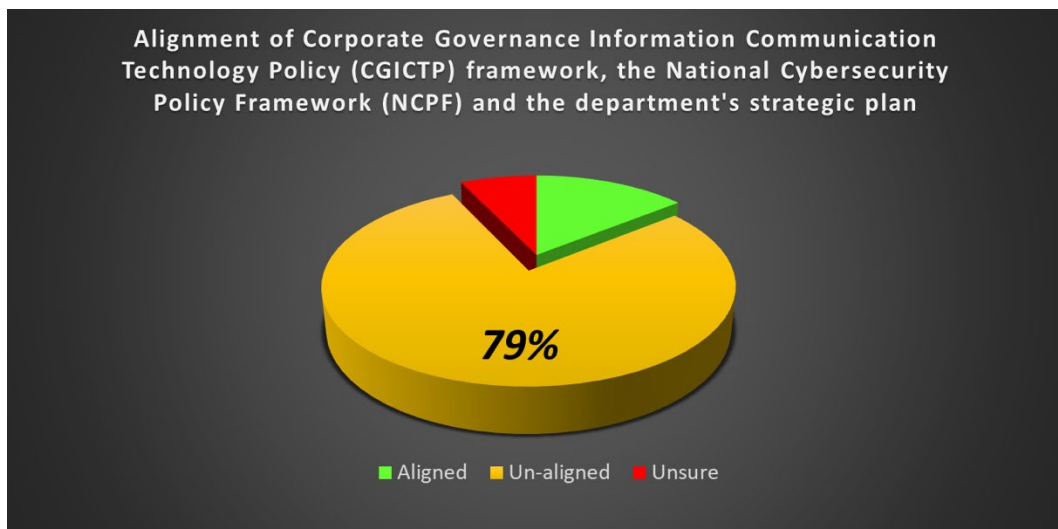
Figure 37: Process to identify critical functions and processes, information or business assets that are essential



Source: Harris, 2021

During the initial stages of the literature review, it emerged that there was a lack of literature referring to the alignment of the frameworks and strategies in government. Therefore, the data were analysed to investigate alignment between the Corporate Governance Information Communication Technology Policy (CGICTP) framework, the National Cybersecurity Policy Framework (NCPF) and the department's strategic plan to promote cybersecurity.

Figure 38: Alignment of Corporate Governance Information Communication Technology Policy (CGICTP) framework, the National Cybersecurity Policy Framework (NCPF) and the department's strategic plan



Source: Harris, 2021

It is important to highlight that a high percentage of the respondents stated that there is no alignment of the frameworks and strategies. As two of the fourteen respondents stated:

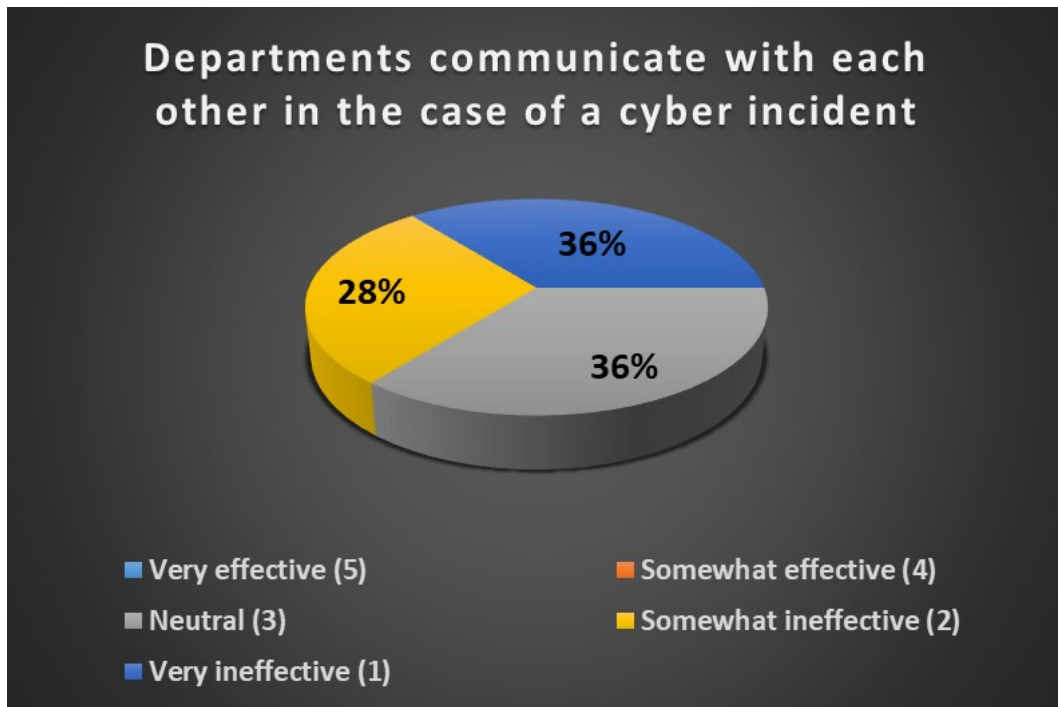
“Alignment is an issue. There is no guidance from national on the alignment of these documents or frameworks. Departments tend to have these in place to be compliant and that is all. How these different policies, strategies and framework align with each other is something that needs to be discussed” (respondent 6).

“The policy has no functionality in the real operational world” (respondent 5).

Prior research studies have noticed the importance of alignment (Bohnert, Gatzert, Hoyt, & Lechner, 2019); however research regarding the alignment of cybersecurity with government frameworks and department strategies remains a problem.

Communication is a critical part of cybersecurity when it comes to responding to an incident. Departments need a communication plan or procedure in place as to how they will communicate and coordinate in a cybersecurity incident. Data extracted tries to establish from the documentation if there is a communication plan or an informal arrangement regarding how departments communicate with one another when there is a cybersecurity incident. Figure 39 data outlines that poor communication takes place in departments when it comes to cybersecurity incidents. A cybersecurity incident or data breach notification procedure or policy could not be identified. However, bits and pieces of cybersecurity communication could be identified in IT security policies, cybersecurity policies, disaster recovery plans, and other related documents.

Figure 39: Departments communicate with each other in the case of a cyber incident



Source: Harris, 2021

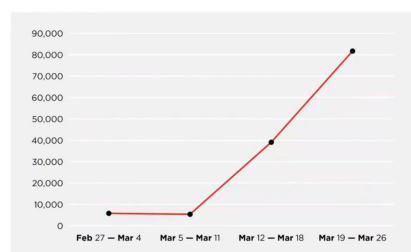
4.7 Emerging Theme - ICT Security trends and threats during Covid 19

Through participant observation in the National GITOC - information security meeting that the researcher did not foresee, an emerging theme was ICT Security trends and threats during Covid 19.

Presenter Comments:

“Massive phishing attempts have been recorded this year.”

Coronavirus-Themed Malicious Email



- February - 5,000 malicious emails blocked
- March - 82,000 malicious emails blocked

For more information on this trend, read our blog:

- [COVID-19 Outbreak Prompts Opportunistic Wave of Malicious Email Campaigns](#)

Symantec | Guest | Proprietary and Confidential | Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

BROADCOM

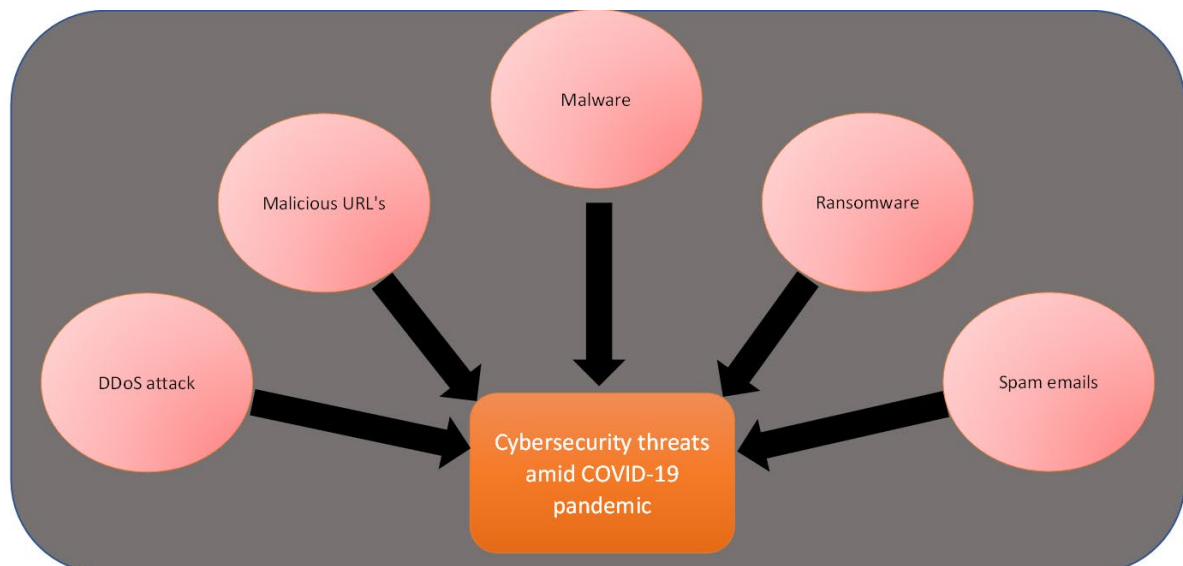
Source: ICT Security trends and threats during Covid 19 – Symantec Presentation

Bad actors worldwide are using the coronavirus as a new tool to deploy and attack government departments. According to Trends micro research (Trends Micro, 2020) there was a 220 times increase in spam email and a 260% increase in malicious URL's during the pandemic. Additionally, the COVID-19 pandemic increased remote working a complex threat landscape that was already under pressure.

Employees were mobilised to work remotely without the security controls or protocols and neglected the implications for cybersecurity in government or organisations. Ransomware, phishing and cloud vulnerabilities presented threats to be watched and managed; securing the remote workforce is undoubtedly the number one concern during the pandemic.

Remote accessing organisational software and databases, which are not secured by end-to-end encryption provided by dedicated servers, making online systems particularly vulnerable to cyber risks and cybercrime. South Africa is particularly vulnerable (Trends Micro, 2020). Data breaches were among the leading cybersecurity trends in the public sector, with sensitive information, employees and the public remaining a cybercriminals target (Mimecast, 2020). An increased threat has evolved with the move to virtual platforms; an excellent example of this exposure is the cyberattacks on the Zoom platform used by government departments for meetings. While previously, such cyberattacks had a small attack footprint.

Figure 40: Top cybersecurity threats amid COVID-19 pandemic



Source: Harris, 2021

Participant observation: MS Teams Virtual Meetings

Participant observation: By observing the discussions and noting down the key issues discussed regarding cybersecurity matters, that can be used as data. Data from the participant observation were generated solely from observations and interactions with participants held on the Microsoft Teams platform (recorded by the researcher). As there was no signed consent, the researcher informed the GITO Council of the researcher's purpose, their continued interaction was taken as consent. The process started by coding data from the transcribed digital extracted data for analysis. Next, the researcher extracted themes and links relating to cybersecurity from the two virtual meetings.

The PGITOC has always been held at the Office of the Premier, and however, due to Covid, the meeting is now held online via Microsoft Teams. The GITO council meeting comprised 80% of the members

joining via MS Teams, observation using the MS Teams platform, the meeting commenced on time and proceeded in the fashion of straight to the point.

Cybersecurity is on the GITOC meetings' agenda and was discussed for 15% of the total meeting length. Members were interested in the cybersecurity agenda item as many departments would like to improve and were eager to hear what sister departments have in place. Departments mentioned they have had Auditor General findings relating to ICT Security and was not defined as cybersecurity. From the observation of the members, it was noted that some members were not comfortable with cybersecurity and listening to the discussions needed a higher level of cybersecurity awareness than the regular staff cybersecurity / ICT security awareness that takes place. An element of this is evident in the impression of the GITO Council meeting, where attendees are encouraged to make cybersecurity a priority.

At the start of the national GITO council – SCISS meeting, the chairperson announced that recordings could take place as the meeting has not been defined as a security level as external presenters were part of the meeting. One hundred seventeen participants joined the MS Teams meeting, which included six external presenters. From the meeting, three key themes were extracted that would benefit the researcher's research. The themes that were extracted: ICT Security trends and threats during Covid 19 presented by Symantec, New SA Trends presented by Wolfpack, Information Risk and ICT Security Policies/Legislations and update on Virtual Communications and Public Cloud presented by SSA. From the observation, the term cybersecurity has not been used and ICT security is used to represent cybersecurity.

4.8 Conclusion

This chapter presented the data collected was designed to determine the rationale of cybersecurity within the government-industry; the researcher presented the data obtained from both the primary and secondary sources—the primary source data collected from semi-structured interviews conducted with fourteen participants. Due to the limited literature on published research regarding cybersecurity, the researcher also used data collected from the government departments and internal/external audit reports—the secondary data obtained using a systematic mapping process to identify any gaps or limitations.

The research found that the top three vulnerabilities to the government show virus or worms as being the top threat or vulnerability and phishing or malicious emails as the second, and theft of devices as the third. The top three current vulnerabilities from threats to government information systems are phishing or malicious mail, Internet services disruption and departmental websites hacked or compromised.

Noted from the data, to improve operational resilience through effective cybersecurity, the top three needs are communication, cybersecurity awareness and cybersecurity recovery plan.

Government departments top three response to cybersecurity incidents is incident response, event monitoring and cybersecurity reporting.

Drawing on these findings, this chapter streamlines a base for the next chapter to discuss the research findings to respond to the research questions. The discussion of the findings will combine all the data sources to understand the research topic.

CHAPTER 5: ANALYSIS OF THE GOVERNMENT CYBERSECURITY LANDSCAPE

5.1 Introduction

While the previous chapter reported findings, this chapter discusses the research findings that were conducted in the provincial government. The purpose of the research was to investigate threats and vulnerabilities in cybersecurity and determine if there is a need to mitigate cybersecurity using frameworks and standards. By investigating cybersecurity alignment with frameworks and standards, the current threats and vulnerabilities can be identified and addressed that impact government information systems. The research looks at what is needed for the provincial government to respond to a cyber incident and what government needs to do to become cyber resilient. The findings in this chapter are supported by the results of queries performed in the ATLAS.TI software. An example of the codes generated in ATLAS.TI can be viewed in section 3.4.4.3 and Table 7: Sample of Themes, Code Groups, and Codes created, where the determinants are related to code groups and dimensions.

It is clear that there appear to be many different definitions related to the term “cybersecurity”. The understanding of the term is varying in literature, frameworks and standards. Although this was not one of the research targets, the same phenomenon was witnessed during the interviews and by analysing the department's documents.

Following the research questions, this chapter discusses the findings. It is structured according to the themes that were used to present the findings in chapter 4, namely, (i) current cyber vulnerabilities of government information systems to external threats, (ii) identification of cybersecurity vulnerabilities in government departments, (iii) needs with respect to improving operational resilience through effective cybersecurity and (iv) government departments’ responses to cybersecurity incidents.

5.2 Current cyber vulnerabilities of government information systems to external threats

This theme partially addresses the question of what are the current cyber vulnerabilities of government information systems to external threats (research question 1). The literature considers cybersecurity risks (vulnerabilities and threats) as one of today's leading and challenging risks. The interviews and document reviews indicate that there is an acknowledgement that the provincial government is facing cybersecurity risk. One of the cybersecurity risks will always be the vulnerability that a weak cybersecurity posture may bring on. Therefore, it is essential that the provincial government assess cybersecurity risks. The research identified provincial government current top cyber vulnerabilities as phishing or malicious mail, internet services interruption and departmental websites hacked or defaced. Key to verifying the research collected, the researcher participated in national government online meetings to gain insight into vulnerabilities affecting the whole government. Malicious emails from phishing attempts have increased in the current years and targeted attempts have been made on the government.

Provincial governments' visibility of cybersecurity vulnerabilities and threats has been identified as lacking from the research; Diesch, Pfaff and Krcmar (2020) highlight the significance of mitigating cybersecurity vulnerabilities and threats through the identification visibility of cybersecurity risks. As discussed in section 1.5.2, cyber incidents that have taken place in the South African government include phishing or malicious mail, internet services interruption and departmental websites hacked or defaced. As identified by the respondents, the provincial department's perceptions are based significantly on the daily and weekly alerts the departments receive from the National Cybersecurity Hub. The data from the research provides a view that the provincial government departments do not understand the vulnerabilities and threats specific to the province. The provincial government has a weakness in identifying current vulnerabilities and threats. The provincial government and its departments need to do a threat analysis to gain a provincial level perspective. Performing a threat analysis can ensure the provincial government moves away from an approach of reactive cybersecurity to proactive cybersecurity. The benefits of performing a threat analysis in the provincial government allow the provincial government departments to understand their cybersecurity environment and modify their cybersecurity protocols or policies and enable vital security operations to safeguard it against cyber-attacks. The cybersecurity threats and vulnerabilities need to be reported to the provincial GITO, HOD forum and Premier of the province. The province can then act against the cybersecurity threats and vulnerabilities by implementing resources to mitigate the risks that apply to their environment. Government needs to become proactive and stop implementing policies, standards, and frameworks for compliance only or avoid having an audit general finding. Data from the unidentified provincial government only matches parts of the systematic map. This emphasises that there may be gaps as critical categories such as inside threats were not extracted from the provincial government departments data. The literature further supports that the identified cybersecurity vulnerabilities and provincial government threats correspond with the literature and research findings. From the literature review, the risk to government information systems can be defined as a potentially damaging consequence due to a cyber-attack or cyber threat that comprises the confidentiality, integrity, and availability of government information systems.

5.3 Identification of cybersecurity vulnerabilities in government departments

This theme partially addresses the question of what are the current cyber vulnerabilities of government information systems to external threats (research question 1). In view of the above, the researcher further looked at the cybersecurity vulnerabilities and incidents in provincial government departments and not specific to government information systems. The findings further support the above, hacked websites in provincial government departments took place and continue to occur. Even though from the interviews, it was determined that departments identify vulnerabilities in their environment, when considering data collected from the documents reviews, a different representation is provided. Data from the document review on the visibility of cybersecurity threats indicated that the provincial departments have poor visibility and could demonstrate a low governance maturity with poor controls and reporting. In essence, this will create a barrier to identify and mitigate cybersecurity risks (Diesch, et al., 2020). The top risks identified not specific to information systems included the theft of devices, virus or malware, and phishing has been identified as part of the vulnerabilities of government information systems.

Department employees and criminals outside of government were identified as threat actors in the provincial government departments. Insider threats identified in the larger systematic map of cyber vulnerabilities were not identified as a threat actor in the provincial government's extracted data.

There was a challenge in the document review, vulnerabilities or threats are categorised differently in departmental reports. This can affect the research as there is no consistency between categories or identification of risks, which could lead to bias towards specific threats or vulnerabilities. Emphasis on wrong cybersecurity controls could create an impact on a department as the prevalent vulnerabilities are not getting addressed. This research found that the document review results contradict the results from the interviews, which indicates that the provincial government will not quickly identify the cybersecurity vulnerabilities and threats in the environment. The researcher data provides a view that the provincial government is not in line with the national cybersecurity policy framework because the identification of cybersecurity risk is low. These factors can potentially influence the availability of government information systems and affect the department's operational resilience. The HOD Forum and GITO Council need to be informed that departments are not aligning with the national cybersecurity policy framework. Provincial departments information technology units need to align the departments IT strategy / IT plan with the department's strategy and include cybersecurity to ensure the department's operational resilience. The researcher suggests that the office of the premier establishes a cybersecurity unit/hub that looks at all departments cybersecurity and allocates resources that include finance and human resources. There is a greater risk if these factors influence the department's operation, for example, the health department, whereby human life could be at stake.

5.4 Needs with respect to improving operational resilience through effective cybersecurity

This theme addresses the question of how provincial government departments mitigate cybersecurity vulnerabilities (research question 3). Operational resilience requires cybersecurity risks to be identified, good governance and strong leadership in the provincial government departments. Government departments leadership, such as executive management, need to understand the roles and responsibilities they need to play for effective cybersecurity and operational resilience. Executive management's commitment to cybersecurity provides a view of accountability in the department. In the interview findings, only half of the department's had their leadership commitment as some departments' executive management focus is purely compliance and receiving a clean audit. One of the reasons that may be the cause of insufficient leadership commitment, as stated in section 4.2.2.2, cybersecurity issues were identified as problematic to explain to executive management as cybersecurity is technical in nature. Lack of leadership or executive management commitment is seen as an inhibitor to achieve effective cybersecurity and can lead to mismanagement. In this respect, the literature emphasises that a top-down approach supports effective cybersecurity and alignment in the context of the government departments business strategy. Alignment has become an organisations' necessity to bring about risk management, effectiveness, resilience, mitigation and compliance (Bohnert, Gatzert, Hoyt, & Lechner, 2019). If executive management is aware of the government department's cybersecurity risks, they would understand the roles and responsibilities they need to play in achieving effective cybersecurity and operational resilience.

The interviews and document review findings indicate department's GITO's or IT managers do not have cybersecurity roles and responsibilities defined; indeed, they were mostly in managerial or senior positions they have dual or multiple roles to play. A small percentage of the departments have cybersecurity as a key performance area or defined in their job descriptions, and this leads the researcher to conclude that there may be low accountability and reporting on cybersecurity in the provincial government departments. The findings from data collected in the stages show that executive management does not understand their role in managing and driving effective cybersecurity.

Literature dictates that operational resilience requires appropriate activities and plans to be implemented in the department's environment. A cybersecurity recovery plan incorporates a business continuity plan, disaster recovery plan and a cybersecurity incident recovery plan. The document reviews and interviews' findings indicate that the provincial government department's do not have the required plans to be operational resilient or have effective cybersecurity in place. A cybersecurity recovery plan that incorporates business continuity, disaster recovery and incident is imperative for operational resilience in the organisation (NIST, 2018). Cyber resilience is about being proactive and not reactive (Carew, 2019). If cybersecurity is not adequately addressed, the cost will be perceived as being to be high, and risks are likely to increase with emerging cyber threats.

Although provincial government departments do not have specific cybersecurity policies and frameworks, the findings in section 4 are consistent with literature revealing organisations and government are aligning their ICT/IT security policies, strategies and frameworks against a combination of international frameworks, policies and standards.

The most popular standard in provincial government departments is COBIT, some of the standards that have been adopted include ISO/ECC 27001, ISO/EC 27002, COBIT and NIST Cybersecurity framework. A combination of information and cybersecurity standards and frameworks have been adopted; only a single department has adopted and customised the NIST cybersecurity framework. The majority indicated they use COBIT, which is best suited accordingly to them for a government perspective; however, this lacks the security aspect. Departments have implemented the provincial security policy, with a small percentage having their own customised or departmental security policies. Departments have implemented controls to mitigate cybersecurity risk, and the further data support that controls identified with the lowest ratings such as malware and awareness is not effective in the departments. Only three-quarters of the departments have NCPF mentioned in their departmental documents; this can imply that there is an alignment issue between the department, provincial and national. The interviews and document review findings revealed that there are some challenges in government departments to implement effective cybersecurity. The main inhibitors to effective cybersecurity were identified as cybersecurity risks, misalignment, and lack of cybersecurity awareness.

The NCPF conveys that a cybersecurity culture is required in departments, a cybersecurity culture that implements cybersecurity awareness can lay the foundation for effective cybersecurity in a department. Awareness training and including employees in security activities is essential for building a cybersecurity culture (Tambo & Adama, 2017; Craig, 2018). As to literature, cybersecurity awareness is critical for effective cybersecurity and resilience.

Cybersecurity awareness seems like the first line of defence for a department, departmental employees and executive management need to be aware of the risks the organisation may face and the impact a cyber incident may have. Departments are not in line with the NCPF as awareness in the departments are not implemented or specific to cybersecurity. As noted from the national online meetings, there is no consistency in cybersecurity awareness in departments, and cybersecurity is an issue when conveying to executive management. There was a challenge in the document review as departments report differently, awareness meetings are held in the department; however, the details of the awareness was not disclosed. Some departments awareness were scheduled and recorded no attendance of employees. Departments are obligated to provide security awareness as to the auditor general audits and compliance. The concern is that awareness is only implemented for compliance, staff awareness is insufficient and is not specific to cybersecurity. The findings, corroborated by the interviews and document review, indicated the lack of cybersecurity awareness in departments, which leads to cybersecurity not being taken seriously by executive management and employees, and non-compliance to the NCPF. The researcher data promotes a view that there is a lack of education and awareness in the provincial departments, and this can be an issue as a cybersecurity culture influences the effectiveness of effective cybersecurity. Departments having real-time awareness during a cyber incident can help the department mitigate the cybersecurity risk and respond to the attack. The HOD's of the provincial departments needs to be informed of the status of cybersecurity in their respective departments and allocate resources to mitigate the risks associated with cybersecurity and operational resilience. The researcher believes the involvement of all the provincial government departments staff would ensure a cybersecurity culture and improve the effectiveness of cybersecurity in the province.

5.5 Government departments' responses to cybersecurity incidents

This theme addresses the question of how government departments currently respond to cybersecurity incidents (research question 2). Effective cybersecurity requires incident response capability, and this is important for every organisation. Implementing appropriate measures to respond to a cybersecurity incident involves people, systems, and processes to detect and respond and restore the operational services of the department that were impaired by a cybersecurity incident (NIST, 2018). As previously discussed in section 5.4, responding to a cybersecurity incident requires a cybersecurity recovery plan that incorporates business continuity, disaster recovery and an incident recovery plan that supports operational resilience in the organisation (NIST, 2018). The incident recovery plan manages cybersecurity incidents and mitigates the cybersecurity risk to save the costs that may occur due to the incident compared to an increased cost that may have cost to recover. The research found that some of the department's had parts of the cybersecurity recovery plan; none of the departments had all the required plans.

The interviews and document review findings indicate that the departments believe they have some controls in place to respond to cybersecurity incidents. Controls required to respond to a cybersecurity incident include incident response, event monitoring and cybersecurity reporting (NIST, 2018). Data from the document review on the controls in departments indicated that departments have poor controls in place to respond to a cybersecurity incident. The limited departments with controls have primary controls specific to incident response and no event monitoring or cybersecurity reporting.

Departments rely on the IT unit or external SITA to detect incidents focused on the government department. An effective incident response plan outlines how cybersecurity incidents get managed and assists in restraining the impact if an incident occurs and requires communication from all the stakeholders.

Communication is critical when responding to a cybersecurity incident, and the research found that departments do not have a cybersecurity incident or data breach notification procedure. Departments do not communicate with one another regarding cybersecurity incidents, and effective communication is a critical part of the incident response plan or responding to a cybersecurity incident. Departments need to have a communication plan in place so that cyber response activities can be coordinated and all relevant parties will be involved. The findings corroborated by the interviews and document review, departmental GITO's or IT Managers could not identify whose role is to respond to a cybersecurity incident. Almost half the respondents believed there is no role to be played by departments, provincial (GITOC) or SITA. Lack of leadership or executive management commitment is seen as an inhibitor to achieve effective cybersecurity and can lead to mismanagement. The data collected in the interviews supports that there is no accountability when it comes to cybersecurity and executive management buy-in is essential for cybersecurity.

As discussed in the literature review, Section 2.3.1, effective alignment reimburses a positive effect. The interviews and document review findings indicate that department frameworks and policies, and strategies are not aligned. Without the alignment of cybersecurity and risk, resilience cannot be improved in departments, as cybersecurity risks considered an essential factor for digital transformation and e-government services (ITU, 2018b). The national department, State Security Agency, reported that a national information security governance framework had been drafted to resolve issues such as alignment. The national information security governance framework (SSA, 2020) intends to solve the alignment issues departments are having, data from the research provides a view that at provincial government there is more than an alignment issue. Currently, government departments are only utilising parts of COBIT that converse with the needs of the department, the national information security governance framework utilises the whole of COBIT 5 and involves creating committees for alignment. The framework does provide alignment between a number of other best practices and standards such as ISO 27002, NIST Cybersecurity Frameworks, SANS 20 Critical Security Controls, NERC CIIP, NIST Risk Management Guide and the Microsoft Security Development Lifecycle. However, the framework does not stipulate how the alignment between the departmental and provincial strategies and frameworks will be linked.

The researcher believes that risk management and cybersecurity are intertwined, the benefits derived from cybersecurity and risk management have not been fully gained, which can be construed as mismanagement of risks. The benefits derived from cybersecurity and risk management have not been fully gained. Managing departmental risks with cybersecurity risks and aligning to business is a problem whereby alignment is missing or is not established in government departments. Less than half the respondents have a clear view as to what is alignment; however, the data extracted could not indicate if any alignment had been implemented in their respective departments. Alignment is a necessity to bring about risk management, effectiveness, resilience, mitigation and compliance (Bohnert, Gatzert, Hoyt, & Lechner, 2019). The involvement of senior management in the departments and the GITO council in the province can assist in the identification of risks, mitigating the related risks with the support of senior management, departmental GITO's and IT/ICT will ensure effective

mitigation of cybersecurity and departmental risk. The GITO council should be making departments HOD's and the premier aware of non-compliance in departments and implement measures to ensure that cybersecurity incidents in the departments are reported to the provincial GITO council to ensure that the cybersecurity incidents get a response and cybersecurity controls to get amended to mitigate future incidents.

5.5 Conclusion: Integrated view of vulnerabilities, responses and people management

Cybersecurity requires an integrated approach to vulnerabilities, responses and people management in provincial government departments. By bringing together the various functions and dependencies with other parts of the organization, operational resilience can be improved. The identification of cybersecurity vulnerabilities is critical for the provincial government to respond to cyberattacks and threats, this cybersecurity risks can be mitigated by incorporating people management with programs such as cybersecurity awareness. Cybersecurity vulnerabilities, responses and people management are interlinked and need to be aligned to improve the provincial government's operational resilience.

One of the key implications is that there is no alignment between provincial departments regarding cybersecurity. There was a challenge in the document review, vulnerabilities or threats are categorised differently in departmental reports. Reviewing the data collected with the aid of ATLAS.TI computer software and generating codes and groupings, the researcher noted that the document review results contradict the results from the interviews, which indicates that the provincial government will not quickly identify the cybersecurity vulnerabilities and threats in the environment. In this regard, the provincial government is not in line with the national cybersecurity policy framework because the identification of cybersecurity risk is low. The interviews and document review findings indicate the department's GITO's or IT managers do not have cybersecurity roles and responsibilities defined; indeed, they were mostly in managerial or senior positions. Provincial government department's do not have the required plans to be operational resilient or have effective cybersecurity in place.

Critical to the implementation of cybersecurity is the alignment and implementation of frameworks and standards. The most prevalent standards in provincial government departments are COBIT, some of the standards that have been adopted include ISO/ECC 27001, ISO/EC 27002, COBIT and NIST Cybersecurity framework. The challenges in provincial government departments implementing effective cybersecurity and main inhibitors to effective cybersecurity were identified as cybersecurity risks, misalignment and lack of cybersecurity awareness. Departments are not in line with the NCPF as awareness in the departments are not implemented or specific to cybersecurity. Interviews and document review indicated the lack of cybersecurity awareness in departments, leading to cybersecurity not getting taken seriously by executive management and employees and non-compliance to the NCPF. Critical to the provincial government, the NCPF needs to be implemented in the provincial government departments.

The research found that some of the department's had parts of the cybersecurity recovery plan; none of the departments had all the plans, a cybersecurity recovery plan that incorporates business continuity, disaster recovery and an incident recovery plan. The limited departments with controls have primary controls specific to incident response and no event monitoring or cybersecurity

reporting. Departments rely on the IT unit or external SITA to detect incidents focused on the government department.

Departments need to have a communication plan in place so that cyber response activities can be coordinated and all relevant parties will be involved. Lack of leadership or executive management commitment is seen as an inhibitor to achieve effective cybersecurity and can lead to mismanagement.

The data collected in the interviews supports that there is no accountability when it comes to cybersecurity and executive management buy-in is essential for cybersecurity. Risk management and cybersecurity are intertwined, the benefits derived from cybersecurity and risk management have not been fully gained, which can be construed as mismanagement of risks. Data extracted could not indicate if any alignment had been implemented in their respective departments.

CHAPTER 6: CYBERSECURITY IN PROVINCIAL GOVERNMENT: RESEARCH SUMMARY, RECOMMENDATIONS AND CONCLUSION

6.1 Introduction

This section presents a combination of the research findings interpreted and discussed from the analysis of data collected from the interviews and document review and provides evidence of how the research aims have been fulfilled. Linking all the previous sections, this final section reaffirms the findings' implications, contributions, and limitations. Chapter 1 introduced the study and described the research approach. The research aimed to investigate threats and vulnerabilities in cybersecurity and determine if there is a need to mitigate cybersecurity using frameworks and standards. By investigating cybersecurity alignment with frameworks and standards, the current threats and vulnerabilities can be identified and addressed that impact government information systems. In addition, the research looked at what is needed for the government to respond to a cyber incident and what government needs to do to become cyber resilient. Chapter 2 presented a literature review on cybersecurity. Chapter 3 discussed the research methodology and research design that guided the research study. In contrast, Chapter 4 presented the qualitative data collected from the interviews, document review and undergoing a systematic mapping procedure. Finally, chapter 5 presented a discussion on the qualitative data findings.

This chapter explores how the research objectives and research questions are investigated and answered. Section 6.2 justifies the research scope, followed by a brief overview of how the research questions 6.3 were addressed. Section 6.4 outlines the limitations, and 6.5 recommendations from the research and a view for future research, section 6.6 the contribution to knowledge.

6.2 Research justification

This research was intended to investigate if the government identifies cyber risks and establishes a cyber risk management approach through strategies, policies, and acceptable cybersecurity practices. The research further tries to identify the factors that influence or affect cybersecurity effectiveness in government departments. While this study is limited in scope to government departments, the results may easily be applied to government entities and private sector organisations as the cybersecurity effectiveness of government departments are critical to the maintenance of services to the public.

6.3 Results determined by research questions

The research questions addresses the research gaps and if the research objectives have been met.

6.3.1 Question 1 - What are the current cyber vulnerabilities of government information systems to external threats?

The first question of the research was identifying the current cyber vulnerabilities of government information systems to external threats. This research had two approaches to fulfil this objective: review literature to identify the current cyber vulnerabilities of government information systems to external threats and to review the literature and address questions to respondents during the semi-structured interviews and document review.

The first approach showed the trends in the literature regarding cyber vulnerabilities and threats to the government. Many countries across the globe are embracing emerging trends in cyberspace, and cybersecurity concerns are accumulating due to reports of increased breaches and attacks (Fearn, 2017; van Niekerk, 2017; SABC News, 2017). The research identified vulnerabilities and threats influencing the provincial government departments environment. The research agrees with other researchers; however, this research contribution goes beyond their research. Creating knowledge about real-world practice and not only theory. Considering the broad spectrum of cybersecurity risks and cyber vulnerabilities and threats, the following cyber incidents in the environment were identified: hacked websites, ransomware, file server attacks, blockchain attack, denial of service attacks, phishing, malware and social engineering were recorded.

A weak cybersecurity posture was identified as one of the primary cybersecurity risks. The current cybersecurity vulnerabilities likely to affect the provincial government systems were identified as website attacks, user access violation, virus or malware infection, ineffective firewalls, ransomware attack or infection, disruption of internet services, phishing or malicious emails, information theft, awareness in departments, hacking and denial of services attacks. The top three identified cyber vulnerabilities most likely to affect the provincial government information systems are malware, hacking and phishing. The threat actors posing cybersecurity threats to the departments were identified as employees, criminals and hacktivists. Comparing this with the literature analysis, it was noted that this coincides with top vulnerabilities and threats as the research shows consistency in the results.

The provincial government visibility of cybersecurity vulnerabilities and threats has been identified as lacking. Findings from the interviews and document review indicated that departments have poor visibility of cybersecurity threats and vulnerabilities. The result can indicate a low governance maturity with poor controls and reporting. Department employees and criminals outside of government were identified as the threat actors. Emphasis on wrong cybersecurity controls could create an impact on the department as the prevalent vulnerabilities are not getting addressed. The scale of cybersecurity threats and vulnerabilities is escalating in the provincial government, and the impact of cyberattacks on the provincial government's information systems can be devastating. These factors influence the availability of government information systems and operational resilience; further, the provincial government is not complying with the national cybersecurity policy framework. The importance of this research and its contribution can not be stressed enough, and the research provides a means in understanding cyber practice in sub-national government.

6.3.2 Question 2 - How do government departments currently respond to cybersecurity incidents?

Literature dictates that operational resilience requires appropriate activities and plans to be implemented in the department's environment. A cybersecurity recovery plan incorporates a business continuity plan, disaster recovery plan and a cybersecurity incident recovery plan. Effective cybersecurity requires incident response capabilities, implementing measures to respond to a cybersecurity incident involves people, systems and processes to detect and respond (NIST, 2018). Controls required to respond to a cybersecurity incident include incident response, event monitoring and cybersecurity reporting. The document reviews and interviews' findings indicate that the provincial government department's do not have the required plans to be operational resilient or have effective cybersecurity in place.

Some of the provincial government departments have parts of the cybersecurity recovery plan; however, none had all the plans. In addition, the provincial departments have poor controls for incident response and no event monitoring. As a result, the provincial government will not quickly identify the cybersecurity vulnerabilities and threats in the environment and respond quickly.

In this regard, the provincial government is not in line with the national cybersecurity policy framework because identifying cybersecurity risk is low. Department relies on the departmental IT unit or external SITA to detect and respond to cybersecurity incidents. The department's GITO's or IT managers could not identify whose role to respond to a cybersecurity incident. Research data from the document review on the visibility of cybersecurity threats indicated that the provincial departments have poor visibility and could demonstrate a low governance maturity with poor controls and reporting. In essence, this will create a barrier to identifying and mitigating cybersecurity risks (Diesch, et al., 2020). Emphasis on wrong cybersecurity controls could create an impact on a department as the prevalent vulnerabilities are not getting addressed. Communication is problematic as departments do not communicate with each other regarding cybersecurity incidents. Communication is a critical part of a cybersecurity incident recovery plan. Departments need to have a communication plan so that cybersecurity response activities can be coordinated. The maturity level of cybersecurity is deficient, and provincial government departments are only starting to implement cybersecurity. Currently, the response to cybersecurity is inefficient, and incidents are treated as an ordinary IT incident.

Although provincial government departments do not have specific cybersecurity policies and frameworks, the findings are consistent with the literature. This research is based on real-world practice in sub-national government and is not based on theory only. Organisations and government align their ICT/IT security policies, strategies and frameworks against a combination of international frameworks, policies and standards. The most popular standard in the provincial government departments is COBIT, some of the standards that have been adopted include ISO/ECC 27001, ISO/EC 27002, COBIT and NIST Cybersecurity framework. A combination of information and cybersecurity standards and frameworks have been adopted; only a single department has adopted and customised the NIST cybersecurity framework. Interviews and document reviews indicate that the departments believe they have some controls to respond to cybersecurity incidents. Controls required to respond to a cybersecurity incident include incident response, event monitoring and cybersecurity reporting (NIST, 2018). However, findings from the research indicated that departments have poor controls in place to respond to a cybersecurity incident.

6.3.3 Question 3 - How should provincial government departments mitigate cybersecurity vulnerabilities?

There is no single solution to cybersecurity, noting that different frameworks and policies prescribe different approaches. Government departments can determine whether to align or adopt industry frameworks, standards, or combinations of the best practices. Cybersecurity needs to be institutionalised, operationalised and integrated into the department and cannot follow a silo approach to ensure operational resilience. Cybersecurity starts at the top of the department, executive management buy-in and commitment is critical. The South African government's response to the issue of cybersecurity has been the implementation of the National Cybersecurity Policy Framework (NCPF), which is aimed at a coherent and integrated cybersecurity approach to address cybersecurity threats.

Given the global cyber-crime, the public and private sectors have taken cybersecurity precautions to strengthen and mitigate these risks (SSA, 2015). Cybersecurity vulnerabilities mitigated through cybersecurity frameworks, standards, people management and backed up by good vulnerability intelligence can provide an understanding of how and why threat actors are targeting particular vulnerabilities. In addition, the National Cybersecurity Policy Framework utilising existing standards and measured using the NIST cybersecurity framework ensures that the government's cybersecurity vulnerabilities get identified.

Although provincial government departments do not have specific cybersecurity policies and frameworks, departments align their ICT/IT security policies, strategies and frameworks against a combination of international frameworks, policies and standards. Departments have implemented a combination of standards such as COBIT, ISO/ECC 27001, ISO/ECC 27002 and the NIST Cybersecurity framework. COBIT is a common favourite for most departments and the provincial IT security policy. The majority of the provincial government departments have control frameworks in place. However, these controls need enhancement or are not consistently applied or operating effectively. Some of the provincial government departments' challenges are the inhibitors to cybersecurity, such as cybersecurity risks, misalignment, and lack of cybersecurity awareness.

Cybersecurity awareness is the first line of defence for a provincial government department. Departmental executive management and the department employees need to be aware of the cybersecurity risks in the organisation and the impact a cybersecurity incident may have. Provincial government departments need to comply with the national cybersecurity policy framework, and as noted from the national online meeting, departments are not implementing cybersecurity awareness. The lack of cybersecurity awareness in the departments provides an impression that the departments executive management is not taking cybersecurity seriously. People are the most significant vulnerability in any organisation, and people management is critical to ensure a cyber-secure culture that can mitigate overall cyber-related business risks. A commendable component of the NCPF is how it targets awareness and education as critical pillars to cybersecurity due to the human factor. Mbanaso, Abrahams and Apene (2019) research further support cybersecurity standards, awareness, and alignment to mitigate potential inside and outside vulnerabilities or attacks for operational resilience. Awareness training and including employees in securing activities are essential for building a cybersecurity culture (Tambo & Adama, 2017; Craig, 2018). The top three needs are communication, cybersecurity awareness, and a cybersecurity recovery plan to improve operational resilience through effective cybersecurity.

The provincial government department implements cybersecurity awareness as a matter of compliance so that the departments do not get an audit finding. Although the NCPF conveys that a cybersecurity culture is required, the provincial government departments fail and prohibit them from implementing effective cybersecurity. Executive management needs to understand the roles and responsibilities they need to play for effective cybersecurity and operational resilience. Executive management commitment to cybersecurity provides accountability, lack of leadership or executive management commitment is seen as an inhibitor to achieving effective cybersecurity. Key to cybersecurity is that executive management needs to be aware of the potential or current cybersecurity risks and the impact that cybersecurity risks have on the department, such as disrupting government information systems. Executive management needs to understand what controls are required to mitigate the risks via frameworks, policies and standards.

Executive management has not defined the role of cybersecurity to the department's GITO's and IT managers; this may lead to an accountability and reporting issue. This indicates that executive management does not understand their role in managing driving effective cybersecurity. Implementing a policy approach, frameworks can be reinforced as policies are expected to facilitate rather than regulate. Through cybersecurity frameworks, the provincial government can facilitate the identification of critical systems and protect the critical systems from evolving cyber threats that can disrupt business operations.

Cybersecurity frameworks assist those charged with cyber governance at the organisation to mitigate the risks associated with adopting and deploying cybersecurity. The benefits of frameworks are that it assists enterprises in achieving their objectives for the governance and management of cybersecurity. Mbanaso, Abrahams and Apene (2019) research further support cybersecurity standards to promote effective management for cybersecurity risks in organisations. The research further supports their findings by creating knowledge on real-world practice in the sub-national government. Research has shown that for the government to respond to cyber incidents, departments need to have cyber resilience that can mitigate cyber risks. Cyber resilience is not only about technology, and it covers people and processes. Cyber resilience cannot exist in isolation and needs to be integrated and aligned in the organisation. The provincial government fails to have operational resilience or cyber resilience, and there is a need for provincial government leadership or executive management of the departments to commit to cybersecurity. There is no accountability for cybersecurity as the departments' executive management has not shown the buy-in required to implement effective cybersecurity. Communication is critical when responding to a cybersecurity incident, and the research found that departments do not have a cybersecurity incident or data breach notification procedure. Departments do not communicate regarding cybersecurity incidents, and effective communication is a critical part of the incident response plan or responding to a cybersecurity incident.

6.3.4 Main Question - How can provincial government departments improve operational resilience through effective cybersecurity?

This research's first objective was to identify and analyse why and how provincial government departments can improve operational resilience through effective cybersecurity. This research had two approaches to fulfil this objective: reviewing the literature on why provincial government departments can approve operational resilience through effective cybersecurity and reviewing the literature, and addressing questions to respondents during the semi-structured interviews and document review.

The first approach showed that literature supports operational resilience through cybersecurity standards, awareness and alignment, promoting mitigation of potential inside and outside vulnerabilities or attacks (Mbanaso, Abrahams and Apene, 2019). Prior literature from research studies also dictates the importance of alignment (Bohnert, Gatzert, Hoyt, & Lechner, 2019) for operational resilience. A lack of literature on government alignment that guides the implementation was also identified, and alignment maturity in provincial government is yet to be achieved. Alignment and coordination across government are needed to implement the National Cybersecurity Policy Framework.

The research findings promote for provincial government departments to have operational resilience through cybersecurity standards, awareness and alignment, promoting mitigation of potential inside and outside vulnerabilities or attacks (Mbanaso, Abrahams and Apene, 2019). Responding to cyber incidents through implementing frameworks, standards and people management can ensure operational resilience in the organisation. The NIST Cybersecurity framework ensures that the cybersecurity vulnerabilities, needs and responses are identified.

Literature dictates that operational resilience requires appropriate activities and plans to be implemented in the department's environment. A cybersecurity recovery plan incorporates a business continuity plan, disaster recovery plan and a cybersecurity incident recovery plan. The provincial department needs to implement all the plans required for operational resilience; without these plans, the department cannot look at cyber resilience or effective cybersecurity. A recovery plan allows the department to restore systems to normal operations and at an acceptable level timely. Through cybersecurity frameworks, the provincial government can facilitate the identification of critical systems and protect the critical systems from evolving cyber threats that can disrupt business operations.

Responding to cyber incidents through implementing frameworks, standards and people management can ensure operational resilience in the organisation. The NIST Cybersecurity framework ensures that the cybersecurity vulnerabilities, needs and responses are identified under categories (Access Control, etc.), and subcategories function referenced to existing standards (ISO/IEC 27001, COBIT, etc.) (National Institute of Standards and Technology, 2018) to ensure operational resilience in government. Operational resilience requires that the appropriate activities and plans need to be implemented in the department's environment. A Cybersecurity recovery plan incorporates the business continuity plan, disaster recovery plan and incident plan. A recovery plan allows the department to restore systems to normal operations and at an acceptable level timely. From the data extracted from the document review and systematic mapping, departments reported they had some or none of the cybersecurity recovery plan requirements. This conclusion is verified as the business continuity and disaster recovery plan score in the bottom four lowest controls in place.

Provincial governments in South Africa needs to focus on the lessons learnt in this research. The implementation of cybersecurity frameworks is critical for improving operational resilience in government departments. Provincial governments need to implement frameworks, policies and standards that incorporate people management as cybersecurity awareness is critical. The national CSIRT focuses mainly on sectors such as the financial sector and needs to look at the three spheres of government, national, provincial and local government and the alignment of cybersecurity within the government departments and municipalities.

The research findings indicate that the provincial government department's do not have the required plans to be operational resilient or have effective cybersecurity in place. Controls required to respond to a cybersecurity incident include incident response, event monitoring and cybersecurity reporting (NIST, 2018). Findings from the research indicated that departments have poor controls in place to respond to a cybersecurity incident. People are the most significant vulnerability in any organisation, and people management is critical to ensure a cyber-secure culture that can mitigate overall cyber-related business risks. A commendable component of the NCPF is how it targets awareness and education as critical pillars to cybersecurity due to the human factor.

The scale of cybersecurity threats and vulnerabilities is escalating in the provincial government, and the impact of cyberattacks on the provincial government's information systems can be devastating. These factors influence the availability of government information systems and operational resilience; further, the provincial government is not complying with the national cybersecurity policy framework. Cybersecurity needs to be institutionalised, operationalised and integrated into the department and cannot follow a silo approach to ensure operational resilience.

Cybersecurity starts at the top of the department, executive management buy-in and commitment is critical. Unfortunately, the lack of cybersecurity awareness in the departments provides an impression that the departments executive management is not taking cybersecurity seriously.

Executive management needs to understand the roles and responsibilities they need to play for effective cybersecurity and operational resilience. Executive management commitment to cybersecurity provides accountability, lack of leadership or executive management commitment is seen as an inhibitor to achieving effective cybersecurity. The provincial government fails to have operational resilience or cyber resilience, and there is a need for provincial government leadership or executive management of the departments to commit to cybersecurity. There is no accountability for cybersecurity as the departments' executive management has not shown the buy-in required to implement effective cybersecurity.

The provincial government departments are unaware of how inadequately prepared they are, and the lack of capabilities to prepare, anticipate, respond and recover from any cybersecurity incident. As a result, many of the provincial departments will not be able to recover critical systems to normal operations at an acceptable level or in a sufficient timeframe. The Cabinet of South Africa, as part of the implementation of the fourth industrial revolution, needs to emphasise the critical need for cybersecurity to be implemented at all levels of government and resources allocated as required.

6.4 Research limitations

The research used qualitative methods and can be considered open to possible subjectivity. However, a lack of quantitative is a limitation specific to qualitative studies. Perhaps the use of mixed methods would have provided additional views or more evident results to the findings. Regarding the primary data collection, another limitation can be related to the respondents selected. The respondents' selection was based on a predefined set of expectations related to their government departments' positions and their information technology and security credentials. Conceivably, future research would include views of the department's executive management, employees, and the department's operational side to be more inclusive.

Another limitation is the number of respondents. The fourteen respondents were from twelve departments/organisations. Two of the respondents were from external organisations. One of the more significant provincial government departments chose not to participate, and their responses may have been beneficial to the research. More than one respondent from the same department may have improved the responses' quality as there was a discrepancy between the data collected from interviews and the document reviews. Due to the limited literature on published research regarding cybersecurity, the researcher also used data collected from the government departments and internal/external audit reports.

Another research limitation refers to the geographical dispersion of the respondents. This research was restricted to one province in South Africa and only provincial departments. The problem with this approach was that the research was limited to a pool of respondents.

Research published from 2016 till today has limited research concerning South Africa and cybersecurity. When extending the search criteria to include government, the data presents a tiny percentage for the South Africa government and cybersecurity.

A further potential source of limitations and gaps in the research can be the fact that only research published in the English language has been selected. This decision may result in a possible threat to rationality because, potentially, necessary research published in other languages may not have been selected. However, the English language is the most widely used language for scientific papers, so that this bias can be reasonably considered as minimal.

6.5 Recommendations for future research

Cybersecurity is constantly evolving, and there are multiple cybersecurity frameworks and standards available to assist government departments in implementing risk-based controls. Cybersecurity is a relatively new security area; published academic and industry research on this topic relating to South Africa is very limited. Future research should focus on implementing these cybersecurity frameworks, and research can analyse why the guidance of these frameworks fails to provide adequate cybersecurity in government departments. As some of the provincial government departments are considering adopting or have adopted the NIST Cybersecurity framework, there could be beneficial research to look at the weaknesses of the NIST framework and other cybersecurity frameworks, standards and policies. The new national information security governance framework is to be implemented in government departments, and research can investigate how the alignment between the departmental and provincial strategies and frameworks will be linked.

Cybersecurity awareness approaches are still lacking in provincial government departments, and research is needed in formulating an organisational cybersecurity awareness framework for a government that promotes operational resilience. Another avenue of research might focus on the legislation of cybersecurity, exploring the specifics of different countries.

Clearly, many cybersecurity areas require research as to the benefits for the South African government. New cybersecurity areas can look at artificial intelligence and machine learning that can assist cybersecurity in identifying, monitoring, detecting and responding to cybersecurity incidents to make better decisions in government departments for effective and resilient cybersecurity.

6.6 Conclusion: Contribution to knowledge

This original research explored cybersecurity vulnerabilities and threats, risks and challenges related to cybersecurity in provincial government departments. The in-depth data is a vital contribution to knowledge in understanding cybersecurity practice in the sub-national government. The research found the following vulnerabilities and threats influencing the provincial government are phishing or malicious mail, internet services interruption caused by the top five categories of the web attacks SQLi (SQL Injection), DDoS (Distributed Denial of Service), defacement, account hijacking and malware, departmental websites hacked or defaced and theft of devices.

The research found that provincial government departments are exposed to cybersecurity vulnerabilities and threats because they do not have adequate controls in place. The provincial government visibility of cybersecurity vulnerabilities and threats has been identified as lacking. The research findings indicated that departments have poor visibility of cybersecurity threats and vulnerabilities, and the result can indicate a low governance maturity with poor controls and reporting. Emphasis on wrong cybersecurity controls could create an impact on the department as the prevalent vulnerabilities are not getting addressed. The scale of cybersecurity threats and vulnerabilities is escalating in the provincial government, and the impact of cyberattacks on the provincial government's information systems can be devastating.

There is no single solution to cybersecurity, different frameworks and policies prescribe different approaches. Government departments can determine whether to align or adopt industry frameworks, standards, or combinations of the best practices. Cybersecurity needs to be institutionalised, operationalised and integrated into the department and cannot follow a silo approach to ensure operational resilience.

Controls need to be prioritised to focus on the top cybersecurity risks, vulnerabilities and threats. Some of the provincial government departments have parts of the cybersecurity recovery plan; however, none of the departments had all the plans. The provincial departments have poor controls for incident response and no event monitoring. Department relies on the departmental IT unit or external SITA to detect and respond to cybersecurity incidents.

Inductive reasoning allowed the researcher to generalise the findings to all provincial government departments. A recommendation to the provincial departments would be to create open communication to foster the right culture for cybersecurity and implement cybersecurity awareness that involves everyone from top to bottom. Communication is a critical part of a cybersecurity incident recovery plan. Departments need to have a communication plan so that cybersecurity response activities can be coordinated. Executive management commitment to cybersecurity provides accountability, lack of leadership or executive management commitment is seen as an inhibitor to achieving effective cybersecurity. Executive management needs to understand the roles and responsibilities they need to play for effective cybersecurity and operational resilience. Cybersecurity awareness is the first line for a provincial government department. The lack of cybersecurity awareness in the departments provides an impression that the departments executive management is not taking cybersecurity seriously. The provincial government department implements cybersecurity awareness as a matter of compliance so that the departments do not get an audit finding. The NCPF conveys that a cybersecurity culture is required, the provincial government departments are failing at this and prohibits them from implementing effective cybersecurity. There is no other significant research on cybersecurity in government at the sub-national level in South Africa. The originality of this research contributes to knowledge by offering in-depth data of a real-world view of cybersecurity in sub-national government.

LIST OF REFERENCES

- Abutabanjah, S & Jaradat, R. (2018). Clarification of research design, research methods, and research methodology: A guide for public administration researchers and practitioners. *Teaching Public Administration Journal*. 36. doi:10.1177/0144739418775787
- Alshayeb, M., Humayun, M., Niazi, M., Jhanjhi, N. Z. & Mahmood, S. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. *Arabian Journal for Science and Engineering*, 45, 3171–3189. doi:10.1007/s13369-019-04319-2
- Arabo, A., & Pranggono, B. (2021). COVID-19 pandemic cybersecurity issues. *Internet Technology Letters*. 4:e247. doi:10.1002/itl2.247
- Auerbach, C., & Silverstein, L. (2003). Qualitative data: An introduction to coding and analysis. New York University Press.
- Azmi, R., Tibben, W., & Win, K. (2018). Review of cybersecurity frameworks: context and shared concepts, *Journal of Cyber Policy*, 3:2, 258-283, doi:10.1080/23738871.2018.152027
- Bazeley, P. (2009). Analysing qualitative data: More than 'identifying themes'. *Malaysian Journal of Qualitative Research*, 2(2):6-22.
http://www.researchsupport.com.au/Bazeley_MJQR_2009.pdf
- Berg, B. L. (2009). Qualitative research methods for the social sciences. London: Pearson.
- Bohnert, A., Gatzert, N., Hoyt, R., & Lechner, P. (2019). The drivers and values of enterprise risk management: evidence from ERM ratings. *The European Journal of Finance*, 25(3), 234 - 255. doi:10.1080/1351847X.2018.1514314
- Breakfast, S. (2018). A hacker has claimed responsibility for attack on Environmental Affairs website. <https://www.thesouthafrican.com/news/environmental-affairs-website-cyber-attack/>
- Broh, S., Hyug, I., Jhanjhi, N. Z., Liang, C., & Ren, A. (2018). A three-level ransomware detection and prevention mechanism., *Journal of EAI Endorsed Transactions on Energy Web*, 7, 26, doi: 10.4108/eai.13-7-2018.162691
- Brohi, S., Dion, Y. (2020). An experimental study to evaluate the performance of machine learning algorithms in ransomware detection. *Journal of Engineering Science and Technology*., 15, 2, 967–981, https://www.researchgate.net/publication/340923541_AN_EXPERIMENTAL_STUDY_TO_EVALUATE_THE_PERFORMANCE_OF_MACHINE_LEARNING_ALGORITHMS_IN_RANSOMWARE_DETECTION/stats
- Brookson, et al. (2015). *Definition of cybersecurity: Gaps and overlaps in standardisation*. Heraklion. doi:10.2824/4069
- Carew, J. (2019). *The business case for cyber resilience*. <https://www.itweb.co.za/content/PmxVE7KXRR5MQY85>
- Chandarman, R., & Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. *The African Journal of Information and Communication (AJIC)*, 20, 133-155. doi:10.23962/10539/23572

- Chigada, J. & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. *South African Journal of Information Management*, 23(1), a1277. doi:10.4102/sajim.v23i1.1277
- Chigada, J. & Kyobe, M. (2018). Evaluating Factors Contributing to Misalignment of the South African National Cybersecurity Policy Framework. CONF-IRM 2018 Proceedings. 4. <http://aisel.aisnet.org/confirm2018/4>
- Chow, L. (2014). The strengths and weaknesses of research methodology: Comparison and complimentary between qualitative and quantitative approaches. *IOSR Journal of Humanities and Social Science*, 19, 99-104. doi:10.9790/0837-194399104
- Craig, J. (2018). Cybersecurity research: Essential to a successful digital future. *Journal of Engineering*, 4, 9–10. doi:10.1016/j.eng.2018.02.006
- Creswell, J. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches*. SAGE Publications. http://fe.unj.ac.id/wp-content/uploads/2019/08/Research-Design_Qualitative-Quantitative-and-Mixed-Methods-Approaches.pdf
- Cybenko, G. (2016). Quantifying and measuring cyber resiliency. *98250R*. doi:10.1117/12.2230586.
- Dalal, R.S., Howard, D.J., Bennett, R.J. et al (2021). Organizational science and cybersecurity: abundant opportunities for research at the interface. *Journal of Business and Psychology*. doi:10.1007/s10869-021-09732-9
- Department of Employment & Labour. (2020). *Department of Employment and Labour employee arrested for cyber crime*. Department of Employment & Labour. <http://www.labour.gov.za/departments-of-employment-and-labour-employee-arrested-for-cyber-crime>
- Department of Labour. (2018). *Labour acknowledges attempted cyber-attack on website*. Department of Employment and Labour. <https://www.gov.za/speeches/departments-of-labour-acknowledges-attempted-cyber-attack-its-website-3-sep-2018-0000>
- Didenko, A. (2018). Regulating fintech: Lessons from Africa. *San Diego International Law Journal*, 19, 311-370. <http://digital.sandiego.edu/ilj/vol19/iss2/5>
- Diesch, R., Pfaff, M., Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers, *Journal Computers & Security*, 92, 101747. doi:10.1016/j.cose.2020.101747
- Dixon, W. & Balson, D. (2020). How COVID-19 shows the urgent need to address the cyber poverty gap. <https://www.weforum.org/agenda/2020/03/covid-19-pandemic-shows-the-urgency-for-addressing-the-cyber-poverty-gap/>
- DTPS. (2017). *National e-Strategy*. Government Gazette.
- Dyess, C. (2020). Maintaining a balance between agility and security in the cloud. *Journal Network Security*, 2020, 3, 14-17. doi:10.1016/S1353-4858(20)30031-3
- ENISA. (2019). *State of vulnerabilities2018/2019: Analysis of Events in the life of Vulnerabilities*. European Union Agency for Cybersecurity. doi:10.2824/139301

- Etheridge, J. (2018). *Hawks, SSA probing major 'leak' of personal data of SA drivers who use ViewFines*. <https://www.news24.com/SouthAfrica/News/hawks-ssa-probing-major-leak-of-personal-data-of-sa-drivers-who-use-viewfines-20180524>
- Fachkha, C. (2015). *Darknet as a Source of Cyber Threat Intelligence: Investigating Distributed and Reflection Denial of Service Attacks*. Concordia University Montreal, Quebec, Canada. https://www.researchgate.net/publication/305827339_Darknet_as_a_Source_of_Cyber_Threat_Intelligence_Investigating_Distributed_and_Reflection_Denial_of_Service_Attacks
- Fearn, N. (2017). *Critical lack of skills could be the biggest security challenge*. IDG Connect. <https://www.idgconnect.com/idgconnect/analysis-review/1012795/critical-lack-skills-biggest-security-challenge>
- Fink, A. (2014). *Conducting research literature reviews: From the internet to paper. 4th ed*. Thousand Oaks, CA: Sage. https://books.google.co.za/books/about/Conducting_Research_Literature_Reviews.html?id=4cKhAQAAQBAJ&redir_esc=y
- Fuzile, L. (2015). *Public Sector Supply chain management review*. National Treasury. <http://www.treasury.gov.za/publications/other/SCMR%20REPORT%202015.pdf>
- Gash H. (2014) Constructing constructivism. *Constructivist Foundations*. 9(3): 302–310. <http://constructivist.info/9/3/302>
- Gcaza, N & Solms, R. (2017). A Strategy for a Cybersecurity Culture: A South African Perspective. *Electronic Journal of Information Systems in Developing Countries*. 80. 1-17. Doi:10.1002/j.1681-4835.2017.tb00590.x.
- Gourisetti, S., Patangia, M. (2020). Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritised gap analysis, *Future Generation Computer Systems*, 105, 410-431. <https://doi.org/10.1016/j.future.2019.12.018>.
- Hassad, R. (2020). A foundation for inductive reasoning in harnessing the potential of big data. *Statistics Education Research Journal*, 19(1), 238–258. <http://iase-web.org/Publications.php?p=SERJ>
- Hammarberg, K., Kirkman, M., de Lacey, S. (2016). Qualitative research methods: when to use them and how to judge them, *Human Reproduction*, 31, 3, 498–501. doi:10.1093/humrep/dev334
- Héroux, S., & Fortin, A. (2017). Exploring the influence of executive management diversity on IT governance. *Journal of Information Systems and Technology Management (JISTEM)*, 14, 401-429. doi:10.4301/S1807-17752017000300007
- ISACA. (2018). *COBIT 2019*. ISACA. https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/cobit-2019-toolkit_v12.7z?la=en&hash=8E54167154AF1E8E34E13B61400A0056438EC1B9
- ISO. (2018). *ISO / IEC 27000 Fifth edition 2018-02*. ISO. https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip

- Ince, M. (2018). Accountability in question: A critical review of public accountability. Google Scholar. https://www.researchgate.net/publication/327775870_ACCOUNTABILITY_IN_QUESTION_A_CRITICAL_REVIEW_OF_PUBLIC_ACCOUNTABILITY/references
- ITU. (2018a). *2018 Global Cybersecurity Index (v3)*. Switzerland: ITUPublications. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
- ITU. (2018b). *Guide to developing a National Cybersecurity Strategy*. International Telecommunication Union (ITU). https://www.itu.int/pub/D-STR-CYB_GUIDE.01-2018
- Jaccard, J., Nepal, S. (2014), A survey of emerging threats in cybersecurity, *Journal of Computer and System Sciences*, 80, 5, 973-993. doi:10.1016/j.jcss.2014.02.005
- John S., Doukas J., Song S., Comstock J. (2018), Advancing Cybersecurity From Medieval Castles To Strategic Deterrence: A Systems Approach To Cybersecurity. *Proceedings of the International Annual Conference of the American Society for Engineering Management. American Society for Engineering Management (ASEM)*, Jan. 2018, p. 1. https://www.researchgate.net/publication/329020707_Advancing_Cybersecurity_from_Medieval_Castles_to_Strategic_Deterrence_A_Systems_Approach_to_Cybersecurity/stats
- Kaspersky. (2019). *Kaspersky Security Bulletin 2019 Statistics*. Kaspersky. <https://securelist.com/kaspersky-security-bulletin-2019-statistics/95475/>
- Krumay B., Bernroider E.W.N., Walser R. (2018). Evaluation of Cybersecurity Management Controls and Metrics of Critical Infrastructures: A Literature Review Considering the NIST Cybersecurity Framework. *NordSec 2018: Secure IT Systems*, 11252, 369-384. doi: 10.1007/978-3-030-03638-6_23
- Lees, M. J., Crawford, M., & Jansen, C. (2018). Towards industrial cybersecurity resilience of multinational corporations. *IFAC-PapersOnLine*, 51, 30, 756-761. doi:10.1016/j.ifacol.2018.11.201
- Marble, J., Lawless, W., Mittu, R., Coyne, J., Abramson, M., Sibley, C. (2015). The Human Factor in Cybersecurity: Robust & Intelligent Defense. *Journal of Advances in Information Security*. 56. 173-206. Doi:10.1007/978-3-319-14039-1_9.
- Mbanaso, U. M. (2016). Cyber warfare: African research must address emerging reality. *The African Journal of Information and Communication (AJIC)*, 18, 157-164. doi: 10.23962/10539/21789
- Mbanaso, U. M., Abrahams, L., & Apene, O. Z. (2019). Conceptual design of a cybersecurity resilience maturity measurement (CRMM) framework. *The African Journal of Information and Communication (AJIC)*, 23, 1–26. doi.org/10.23962/10539/27535
- McAfee. (2018). *The economic impact of cybercrime and no slowing down*. McAfee. <https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf>
- Mimecast. (2020). State of Email Security 2020 report. Mimecast. https://www.mimecast.com/state-of-email-security/?utm_source=BusinessTech&utm_medium=SponsoredArticle&utm_term=February2021

- Mshunqane, Z. (2017). Government and private sector cooperation on security of critical information infrastructures. <https://hdl.handle.net/10539/26268>
- Myers, M. D. (2013). *Qualitative research in business and management 2nd Edition*. London, Thousand Oaks, New Delhi and Singapore: Sage.
- NIST. (2018). *Framework for improving critical infrastructure cybersecurity*. National Institute of Standards and Technology. doi:10.6028/NIST.CSWP.04162018
- Nguyen, P., Ali, S., & Yue, T. (2017). Model-based security engineering for cyber-physical systems: A systematic mapping study. *Information and Software Technology*, 83, 116 -135. doi:10.1016/j.infsof.2016.11.004
- Paton, C. (2019). *City of Joburg, banks under cyber attack*. Timeslive: <https://www.timeslive.co.za/news/south-africa/2019-10-25-city-of-joburg-banks-under-cyber-attack/>
- Patrick, H. (2016). *Security information flow in the public sector: KZN Health and Education*. *Journal of Information Warfare*, 15, 68-85. https://www.researchgate.net/publication/312027935_Security-Information_Flow_in_the_South_African_Public_Sector
- Patton, M. Q., & Cochran, M. (2002). *A Guide to using qualitative research methodology*. *Medicins Sans Frontieres*. http://evaluation.msf.org/sites/evaluation/files/a_guide_to_using_qualitative_research_methodology.pdf
- Parsons, T. (2019). The state of web vulnerabilities, *Computer Fraud & Security*, 2019, 1, 20. doi:10.1016/S1361-3723(19)30011-9
- Paulus, T., Atkins, D. P., Macklin, R., & Woods, M. (2017). The discourse of QDAS: Reporting practices of ATLAS.ti and NVivo users with implications for best practices. *International Journal of Social Research Methodology*, 20(1), 35-47. doi:10.1080/13645579.2015.1102454
- Pettersson, R. (2010). Information design—principles and guidelines. *Journal of Visual Literacy*. 29. 167–182. Doi:10.1080/23796529.2010.11674679.
- Pretorius, M., & Ngejane, H. (2019). Best practices for establishment of a national information security incident management capability (ISIMC). *The African Journal of Information and Communication (AJIC)*, 24, 1-20. doi.org/10.23962/10539/28656
- Rashid, Y., Rashid, A., Warraich, M. A., Sabir, S. S., & Waseem, A. (2019). Case Study Method: A Step-by-Step Guide for Business Researchers. *International Journal of Qualitative Methods*, 18, 1-13. doi.org/10.1177/1609406919862424
- Ravitch, S.M. & Mittenfelner Carl, N. (2016). *Qualitative Research Design: Bridging the Conceptual, Theoretical and Methodological*. London: SAGE
- SABC News. (2017). *Cyber-attacks reaching a critical point in SA*. SABC News. www.sabcnews.com

- Schneier, B. (2014). The Future of Incident Response. *Security & Privacy, IEEE*. 12. 96-96. Doi:10.1109/MSP.2014.102.
- Sinkovics, N. (2018). Pattern matching in qualitative analysis, *The SAGE handbook of qualitative business and management research methods* (pp. 468-485). Sage Publications Ltd. https://www.researchgate.net/publication/323856200_Pattern_matching_in_qualitative_analysis
- Smit, B. (2014). Teaching Atlas.ti™ in South Africa: Reflections on doctoral preparedness, *Journal of Social Sciences*, 40:2, 213-217. doi: 10.1080/09718923.2014.11893318
- Smith, C. (2019a). *Lazarus group behind recent cyberattack on South Africa - Kaspersky*. <https://www.fin24.com/Companies/ICT/lazarus-group-behind-recent-cyberattack-on-south-africa-kaspersky-20190814>
- Smith, C. (2019b). *Major spike in SA cyber attacks, over 10 000 attempts a day - security company*. <https://www.fin24.com/Companies/ICT/major-spike-in-sa-cyber-attacks-over-10-000-attempts-a-day-security-company-20190429>
- Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333 - 339. doi:10.1016/j.jbusres.2019.07.039
- SSA. (2015). *The National Cybersecurity Policy Framework (NCPF) for South Africa*. South Africa Government Gazette. https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf
- SSA. (2020). Draft National information security governance framework. South Africa Government.
- Stoneman, P., & Gilbert, G. (2016). *Researching social life. 4th Edition*. Sage Publications. <https://uk.sagepub.com/en-gb/eur/researching-social-life/book242913>
- Sutherland, E. (2017). Governance of Cybersecurity - The Case of South Africa. *The African Journal of Information and Communication*, 20, 83 - 112. doi:10.23962/10539/23574
- Tambo, E., & Adama, K. (2017). Promoting cybersecurity awareness and resilience approaches, capabilities and actions plans against cybercrimes and frauds in Africa. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, 6(3), 126-138. doi:10.17781/P002278
- Tehrani, P., Manap, N., Taji, H. (2013). Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime, *Computer Law & Security Review*, 29,3, 207-215. doi:10.1016/j.clsr.2013.03.011
- Terrell, S. (2012). *Mixed-methods research methodologies*. The qualitative report. <http://www.nova.edu/ssss/QR/QR17-1/terrell.pdf>
- United Nations. (2018). *United Nations E-Government Survey 2018*. United Nations. https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2018-Survey/E-Government%20Survey%202018_FINAL%20for%20web.pdf

- Urgessa, W. (2019). Multilateral cybersecurity governance: Divergent conceptualisations and its origin. *The International Journal of Technology Law and Practise*. doi:10.1016/j.clsr.2019.105368
- Van Niekerk, B. (2017). An analysis of cyber-incidents in South Africa. *The African Journal of Information and Communication*, 20, 113 - 132. doi:10.23962/10539/23573
- Verizon. (2019). *2019 data breach investigations report*. Verizon. <https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf>
- Von Solms, B., & von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information and Computer Security*, 26, 2-9. doi:10.1108/ICS-04-2017-0025
- Weber, L., Rudman, R. (2018), 'Addressing the incremental risks associated with adopting Bring Your Own Device', *Journal of Economic and Financial Sciences* 11(1), a169. <http://dx.doi.org/10.4102/jef.v11i1.169>
- Williams, M., Barranco C., Motahar S., Sumi D., Monika M. (2020). A vulnerability analysis and prediction framework, *Computers & Security*, 92, 101751. doi:10.1016/j.cose.2020.101751
- Yin, R. K. (2013). Case study research: Design and methods (4th Ed.). *Canadian Journal of Action Research*, 14(1), 69-71.

APPENDIX A:

UNIVERSITY OF THE
WITWATERSRAND,
JOHANNESBURG



INTERVIEWS QUESTIONS GUIDE

Title of Research: Achieving operational resilience by aligning cybersecurity vulnerabilities, needs and responses in the provincial government

Researcher: Donovan Quinton Harris, Masters student at the University of the Witwatersrand, Johannesburg. Email: dharris@kimberley.co.za

A. Organisational profile (will not be reported against your data, only for the researcher to understand the organisational context)

- i. Please specify in which unit/directorate and in which provincial department you reside.
 - Please specify.....
.....
- ii. In which programme within the department does ICT fall?
 - Please specify.....
.....
- iii. Does executive management in your department understand and commit to the roles they need to play and assign relevant responsibilities to oversee the development and implementation of cybersecurity approaches and other security related matters?
 - Please specify.....
.....

B. Interviewee profile

- iv. What is your position within the department?
 - Government Information Technology Officer (GITO)
 - IT/ICT Manager
 - ICT Security Professional
 - Other (Please specify)
.....
.....

- v. In terms of years of experience in your current role, how would you define your employment status? (will not be reported against your data, only for the researcher to understand the organisational context)
 - At least 1 year but fewer than 3 years
 - At least 3 years but fewer than 5 years
 - At least 5 years but fewer than 10 years
 - Other (Please specify)

.....
- vi. Describe your experience in terms of your interaction with cybersecurity within your department?
 - Please specify.....

.....
- vii. Is cybersecurity one of your key performance areas in your job description as GITO / IT Manager / ICT Security/ other for your department?
 - Please specify.....

.....

C. Current cyber vulnerabilities of government information systems to external threats

1. What can you tell me about your departments position in terms of preparation against cybersecurity risks?
 - Please specify.....

.....
2. Describe if any known cyber incidents that have taken place in your department or in the NCPG?
 - Please specify.....

.....

D. Identification of cybersecurity vulnerabilities in government departments

3. How does your unit/directorate identify cybersecurity vulnerabilities in your environment?
 - Please specify

.....

4. Describe the type of cyber vulnerabilities in your environment most likely to affect your departments information systems?
 - Please specify

.....

E. Needs with respect to improving operational resilience through effective cybersecurity

5. What do you think the NC provincial government departments need to do to improve operational resilience through effective cybersecurity?
 - Please specify.....

.....
6. Effective cyber resilience needs a cybersecurity awareness program, describe your cybersecurity awareness program in your department and if your department needs to improve?
 - Please specify.....

.....
7. The key to ensuring operational resilience is having a recovery plan. To what extent is your departments recovery plan (including a business continuity plan, disaster recovery plan and incident recovery plan) needs suitable for your environment?
 - Please specify.....

.....

F. Government departments' responses to cybersecurity incidents

8. Describe how you identify and control cybersecurity risks in your department and what measures you implement to respond and mitigate risks?
 - Please specify.....

.....
9. What is the role of the departmental cybersecurity team, SITA and the GITO Council in responding to cybersecurity incidents?
 - Please specify.....

.....

10. How is the Corporate Governance Information Communication Technology Policy (CGICTP) framework, the National Cybersecurity Policy Framework (NCPF) and the department's strategic plan aligned to promote cybersecurity?

➤ Please
specify.....
.....

APPENDIX B:

UNIVERSITY OF THE
WITWATERSRAND,
JOHANNESBURG



Document Review Guide

Title of Research: Achieving operational resilience by aligning cybersecurity vulnerabilities, needs and responses in provincial government

Researcher: Donovan Quinton Harris, Masters student at the University of the Witwatersrand, Johannesburg. Email: dharris@kimberley.co.za

Documents to be reviewed:

- ICT Frameworks / Cybersecurity Frameworks / ICT Security frameworks
- ICT Policies relating to Cybersecurity / ICT Security
- Departments IT Strategic Plan / IT Plan
- Job descriptions of GITO's, IT Managers, ICT Specialists
- Auditor General and Internal Audit reports on ICT Security
- MPAT reports
- Departmental reports relating to IT Security and Cybersecurity

Document Review Questions:

G. Current cyber vulnerabilities of government information systems to external threats

- viii. How do the relevant documents rate the level of visibility of cybersecurity threats in the department?
- Very poor / Poor / Average (OK) / Good / Very good
 - Other (Please specify)
-
- ix. What do the relevant documents reveal about the type of cyber vulnerabilities most likely to affect the departments information systems?
- Social engineering (phishing) / Malware (worms; viruses; Trojans; spyware) / Hackers
 - Web vulnerabilities / Ransomware / Access Control
 - Other (Please specify)
-
- x. What are the top three cyber risks (threats and vulnerabilities) the relevant documents reveal?
- Ransomware / Virus or Worm / Trojan / Denial of Service

- Theft of devices / Phishing or Malicious emails
- Other (Please specify)

.....

xi. What do the relevant documents define as the threat actors posing cybersecurity threats to the department?

- Employees / Hacktivist / Terrorists / Hackers / Criminals from outside / Cyber Warfare
- Other (Please specify)

.....

H. Mitigation of cybersecurity vulnerabilities in government departments

xii. What do the relevant documents reveal on Cybersecurity governance implemented in the department?

- National Frameworks & Policies / Provincial Frameworks & Policies / Departmental Frameworks & Policies
- Other (Please specify)

.....

xiii. What are the main inhibitors (internal and external) that might impede on the implementation of effective cybersecurity as to relevant documents?

- Compliance / Collaboration / Risk identification / Misalignment in department
- Silo approaches / Strategic alignment / Lack of awareness / Employees / Cost
- Other (Please specify)

.....

xiv. What do the relevant documents reveal on cybersecurity frameworks / standards in the department?

- ISO/IEC 27001 & ISO/IEC 27002 / COBIT / NIST Cybersecurity framework
- NIST / IASME Governance / CIS / COSO
- Other (Please specify)

.....

xv. Relevant documents reveal what controls are in place to mitigate cybersecurity vulnerabilities in the environment?

- Firewall / Virus protection / Malware protection / Patch management / BC / DRP
- User access management / Data encryption / Password policies / System Change Control
- Risk Management / Project Management / User awareness training

- Other (Please specify)

.....

xvi. What do the relevant documents reveal on controls and measures placed in the department to mitigate Cyber-attacks that exploit the human factor?

- User awareness training / Cybersecurity culture / Educational training
- Other (Please specify)

.....

xvii. What do the relevant documents reveal on the frequency of cybersecurity awareness in the department?

- Annually / Bi-annually / Quarterly / Monthly
- Other (Please specify)

.....

I. Government departments' responses to cybersecurity incidents

xviii. What do the relevant documents reveal about the controls in the department to respond to cybersecurity incidents?

- Incident response / Event monitoring / Cybersecurity reporting
- Other (Please specify)

.....

xix. What type of intelligence does the relevant documents reveal to detect threats aimed at the environment in the department?

- Rely on IT / Rely on Staff to report / Review of audit logs / Incident event detected
- Rely on detection tools / Rely on SITA
- Other (Please specify)

.....

xx. What process do the relevant documents reveal is in place to identify critical functions and processes, information or business assets that are essential to the department?

- Rely on IT / Function allocated to an individual or unit / Rely on Committee (IT Steering, IT Strategy)
- Other (Please specify)

.....

xxi. How do the relevant documents rate the NCPG, how well do the departments communicate with each other in the case of a cyber incident? (on a scale of 1 – 5, 1 representing the lowest value)

- Very effective (5) / Somewhat effective (4) / Neutral (3)
- Somewhat ineffective (2) / Very ineffective (1)

J. Improving operational resilience through effective cybersecurity

- xxii. Do the relevant documents reveal how the department conducts cyber threat intelligence, to identify, detect, and respond to cyber threats?
- Please
specify.....
.....
- xxiii. What do the relevant documents reveal about the understanding of strategic alignment? For example, what is the purpose, who is responsible, how can it be achieved, how important is strategic alignment for cybersecurity?
- Please
specify.....
.....

APPENDIX C:

Ethics clearance certificate



SCHOOL OF Literature, Language and Media RESEARCH ETHICS COMMITTEE

CLEARANCE CERTIFICATE

PROTOCOL NUMBER: SLLM-M20-01

PROJECT TITLE

Achieving operational resilience by aligning cybersecurity vulnerability needs and responses in provincial government

INVESTIGATOR

Donovan Harris

SCHOOL/DEPARTMENT

SLLM/ ICT Policy and Regulation

DATE CONSIDERED

28 Aug 2020

DECISION OF THE COMMITTEE

Approved

This ethical clearance is valid for 2 years and may be renewed upon application.

EXPIRY DATE

Date of submission of the project report

ISSUE DATE OF CERTIFICATE

Aug 2020

CHAIRPERSON

Colleen Dawson

cc: Supervisor : Lucienne Abrahams

DECLARATION OF INVESTIGATOR

To be completed in duplicate and **ONE COPY** returned to the Chairperson of the School/Department ethics committee.

I fully understand the conditions under which I am authorized to carry out the abovementioned research and I guarantee to ensure compliance with these conditions. Should any departure to be contemplated from the research procedure as approved I/we undertake to resubmit the protocol to the Committee.

[Signature]
Signature

Date

28/08/2020

PLEASE QUOTE THE PROTOCOL NUMBER ON ALL ENQUIRIES