



University of Fort Hare
Together in Excellence

**A contingency management framework to mitigate
cybersecurity threats to electronic health records in the
public health sector in South Africa**

By

MBULELO NGXABANE

201916992



DISSERTATION

University of Fort Hare
Together in Excellence

Submitted in fulfilment of the requirement for the degree

Master of Commerce in Information Systems

FACULTY OF MANAGEMENT AND COMMERCE

at the

UNIVERSITY OF FORT HARE

Supervisor:

Professor: L Cilliers

Co-supervisor:

Mr. D Boucher

Declaration of Ownership, Authorship, and Ethical Clearance

I, Mbulelo Ngxabane, student number 201916992, hereby declare that I am fully aware of the University of Fort Hare's policy on plagiarism and I have taken every precaution to comply with the regulations. I hereby declare that this Master's dissertation is my own original work submitted to the University of Fort Hare in fulfilment of the requirements for the degree Masters: Information Systems, in the Faculty of Management and Commerce. Where other authors' works have been consulted, due acknowledgment has been given in-text and in the reference list at the end.

In addition, I affirm that I am fully aware of and have followed every precaution to be in compliance with the University of Fort Hare's policy on research ethics. I have been given ethical clearance by the research ethics committee at the University of Fort Hare, and my reference number is CIL021SNGX01.



University of Fort Hare
Together in Excellence

A handwritten signature in black ink, appearing to be 'Mbulelo Ngxabane', is written over a solid horizontal line.

SIGNED

17 November 2021

DATE

Abstract

Most developing countries in the African continent, including South Africa, seem to be lagging behind in research, policy development, and how to prevent cybersecurity threats. These findings are evident in the significant number of cyberattacks recorded in the Cost of Data Breach Study and Global Analysis by Ponemon Institute. Research studies are placing the blame on the element of portability in electronic health records (EHRs) that has contributed to numerous vulnerabilities to hospital healthcare data. As a result, the healthcare information of patients in those hospitals that are equipped with interconnected medical devices is exposed to cybersecurity threats.

The purpose of the study was to develop a healthcare contingency management framework that can be used by healthcare institutions to mitigate cybersecurity threats to EHRs in the public health sector in South Africa. The integrated systems theory (IST) which amalgamated five different theories relating to information security management was used as a theoretical foundation in this study. In achieving this purpose, the literature review was selected as the research design best suited to answer the question presented in this research study. An expert review was used to refine the framework outcome using interviews and questionnaires.

The contribution that will be made by this study will be in a form of a conceptual framework that will be used to mitigate cybersecurity threats concerning EHRs in the public health sector. The healthcare contingency management framework (HCMF) can be adopted by either the National Health Department or Provincial Health Department to be used by healthcare facilities as a guide in reviewing their support function, process management, governance management, and their contingency management.

Similar future studies need to be conducted on large scale such as in the whole public sector with the focus on the health sector.

Keywords: Cybersecurity; electronic health record (EHRs); contingency management; public healthcare, and South Africa.

ACKNOWLEDGEMENTS

In honor of those who made commitments in this journey, I would like to thank the following people:

- The almighty God for the providence, wisdom, and grace he bestowed on me. I accomplish nothing without Him, whatever I do will consistently be for the wonder of you.
- My mother for her unwavering support and prayers through the most difficult time I was going through during the time of writing this dissertation.
- Professor Liezel Cilliers for sticking with me throughout this journey. Your guidance, persistence, insight, and responsibility have made it feasible for me to finish my work. You have given me ultimatums, however, all of that was to ensure I finish my work. I will forever be indebted to you. May the Lord bless you abundantly and grant you more wisdom.
- Mr. D Boucher, your undivided support in this research study is much appreciated.
- The Information Systems Department staff for their constructive criticism during the course of this dissertation.
- My family members, especially Andile Ngxabane, for the emotional support during the most difficult time of my life – the time of writing this dissertation.
- I would also like to thank the expert reviewers who constantly provided input in achieving this milestone.
- Last but not least, my wife and kids for all the support they have given me. Often at times I would spend more time at my workstation and have no time to support them, but they proceeded to urge and support me to finish my research.



University of Fort Hare
Together in Excellence

Table of Contents

CHAPTER 1: INTRODUCTION	1
1.1 Introduction	2
1.2 Problem statement	3
1.3 Research question.....	4
1.3.1 Main research question	4
1.3.2. Research sub-questions	5
1.4 Objective of the research study	6
1.5 Significance of study	6
1.6 Literature review	7
1.6.1 Electronic health records (EHRs)	7
1.6.2 Cybersecurity	8
1.6.3 Theoretical literature	11
1.6.4 Integrated system theory	13
1.7 Research methodology	15
1.7.1 Philosophical research paradigm	15
1.7.2 Research approach	16
1.7.3 Research methods	16
1.7.4 Research design	17
1.7.5 Data collection methods.....	18
1.7.6 Primary data	20
1.7.7 Data analysis methods.....	22
1.7.8 Data trustworthiness.....	23
1.8 Delimitation of the research study	24
1.9 Ethical considerations	24
CHAPTER 2: RESEARCH METHODOLOGY	26
2.1 Introduction	27
2.2 Philosophical research paradigm.....	27
2.2.1 Positivism.....	28
2.2.2 Interpretivism	28
2.2.3 Pragmatism	29
2.3 Selecting an appropriate research paradigm.....	29
2.4 Research approach.....	31

2.4.1	Inductive approach.....	32
2.4.2	Deductive approach	32
2.5	Research methods.....	33
2.5.1	Qualitative research methods.....	33
2.5.2	Quantitative research methods.....	33
2.5.3	Mixed methods.....	33
2.6	Research design.....	34
2.6.1	Data collection methods.....	34
2.6.2	Secondary data	35
2.6.3	Primary data	38
2.6.4	Data trustworthiness.....	41
2.7	Delimitation of the research project.....	42
2.8	Ethical considerations	42
2.9	Conclusion.....	43
CHAPTER 3: LITERATURE REVIEW.....		44
3.1	Introduction	45
3.2	Cybersecurity overview in South Africa.....	46
3.3	Lack of information security in healthcare facilities.....	46
3.4	Information security legislation in South Africa.....	48
3.4.1	The Electronic Communications and Transactions Act.....	49
3.4.2	The Protection of Personal Information Act (POPIA).....	49
3.4.3	The National Cybersecurity Policy Framework	50
3.5	Introduction to maturity models.....	52
3.5.1	Importance of maturity models.....	52
3.5.2	The Cybersecurity Capability Maturity Model (C2M2) architecture	54
3.5.3	Cybersecurity Maturity Model (CMM)	58
3.5.4	The threats landscape	61
3.6	Theoretical framework	64
3.6.1	Protection motivation theory (PMT).....	64
3.6.2	Integrated system theory (IST) background	66
3.7	Conclusion.....	74



CHAPTER 4: CONTINGENCY MANAGEMENT FRAMEWORK FOR CYBERSECURITY	76
4.1 Introduction	77
4.2 Cybersecurity initiatives in developed countries	77
4.3 United States cybersecurity framework (US CSF)	79
4.3.1 The framework core	79
4.3.2 United States cybersecurity framework implementation tiers	83
4.4 The Australian cybersecurity perspective	86
4.4.1 Australia’s cybersecurity strategies	86
4.5 Canada’s cybersecurity	91
4.5.1 Implementing the strategy.....	92
4.6 Turkey’s cybersecurity.....	94
4.6.1 The engagement model.....	95
4.6.2 Cyber security strategies in Turkey	95
4.7 Findings from comparative analysis	98
4.7.1 Security policy	98
4.7.2 Risk management.....	99
4.7.3 Internal control.....	99
4.7.4 Information auditing	100
4.8 Conclusion.....	100
CHAPTER 5: CONCEPTUAL FRAMEWORK.....	102
5.1 Introduction	103
5.2 A recap of Cybersecurity and EHR initiatives	104
5.2.1 The United States cybersecurity blueprint.....	104
5.2.2 The Australian cybersecurity blueprint.....	105
5.2.3 The Canadian cybersecurity blueprint	106
5.2.4 Turkey’s cybersecurity blueprint	106
5.3 Proposed conceptual framework	108
5.3.1 Proposed South African HCMF Tiers.....	110
5.3.2 Expert review	120
5.4 Conclusion.....	127
CHAPTER 6: CONCLUSION	128



University of Fort Hare
Together in Excellence

6.1	Introduction	129
6.2	Research problem.....	129
6.3	Research question.....	130
6.4	Research methodology	132
6.5	Contribution made by this study	134
6.6	Limitations and recommendations for future research.....	135
6.7	Conclusion summary.....	135
	Reference List.....	136
	Appendix A: Ethical clearance.....	158
	Appendix B: Proof reader certificate.....	160
	Appendix C: Turnitin report.....	161
	Appendix D: Expert review questionnaire.....	162



University of Fort Hare
Together in Excellence

List of Figures

Figure 1: Cybersecurity Maturity Model	12
Figure 2: Integrated System Theory	14
Figure 3: Literature review	18
Figure 4: Continuum of Core Ontological Assumption.....	30
Figure 5: Literature review	35
Figure 6: Model and domain elements.....	53
Figure 7: C2M2 Domain elements.....	55
Figure 8: Cybersecurity capability maturity model levels.....	56
Figure 9: Cybersecurity Maturity Model	59
Figure 10: Ransomware attacks in 2020 around the world.....	63
Figure 11: Protection motivation theory	65
Figure 12: Integrated System Theory	67
Figure 13: Framework core structure.....	80
Figure 14: Cybersecurity incidents	90
Figure 15: Proposed Healthcare Contingency Management Framework (HCMF)	110
Figure 16: Final Healthcare Contingency Management Framework (HCMF).....	125

List of Tables

Table 1: Details of Expert Participants in the Study	22
Table 2: Applying research philosophical paradigm to the study.....	31
Table 3: Search key terms.....	37
Table 4: Details of Expert Participants in the Study	40
Table 5: Summary of expert reviewers	121
Table 6: Concerns and responses	123
Table 7: Search key terms.....	133

CHAPTER 1: INTRODUCTION



1.1 INTRODUCTION

One of the government's mandates towards its citizens is to promote and improve the quality of public healthcare services that are specifically directed to patient needs (Katuu, 2019). The establishment of the e-health infrastructure forms a fundamental building block in transforming the South African healthcare sector (Kgabo, 2017). E-health provides current information for decision-making by healthcare workers about the health outcomes for patients (Izaara, Ssembatya, & Kaggwa, 2019). Therefore, electronic health records (EHRs) provided the means to promote and improve patient safety (Shah & Khan, 2020).

Granja, Janssen, and Johansen (2018 p. 2) refer to EHRs as “*a record in digital format that is capable of being shared across different healthcare settings, by being embedded in network connected enterprise-wide information systems*”. The record stores healthcare data that is relevant to the patient and includes medical history, laboratory test results, radiology images, demographics, medication and allergies, immunisation status, and billing information (Kleynhans, 2011). They are usually managed and maintained by an agent or third party, e.g. hospital or medical insurance company, over a period of time (Katurura & Cilliers, 2017).

The collection of healthcare data in one database creates an effective communication pathway amongst patients and healthcare facilities (Els & Cilliers, 2018). However, despite the advantages associated with EHRs, Thomas (2016) reveals that these advancements come along with privacy and security issues. Cybersecurity is concerned with safeguarding computer networks with access to the internet against intrusions and maintaining the confidentiality, availability, and integrity of information (Coventry & Branley, 2018). Conversely, recent research focusing on cybersecurity suggests that most data breaches concern healthcare data (Flahault et al., 2018).

News24 (2019) reports malware attacks compromising healthcare data in South Africa increased by 22% in the first quarter of 2019 compared to the first quarter of 2018. The Verizon Data Breach Investigations Report (DBIR) states more than 52% of breaches occurred due to hacking, 28% involved malware and 33% included phishing or social engineering respectively. Flahault (2018) explains in his research study that EHRs are the reason for these occurrences and when they are breached, hospital operations are compromised and patients' lives at risk.

In view of the risks that accompany the ever-increasing reliance on information security, Zastepa, Sun, Clune, and Mathew (2020) find contingency management in the healthcare sector

as a solution to information security. Other than the prevention, detection, and reaction to threats and vulnerabilities, contingency management includes one or more management activities in an organisation (Williams, Ashill, & Naumann, 2017). Continuous development and change are found to be increasing in the legislative environment in South Africa (SA) (Els & Cilliers, 2018).

Amongst others, South Africa (SA) has introduced and applied the National Cybersecurity Policy Framework (NCPF), Protection of Personal Information Act (POPIA), and the Electronic Communication and Transaction Act (ECT) in an attempt to address the security and privacy concern in EHRs. However, this is not enough to mitigate cybersecurity threats in EHRs. Therefore, the adoption of a contingency management framework to mitigate cybersecurity threats in EHRs is considered a contributing factor in the healthcare public sector in South Africa. The following section explains the problem statement and the research question.

1.2 PROBLEM STATEMENT

The proposed implementation of the SA National Health Insurance (NHI) is a reflection of universal healthcare improvement that is consistent with the global vision to improve the accessibility of quality healthcare services (Weeks, 2014). One of the proposed cornerstones of the South African NHI is an EHR system that can identify patients and provide easy access to their health information for decision-making by healthcare workers (Cilliers & Katurura, 2018).

However, advancements in healthcare technology as a whole threaten to expose patient information to new risks that compromise the health and well-being of patients (Flahault et al., 2018). Charlotte Maxeke Academic Hospital in Johannesburg is an example of a South African facility where patients' lives were threatened by a system-wide shut down after a ransomware cyberattack that demanded a bitcoin ransom (News24, 2019). As a result of these ransomware attacks, News24 (2019) presents medical practitioners as unable to access patients' medical records and patient schedules.

For the past decade, South African healthcare facilities equipped with interconnected medical devices using EHRs to exchange or store patient information have experienced cybersecurity threats and vulnerabilities (Flahault et al., 2018). The explosion of internet connectivity to

existing computer networks has resulted in medical devices being exposed to new cyberspace. The State Security Agency has since declared that South Africa is under cyberattack (South African Government, 2015). Hackers' most important information, according to the Ponemon Institute (2016), is related to patients' records. Van Niekerk (2017) indicates that there has been an increase in the number of cyberattacks and medical identity theft with millions of medical records stolen globally.

Van Niekerk (2017) further estimates that ZAR 3.7 billion of indirect losses and ZAR 6.5 billion of direct cost in financial losses from cyberattacks have occurred in the healthcare sector. According to Leppan (2017), South Africa's cybersecurity threats are taking place at a critical stage in the country. It has been reported that South Africa's financial losses are estimated to be approximately ZAR50 billion due to illegal cyber incidents involving online personal records (Van Niekerk, 2017).

In light of the above research problem, the objective of this research study was to develop a conceptual framework that can be used to mitigate cybersecurity threats to EHRs in the public healthcare sector in SA. The section below outlines the research questions that needed to be addressed in order to respond to cybersecurity threats to EHRs in the public health sector in South Africa.


University of Fort Hare
Together in Excellence

1.3 RESEARCH QUESTION

In order to address the problem identified in this study, the following research questions were formulated.

1.3.1 Main research question

This section provides the main question of this research study. It also outlines and explains the three sub-questions formulated to aid in answering the main research question:

How can contingency management of electronic health records mitigate cybersecurity threats in the public health sector of South Africa?

1.3.2. Research sub-questions

The main research question above has been answered through the following sub-questions:

How can cybersecurity threats compromise electronic health records in the public health sector in South Africa?

The issue of patient safety has been the focus of the global healthcare industry with many institutions or countries initiating some form of EHRs (Van Niekerk, 2017). This sub-question aimed to investigate cases of patients' information being compromised during cybersecurity threats as a result of the vulnerability of primary healthcare facilities. When a primary healthcare facility has no access to patient records, medical history reports, drug information, and patient discharge summaries due to ransomware attacks, the result could be catastrophic in patient well-being (Onuiri, Idowu, & Komolafe, 2015).

Kremer and Müller (2013) posit that the protection of EHRs is so important it has become a major concern around the globe. Flahault (2018) proposes the view that EHRs include data that is highly sensitive and valuable to both the hospital and the patient. Once a patient's EHR is compromised or stolen, health information is available for a range of crimes leading to patients' lives at risk.



University of Fort Hare

How can contingency management safeguard information in electronic health records against cybersecurity threats?

Hong, Chi, Chao, and Tang (2003) posit that contingency management is activities that originate from security management and proceed sequentially from security policy, risk management, internal control, and information auditing. To safeguard information in EHR, South African legislative defined policies and procedures including the Protection of Personal Information Act, Minimum information Security Standard as measures to protect its citizens from acts of theft and potential sabotage (South African Government, 2015). However, adherence to policies is voluntary and failure to comply with some of these policies will fundamentally increase the chances of crime. Healthcare contingency management can safeguard EHRs in the public healthcare sector.

How can a framework assist with the contingency management to secure electronic health records against cybersecurity threats in the public health sector in South Africa?

According to SABC News (2017), cybersecurity threats are taking place at a critical stage in SA. This is a result of interconnected medical devices that introduce numerous vulnerabilities and increase hospital exposure to cybercrime. According to the State Security Agency (2015), the South African National Policy Framework (NCPF) was developed in 2012 to promote a cybersecurity culture and to ensure the confidentiality, integrity, and availability (C-I-A) of health information systems to mitigate intentional and non-intentional incidents and attacks. The framework that was developed (in this study) can be used as a guide in hospitals to assist healthcare practitioners to ensure the protection of healthcare records against cybersecurity threats.

1.4 OBJECTIVE OF THE RESEARCH STUDY

- i) Investigate cases of patients' information compromised during cybersecurity threats due to vulnerability of primary care facility;
- ii) Explore strategies that could be applied by contingency management to safeguard information in electronic health records;
- iii) Develop a contingency management framework to assist to secure EHRs against cybersecurity threats in the public health sector in South Africa.

1.5 SIGNIFICANCE OF STUDY

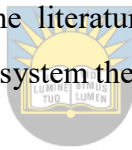
Most developing countries in the African continent, including SA, seem to be lagging behind in research, policy development, and how to prevent cybersecurity threats (Jaquire & Von Solms, 2015). These findings are evident in the significant number of cyberattacks recorded in the Cost of Data Breach study, Global Analysis by Ponemon Institute (Ponemon Institute, 2019). Research studies are placing the blame on the element of portability in EHRs that has contributed to numerous vulnerabilities to hospital healthcare data (Coventry & Branley, 2018).

As a result, the healthcare information of patients in those hospitals that are equipped with interconnected medical devices is exposed to cybersecurity threats (Flahault et al., 2018). As pointed out by Flahault (2018) when discussing the challenges and risks of cybersecurity in hospitals, the researcher identified that once these EHRs are stolen, the information found in them can be widely used for a range of crimes from identity theft to medical fraud.

The SA National Development Plan (NDP) has also made it clear that advancement and usage of cybersecurity are required to address various cyberattacks launched in recent years against the healthcare sector (Mohammed & Musa Bade, 2019). The contribution to be made by this study is in the form of a conceptual framework that can be used to mitigate cybersecurity threats concerning EHRs in the public health sector. The healthcare contingency management framework can be adopted by either the National Health Department or Provincial Health Department to be used by healthcare facilities as a guide in reviewing their support function, process management, governance management, and their contingency management.

1.6 LITERATURE REVIEW

The proliferation of the internet in the past 40 years has disrupted the healthcare sector through the digitalisation of information for greater accuracy and quality in the delivery of health services. Moreover, the growth of health information technology and e-health has allowed cybercriminals an opportunity to exploit healthcare data for their own ends (Jaquire & Von Solms, 2015). The areas of focus in the review of literature include cybersecurity and EHRs in the healthcare sector. A review of the literature was conducted using the Cybersecurity Maturity Model (CMM) and integrated system theory of information security management that underpins the study.



University of Fort Hare

in Excellence

1.6.1 Electronic health records (EHRs)

The emergence of electronic health (e-health) in the healthcare sector was meant to answer issues of increased growth of the human population which entailed challenges to health practitioners who deal with large quantities of health information (Hilma Inoukapo, 2014). E-health strategies developed in various countries including South Africa revealed a trend toward digital transformation in healthcare service (Angst & Agarwal, 2009). For example, New South Wales in Australia indicated that there is a massive opportunity for digital technologies to change how healthcare is operating and this has been progressively recognised around the country and the world at large (eHealth NSW Government, 2016).

South Africa joined the new developments and initiated a project in May 2002 to implement EHR country-wide (Thomas, 2016). Additionally, other countries, such as the United States of America developed the American Recovery and Reinvestment Act (ARRA) to enforce the adoption and implementation of EHRs by all healthcare organisations (Kessler & Hitt, 2016). Further precautionary measures were stipulated in ARRA that mandated penalties for non-compliance (Izaara et al., 2019). Electronic health records are found to be the most important

asset in the healthcare sector as a result of the valuable information they contain, including personally identifiable information (PII) (Le Bris & El Asri, 2021). In addition, these records can be used to analyse health information systems to improve the effectiveness and efficiency of healthcare delivery (Cilliers, & Wright, 2017).

Within the growing context of the digital transformation in healthcare service, EHRs are an important innovation that have opened a whole range of new possibilities including sharing safety within the healthcare sector (Nunu, 2019). These records are usually maintained by the provider over time and may include all of the key administrative clinical data under a particular provider, including demographics, progress notes, problems, medications, past medical history, laboratory data, and radiology reports (Burke, Oseni, Jolfaei, & Gondal, 2019). Furthermore, they can improve healthcare quality, improve accessibility and reduce cost (Chao, Hu, Oi, and Ung, 2015).

Kleynhans (2015) indicates that countries must adhere to legal requirements such as confidentiality and retention of patient information. However, despite the significant advancements that EHRs offer to the healthcare sector, there is widespread concern that cybersecurity threats are placing the health and well-being of patients at risk. Le Bris and Asri (2017) suggest that healthcare organisations are the most trusted entities, but are also the most vulnerable environment for patient information. For example, the case of Charlotte Maxeke Academic Hospital where patients' lives were threatened by a system-wide shutdown after a cyberattack demanded a Bitcoin ransom (News24, 2019).

Speaking at the Hospital Association of SA's annual conference in Cape Town, head of enterprise architecture at Netcare and a pioneer in medical device software suggested that the main purpose of criminal hackers of healthcare technology was identity theft (News24, 2019b). In order to assess the healthcare sector's cybersecurity threats to EHR in South Africa, it is important to understand how the information security professionals are dealing with these challenges.

1.6.2 Cybersecurity

Electronic healthcare technology has been recognised as having the potential to extend, save and enhance lives in SA (Jaquire & Von Solms, 2015). However, it has been noted that there are increasing concerns relating to the security of healthcare data that threaten the well-being of patients (Coventry & Branley, 2018). As a result, cyberspace has become a place of cybercrime starting from across the borders of our county to abroad. Sutherland (2017) put

forward the view that governments globally have growing concerns with the increasing ubiquity of social networks and so much reliance on digital technology. Still, government legislation is yet unable to address the issue of cybersecurity threats.

Cyberspace refers to a national platform in which communication over computer networks occurs (Bay, 2016). Jaquire (2015) refers to cyberspace as a dynamic global platform with cyber-related matters being a global concern. Bucea-Manea-Tonis and Tonis (Bucea Manea, 2017) put forward assertions that cyberspace is found to have triggered a series of economic, social, and political adjustments worldwide.

The available evidence seems to suggest that the term cybersecurity is mostly used to protect against malware and hacker attacks (Bay, 2016; Leppan, 2017). Cybersecurity is further found to be apprehensive of the safeguarding of computer networks against intrusions and maintaining the confidentiality, availability, and integrity of information (Bellekens et al., 2015; Coventry & Branley, 2018). The healthcare sector is currently one of the most targeted through cybersecurity vulnerabilities (Coventry & Branley, 2018). These findings are evident in IBM's Security Cost of Data Breach Report released in 2019, where medical identity theft increased by 12% compared to 2018 (Ponemon Institute, 2019). Furthermore, Mimecast recently conducted a survey "State of email report" in 2019, which presented a 30% likelihood that organisations across the board are experiencing major data breaches (Nathan & Scobell, 2012).

According to Le Bris and Asri (2017) and Kortjan (2013), cybersecurity threats in the healthcare sector are found to be divided into two categories, i.e. targeted attacks and untargeted attacks. Both targeted attacks and untargeted attacks can be performed using cybersecurity technologies. Targeted attacks are hackers intentionally looking for specific assets to blackmail using information from EHR to generate financial gains that are better than selling in the black market (Le Bris & Asri, 2017). A determined attacker will use many ways of hacking that are significant to gain targeted information, and will not give up regardless of the challenges encountered during a penetration attack of the systems (Le Bris & Asri 2017). For example, when an attacker's focus is on EHR, they target both the available number of EHRs in a facility and the information systems used to traverse the EHR.

On the other hand, untargeted attacks are not specific to particular assets, but rather they choose the targets that will increase and maximise their gains (Leppan, 2017). For example, Kortjan (2013) explains that untargeted attacks can be directed toward patients in a hospital. Both

targeted and untargeted attacks include viruses such as worms, ransomware, Trojan horses, denial of service (DoS), cyber-theft attacks, and hacking into healthcare information systems (Le Bris & El Asri, 2021).

Ransomware is regarded as the most popular form of cyberattack targeting hospitals in SA (Le Bris & El Asri, 2021). These findings are evident in the Verizon, (2019) Data Breach Investigations Report (DBIR), where malware and ransomware attacks compromised healthcare data in SA during the year 2019 and continue to make headlines. An example was a ransomware cyberattack at Charlotte Maxeke Academic Hospital in Johannesburg, South Africa, where patients' lives were threatened by a system shutdown (News24, 2019). A ransomware attack on the National Health System Hospitals in the United Kingdom forced the rerouting of ambulances to unaffected hospitals and delayed inpatient treatment plans due to no access to the hospital information system (Flahault et al., 2018). Many types of services in hospitals can be threatened by a cyberattack and can include targeting automated systems managing drug dispensers to automated drug deliveries. Sobers (2019) reports that these breaches exposed 4.1 billion global healthcare records in the first six months of 2019.

In response to cybersecurity threats and challenges, the South African legislative context relating to security and privacy breaches is notable for gaining momentum in protecting its citizens (Ross, 2017). These findings are evident from the South Africans National Development Plan (NDP) where advancement and usage of cybersecurity are required to address various cyberattacks launched in recent years against the healthcare sector (National Planning Commission, 2015). However, adherence to policies is voluntary and failure to comply with some of the recommendations fundamentally increases the chances of crime, threatening patient lives. The National Health Insurance (NHI) regulatory framework was also developed to improve the accessibility of quality healthcare services for all South African citizens (South African National Department of Health, 2017).

The increasing dependence of the healthcare sector on information and communication technology (ICT) at all levels is changing how health organisations conduct their business (Kremer, & Müller, 2013). Jaquire (2015) blames this increase on the emergence of the internet which has transformed how the healthcare sector delivers its services and how cybercriminals use cyberspace to commit acts of crimes. It is evident that there is a need for proper cybersecurity measures as a result of the increasing number of cybersecurity breaches (Bissict, 2016).

1.6.3 Theoretical literature

The research project is defined by theoretical models that describe the boundaries and anchors of the research study. In order to mitigate cybersecurity threats to EHRs in the public health sector in SA, the study employed the CMM and the IST for information security to theoretically inform the development of a contextual framework for public healthcare in South Africa. The following section briefly discusses the CMM.

1.6.3.1 Cybersecurity Maturity Model (CMM)

The CMM is a four-level based cybersecurity maturity model similar to the United States NIST cybersecurity framework designed to evaluate organisation readiness in responding to adverse events, and according to Till (2019), was developed by Nemertes Research group. The fundamental idea of CMM is to identify gaps in organisations equipped with cybersecurity technologies and to develop improvements to protect the information systems asset by making use of CMM maturity levels.

In addition to that, the CMM model was designed as a tool to determine the state of cybersecurity level in an organisation and to define strategies that will explain how cybersecurity systems operate. Furthermore, this model was developed to determine the state of the organisation and actions to prevent the exploitation of weaknesses in the future (Le & Hoang, 2017a). The model focuses on levels of incremental maturity in cybersecurity from level 0 to level 3.

According to Mohammed and Bade (2019), metric levels set in the Cybersecurity Maturity Model are a slightly simplified version of the National Institute of Standards and Technology (NIST) cybersecurity framework approach, but will not fit well with organisational issues that relate to cybersecurity. Figure 1 below depicts the CMM model.

Cybersecurity maturity model



Figure 1: Cybersecurity Maturity Model

(Till, 2019)

1.6.3.2 Brief description of CMM maturity levels

In Figure 1, *Unprepared*, level 0, is where the organisation lacks resources such as humans, processes, and technologies to address cybersecurity vulnerabilities and threats (Le & Hoang, 2017a). For example, according to the South African readiness report by the Department of Telecommunications and Postal Services (2017), only 28% of organisations had a Chief Information Security Officer (CISO), with 27% of organisations having a Chief Technology Officer (CTO). Furthermore, reports indicate that some organisations have failed to implement basic technologies, such as basic firewalling, anti-malware, and some organisations even failed to conduct regular cybersecurity awareness (Bob, Padayachee, Gordon, & Moutlana, 2017).

Reactive, level 1, refers to an organisation that has basic platforms and structures to respond to and handle organisational cybersecurity threats effectively (Le & Hoang, 2017). For example, this includes organisations that are above level 0 (unprepared) with basic resources such as information technology officers like Chief Information Security Officer (CISO) responsible for cybersecurity, implementing incident response policies, conducting awareness training, monitoring firewalls, and putting anti-spam email measures in place (South African Government, 2015). According to the South African Cybersecurity Readiness report conducted in 2017, 37% of companies have discussed basic requirements for cybersecurity, as a cybersecurity plan/strategy and will implement it in the future (Department of Telecommunications and Postal Services, 2017).

Proactive, level 2 – many of the organisations at this level of maturity are found to have implemented some of the security best practice frameworks, such as NIST Cyber Security Framework for Critical Infrastructure (CSF) or Cybersecurity Capability Maturity Model (C2M2) (Van Niekerk, 2017). These organisations have the technology, people, and processes in place to protect them against unexpected attacks from known sources (Kortjan, 2013). In a survey conducted by the South African Cybersecurity Readiness report in 2017, most organisations in the proactive level 2 of the CMM model are found in the private sector and constitute only 7% of the overall organisations (Department of Telecommunications and Postal Services, 2017).

Anticipatory, level 3, can also be compared to level 5 (Vanguard) in the Community Cyber Security Maturity Model (CCSMM) where an institution has multiple resources that include people, processes, and technology to guard against vulnerabilities and threats that could result due to changes in the business and technology environment (Mohammed & Bade, 2019). For example, a majority of organisations are unable to identify what critical assets are needed for the functioning of the organisation (Le & Hoang, 2017). The following section briefly describes the structure of the integrated system theory.

1.6.4 Integrated system theory

Even though the internet offers plenty of information on security research, it has become a common understanding that information security management studies are found in the literature. In tackling cybersecurity issues, understanding why organisations are being attacked, this study depended on existing theories where both the protection motivation theory (PMT) and information security policy (ISP) had interesting views on issues of security prevention. However, the IST construction had better advantages that are founded on multiple theories including, information security policy, risk management, internal control, and information auditing theories (Hong et al., 2003). Furthermore, since it is based on contingency management, this theory puts more emphasis on organisational objectives (Hong et al., 2003). As shown in Figure 2, the integrated system theory includes other theories.

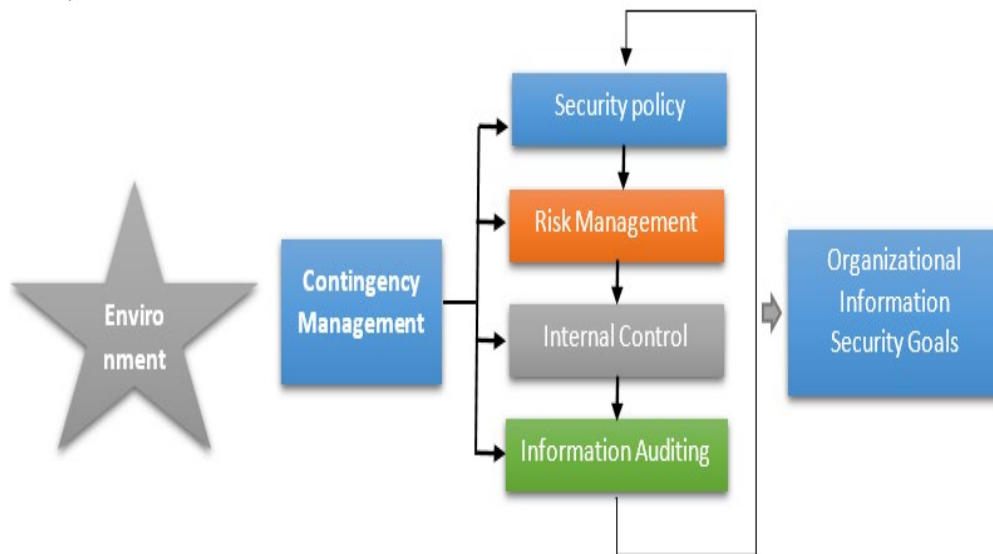


Figure 2: Integrated System Theory

(Hong et al., 2003)

The first part of the theory addresses the environment, with Coventry and Branley (2018) stating that the healthcare environment is targeted and exploited by hackers for financial gain. Kremer and Müller (2013) refer to cyberspace as an “*environment that has triggered a series of social, economic and political arenas*”. The environment part in the figure is represented by a star sign as it signifies the overall healthcare environment in an institution. For this study, the healthcare sector comprised the environment under scrutiny with the intention of protecting it against adverse events through the proposed conceptual framework.

The second part of the theory focuses on contingency management, defined by Hong et al. (2003) as requirements to meet the demands of fast-changing environments. Other researchers define contingency management as the activities that originate from security management and proceed sequentially from security policy, risk management, internal control, and information auditing (Cukier, 2007; Moeti & Kalema, 2014). The main theoretical premise behind the IST theory, as far as this research study is concerned, is the organisational information security goals, where according to Hong et al. (2003) the theory evaluates the organisation in terms of its security scope, parsimony, and accuracy of explanation and the precision of prediction. Hong et al. (2003) further propose that this theory be used with other studies to produce more accurate predictions.

Moody, Siponen, and Pahnla, (2018) discuss the sequential part of the IST theory, saying that the information security policy theory objective is designed to form consensus in an organisation by planning information security, drafting, and implementing the policy, and reviewing it on a regular basis. Jaquire (2015, p. 28) describes information security policy as a comprehensive policy document that outlines the areas of concern that are a risk and a threat to the security of an organisation.

In summary, this research study made use of the CMM and IST to evaluate cybersecurity threats to EHRs in South Africa. The two models were integrated to identify gaps and to develop a contingency management framework for public healthcare in South Africa.

1.7 RESEARCH METHODOLOGY

Research methodology is an organised manner to answer a research problem; it is a process of finding out about a phenomenon by systematically examining its attributes and merits (Burns & West, 2000; Mouton, 1996). Based on the objective of this study, which was to develop a conceptual framework that will be used to mitigate cybersecurity threats to EHRs in the public health sector in South Africa, this section outlines how this study aimed to achieve this. Collis and Hussey (2009) posit that each research project must have a research paradigm and research methodology that guide the construction of the study to be conducted. This research study made use of a research paradigm, approach, methods, and techniques. The following section discusses the philosophical research paradigm adopted by the research study.

1.7.1 Philosophical research paradigm

It is important for a research study to follow a specific research paradigm (Collis, & Hussey, 2013). Most research studies describe a research paradigm as a model that seeks to develop and verify theories about how the research project should be conducted (Bissiet, 2016; Murire, 2016). In Information Systems and Technology (IS/IT) studies, there are two philosophical assumptions, positivism and interpretivism which can be applied to a study (Collis, & Hussey, 2013).

The interpretivist study works from the hypothesis that there are numerous real factors and researchers seek to comprehend the participants' idea (Graff, 2014). In an interpretive research project, the aim is not to prove the hypotheses as is the case with positivist research, but rather, it seeks after to distinguish, investigate and clarify how related and reliant the variables in a social setting are (Oates, 2006; Klein & Myers, 1999).

Since the aim of this research study was to develop a conceptual framework that will be utilized to mitigate cybersecurity threats to EHR in the public health sector in SA, interpretivism was adopted as the research paradigm. Using this approach aided the researcher in investigating the opinions of experts in the domain of security, cybersecurity, and the EHRs in the healthcare sector in order to address identified cybersecurity threats.

1.7.2 Research approach

The research approach according to Bilau, Witt, and Lill, (2018) is concerned about how the researcher connects and figures out the data collected. The research approach followed by the researcher is affected by their ontological and epistemological position (Hothersall, 2019). Thus, the use of the methodology chosen ought be aligned with the objectives of the research project. Two approaches can be applied, namely inductive and deductive approaches.

Saunders et al. (2007) posit that the inductive approach is a theory created from the perception of exact reality and gives a superior comprehension of the nature of the problem. Collis and Hussey (2013) depict the deductive approach as the formation of reasonable and theoretical structures which are tested by experimental perception.

The deductive approach usually looks to test hypotheses through the use of previous or pre-created suggestions to a phenomenon (Rahman, 2015). Liu and Zhang (2015) state that the inductive approach is connected with qualitative investigations wherein the researcher both depicts and interprets a phenomenon they have seen within its specific setting. A deductive approach for the most part looks to test theories through the use of foregoing or pre-created suggestions to a phenomenon (Rahman, 2015).

In order to arrive at a conclusion of the research study based on information assumed, the researcher utilised the inductive reasoning method. An inductive reasoning approach allows the research to construct new theories to arrive at generalisation (Golden-Biddle & Locke, 2007). The next section discusses the methods that were used in this research study in order to complete the research.

1.7.3 Research methods

In research, the tools used for collecting and analysing data are referred to by Collis and Hussey (2009) as research methods. Mkhomazi and Iyamu (2013) posit that there are three approaches that are normally used in research, namely qualitative, quantitative and mixed methods. Kothari

(2004) explains that the qualitative and quantitative approaches are ordinarily utilised in IS/IT research. Brannen (2017) posits that the qualitative method influences the natural scientific method in the human behavioural study which is exclusive to what can be measured and observed objectively. Collis and Hussey, (2013) posit that quantitative methods are generally popular in the research field for testing a theory and hypothesis and are specifically used in the positivist paradigm. However, once the two methods are used in combination they are referred to as mixed method which can likewise be utilised in a research study (Oates, 2006; Graff, 2014). Oates (2006) agrees with the notion that the mixed-method approach encompasses both quantitative and qualitative data collection methods in a research study.

The research method used for this was a qualitative research method in order to properly respond to the questions raised in this study. Cassell and Symon (2004) define the qualitative research approach as a method that seeks to describe and explain, explore and interpret how people perceive a phenomenon based on their experiences. Quantitative methods are concerned with numerical values and require precise measurement of constructs (Murshed & Zhang, 2016). The following segment examines the design approach of this research study.

1.7.4 Research design

Research design “*is the conceptual structure within which research is conducted, constituting the blueprint for the collection and analysis of data*” (Gill & Chew, 2018, p. 251). Thus, a research design must be sufficiently built to respond to the research problem or research question (Mouton, 2001). Creswell (2009) states that the research design is an association between the research question and the actual execution of the research.

There are various research designs related to qualitative research, amongst which is the literature review (Smith, Busi, Ball, & Van Der Meer, 2019). Because of the diversity of literature that now saturates the information security discipline, it is imperative for a researcher to choose the most suitable research design to suite their research study.

Using the literature review allowed the researcher of this study to map existing literature that could apply to the research question. An expert review was used to refine the framework outcome. Figure 3 below is a graphic presentation of a literature review that was adopted in this research study.

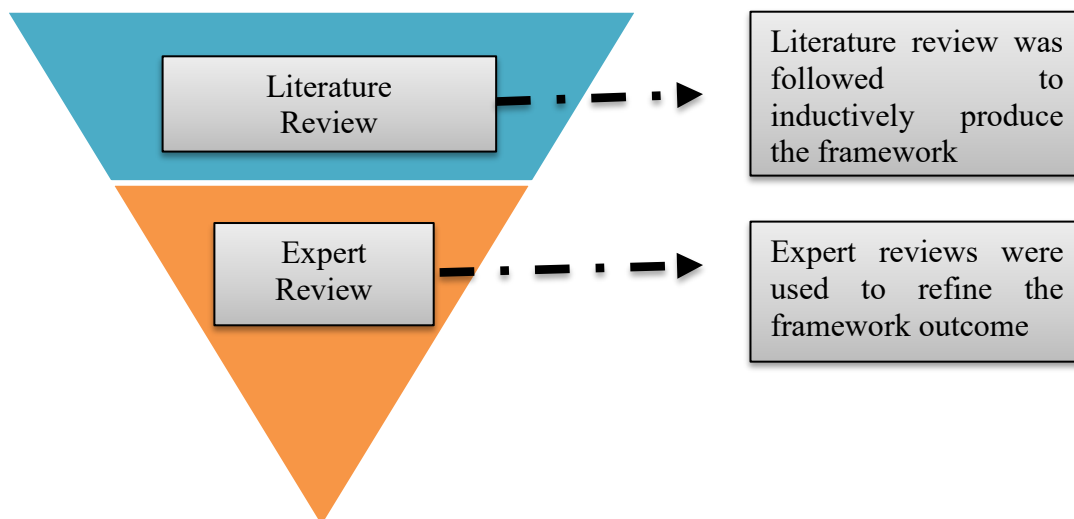


Figure 3: Literature review

1.7.5 Data collection methods

Data collection is a significant piece of the examination cycle which, according to Höpken, Eberle, Fuchs, and Lexhagen (2019), “*provides a trade-off between breadth and depth, and between generalizability and targeting to specific (sometimes very limited) population*”. Interviews, observation, and documentation are found to be the most frequently used techniques to collect data in qualitative research studies (Lewis, 2018). In line with the objective of this study, which was to develop a conceptual framework to mitigate cybersecurity threats to EHR in the public health sector in South Africa, the study made use of a literature review to draw information from existing knowledge. According to Woo, Pettit, Kwak, and Beresford (2011), the literature review can be useful when drawing from existing literature that could apply to the research question (Munyarandzi, 2018). To identify the gap in cybersecurity literature, existing knowledge related to cybersecurity and electronic health records was used to develop a framework.

1.7.5.1 Secondary data

According to the Management Study Guide (2013), secondary data is referred to as data collected for a purpose other than the study in question and is data that can be obtained from other sources. In this study, secondary data was obtained by conducting a step-by-step literature review in phases. Massaro, Dumay, and Guthrie (2016) state that most researchers use a literature review to draw and assess the present information to identify future research needs. The literature review can yield better results when it is done thoroughly and follows a predetermined protocol (Armitage & Keeble-Allen, 2008). Additionally, the literature review

was broken down into three main phases: i) planning, ii) conducting, and iii) reporting the results of the literature review (Dumay, Bernardi, Guthrie, & Demartini, 2016).

Phase 1 – Planning

According to Salkind (2010), planning in research is an applied investigation designed to respond to an inquiry using empirical observation. The first phase involved planning the review and was further broken down into the five-step approach as follows:

- i) *Identification of the need to review* – literature specific to both the domain of cybersecurity and that of EHR in the public healthcare sector in SA was reviewed with the objective to develop a contingency management framework for use in mitigating cybersecurity threats to EHRs in the public health sector in SA.
- ii) *Commissioning a review* – the goal of this step was to develop an investigated literature review from step one that could be used to craft the framework that can be used to mitigate cybersecurity threats to EHRs in the public health sector in SA.
- iii) *Specifying the research questions* – attempting a literature review is mostly aligned to a research problem. Section 1.3.1 of this research study is the formulation of a research question that sought to answer the research study. The research question was further broken down into individual components that were investigated in order to answer the main research question of the study.
- iv) *Developing a review protocol* – this step was very important as it outlined exactly how each step was being carried out. This step was also beneficial in ensuring the researcher's bias was minimised as well as documenting each step of the process which is vital for the replicability of the study. At this step, a review protocol document was developed documenting the protocol to be followed.
- v) *Evaluating the review protocol* – at this step, to ensure the effectiveness of the collected sources, the review document was shared amongst expert reviewers for evaluation.

Phase 2 – Conducting the review

With the developed plan in hand, it was now possible to conduct an actual review of the literature. This stage comprises of five stages: i) identification of research, ii) selection of primary studies, iii) study quality assessment, iv) data extraction and monitoring, and v) data synthesis (Armitage & Keeble-Allen, 2008).

- i) *Identification of research* – the goal of this step was to retrieve all the literature relevant to the research study. Due to the COVID19 pandemic, the University library could not be visited. However, the researcher accessed the following online Subscription Databases at the University: the ACM digital library database, IEEE Xplore database, ISI web of knowledge database, Science Direct database, as well as the university online book lending facility, the OPAC system to gather information. The review protocol document was used to maintain the ledgers for all the online databases, search terms, and phrases for purposes of replicability and validation of the study.
- ii) *Selection of primary studies* – at this step, process efforts were made to eliminate some literature that is irrelevant to the research study. The protocol assists in describing exactly which criteria were used to select the primary studies. The range of primary studies to be utilised was further filtered to a range of five years (2015-2021).
- iii) *Study quality assessment* – the purpose of this step was to remove irrelevant research studies to the area of the study, and as such vetting of the literature against the criteria was done to ensure quality. Furthermore, the secondary screening was conducted based on full-text inclusion and quality screening (Armitage & Keeble-Allen, 2008).
- iv) *Data extraction and monitoring* – using primary sources, data extraction was conducted making use of the key terms and phrases. From the source document, both the key terms and phrases were defined as any phrase or term that related to a question under scrutiny.
- v) *Data synthesis* – synthesis of the extracted data was also conducted using qualitative data analysis. Subsequently, the identification of themes and observation of recurrent trends from the literature results were communicated at the reporting stage.

Phase 3 – Reporting the review

The reporting phase is designed in its nature to report the findings of the review and discuss the results of the problem statement. Furthermore, discussions in this phase informed how the framework would be formulated. Experts reviews were used after this phase to refine the contingency management framework.

1.7.6 Primary data

Sarstedt, Bengart, Shaltoni, and Lehmann (2018) in their research studies allude to data collection as a process of gathering information that relates to a specific topic to be examined using a systematic approach. According to de Kleijn and Van Leeuwen (2018), primary data

collection refers to the process of gathering data from sources to answer a specific research question. The Management Study Guide (2013) agrees with this notion, saying data which is collected by the researcher is referred to as primary data. When adopting a qualitative research method, primary data may be collected utilising various methods including observation, interviews, active participation, and expert reviews (Jennings, 2012). Other research studies describe primary data as information at first hand, compared to secondary data which is used by the researcher, but was collected by someone else, for instance from previous literature (Englander, 2012). Additionally, in a primary data method, the process used to collect and survey the opinions of experts on a particular subject is referred to as expert review (Simon, 2011).

In this research study, primary data was collected through expert reviews, and the experts that were approached for reviews are subject matter experts in cybersecurity and have conducted threat analysis in the field of electronic health records. The literature drawn from secondary data specific to both the domain of cybersecurity and that of EHR in the public health sector in South Africa was reviewed and evaluated by all six experts nominated.

1.7.6.1 Population and sampling

Groves (2004) refers to the population as including a group of people, events, groups, or objects that are the representation one wishes to understand. Flick (2015) posits that a population can be referred to as a description of the study group under scrutiny. In this study, the targeted population for this research was defined to include individuals who are subject matter experts in the healthcare sector, electronic health record systems (EHRs), information security, and have at least conducted threat analysis in the field of cybersecurity. At least two of these individuals must have conducted and published within the subject of EHR implementation in South Africa together with two more individuals who have worked in the public sector in South Africa.

Grey et al. (2016) describe a sample of the population as a portion of a population that is studied in a research project. However, according to Eubank et al. (2016), a population constitutes a large number of potential participants, and the design of this research study did not require a large number of participants. Eubank et al. (2016) and Mbokane (2001) posit that a smaller grouping of people drawn to represent the entire population can be referred to as a population sample.

Therefore, in this research study, the smaller grouping that was identified as a population sample comprised six subject matter experts that were adequate for this task. Furthermore, all six experts were required to respond to open-ended questionnaires to elicit their opinion on the in-depth understanding of cybersecurity in a healthcare setting. The table below explains how the six subject matter experts will be selected.

Table 1: Details of Expert Participants in the Study

No.	Subject Matter Expert	Description
1	Expert in EHR	<i>conducted and published EHR implementation in SA</i>
2	Expert in EHR	<i>conducted and published EHR implementation in SA</i>
3	Expert in EHR	<i>conducted and published EHR implementation in SA</i>
4	Expert in Security	<i>worked in the public or private sector in SA as CISO</i>
5	Expert in Cybersecurity	<i>worked in the public or private sector in SA as CIO or CISO</i>
6	Expert in Cybersecurity	<i>worked in the public or private sector in SA as CIO or CISO</i>

1.7.7 Data analysis methods

Ma (2015, p. 566) defines data analysis as a “*process of moving from the collected data into manageable components in an attempt to achieve understanding and/or interpretation of the investigated results*”. Male (2016) agrees with the notion above saying the researcher can sort perception of the gathered data from the partakers' perspective, identifying patterns and categorising topics and consistencies. Male (2016) further states that the process of data analysis and that of data collection must commence at the same time.

In this research study, data analysis was conducted in one iterative session that was followed by nominated expert reviewers. Eubank et al. (2016) refer to this technique as a process for gathering data from experts with the aim to achieve a convergence of opinions or ideas in a specific domain. Through this technique, experts were provided with a proposed solution to the research question which they were expected to review and then to comment on areas that needed to be improved respectively. A conceptual framework and open-ended questions were sent to experts to obtain information regarding improving the framework.

The communication strategy involved emailing the six expert reviewers a conceptual framework along with open-ended questions intended to cross-examine the reviewers to elicit

any new information from the proposed conceptual framework. Upon receiving feedback with any proposed changes, the researcher implemented these respectively.

1.7.8 Data trustworthiness

The findings of the research should be as trustworthy as possible. Nowell, Norris, White, and Moules (2017) state that trustworthiness is a method that can be used by researchers to encourage themselves and readers to see the importance of their research findings. It is evident from many researchers that qualitative research has become increasingly recognised and valued and as such, it has become important that it is conducted methodologically with useful results (Sinkovics, Penz, & Ghauri, 2008).

As clarified in the previous section, the reason for conducting the iterative session was to ensure the data collected is trustworthy. Nowell et al. (2017) further explain how the concept of trustworthiness is refined, where four techniques are introduced including credibility, transferability, dependability, and confirmability. These methods are based on persistent observation, contextual description, case analysis, and transparency (Kothari, 2004).

Amin et al. (2020) posit that in a qualitative study the concept of credibility is compared or parallel to internal validity and is about ensuring the confidence of the truth in the study. Graneheim and Lundman (2004) in their research study put forward the view that credibility is worried about the accentuation of the research study and alludes to confidence in how to address the intended focus. Nowell et al. (2017) state that credibility is the most important criterion and speaks to the confidence of the study.

Trustworthiness also refers to transferability in qualitative research as external validity concerns the usefulness of findings to the person in another setting (Miller & Brewer, 2015). Graneheim and Lundman (2004) posit that transferability is the degree to which the research discoveries can be transferred to other groups or settings and can be delayed by superficial examination of study.

Another technique of trustworthiness, according to Lincoln and Guba (1989), is dependability which means to account for both issues of instability and design. Connelly (2016) explains dependability as the steadiness of data and its state during the course of the study. Connelly (2016) asserts that dependability is similar to reliability in a qualitative research study.

The final criteria in a qualitative research study are confirmability and Amin et al. (2020) find these criteria to be comparable with the objectivity of the study and concerned with the degree

of consistency with emerging data and interpretations of information. Graneheim and Lundman (2004) in their study confirm the notion of confirmability being a question of verification. Connelly (2016) also affirms these theories saying confirmability refers to the degree of findings being consistent and neutral.

1.8 DELIMITATION OF THE RESEARCH STUDY

The study focused on electronic health records (EHRs) and cybersecurity threats in the public health sector in South Africa. The scope of the research study was restricted to developing a contingency management framework that to mitigate cybersecurity threats to EHRs in the public health sector in South Africa. The study population was limited to six subject matter experts from both the public sector and the University of Fort Hare. The entire research study focused on the cybersecurity technological aspect as well as its governance within the healthcare facility. Furthermore, the scope of this project was restricted to national and provincial public sector departments and excluded private hospitals. The next section discusses ethical considerations.

1.9 ETHICAL CONSIDERATIONS

This study followed the moral guidelines specified by the University of Fort Hare's Research Ethics Committee. Therefore, moral endorsement to lead the research study was sought from the University of Fort Hare's Ethics Committee, (CIL021SNGX01) Appendix A. Resnik (2013) describes ethics in research as a standard manner to differentiate acceptable and unacceptable conduct. Saunders, Lewis, and Thornhill (2003) posit that factors relating to ethics and how a researcher should be conducting research in higher education requires consideration, and these were adhered to in this research as follows:

Anonymity: nominated participants to perform expert reviews were kept anonymous to other participants performing reviews in the study. The personal information of participants that includes their identity and names was kept anonymous, pseudo names were used to represent the participants.

Wilful participation and withdrawal: The voluntary nature of participating in the study was explained to the expert reviewers. Participants were given an option not to participate in the study at anytime should they wish to withdraw.

Risk of harm: Even though it was envisaged that there would be no threat in conducting this study, all members contributing to the study were informed of any hazards and risks that could be encountered in the study.



University of Fort Hare
Together in Excellence

CHAPTER 2: RESEARCH METHODOLOGY



2.1 INTRODUCTION

The previous chapter served as a foundation for the model that was evaluated in this research study. Saunders and Bezzina (2015) view research as the application of different systematised strategies and procedures in pursuit of substantial knowledge. A research methodology is an organised way to respond to a research issue or is a process of finding out about a phenomenon by systematically examining its attributes and merits (Burns & West, 2000; Mouton, 1996). Collis and Hussey (2013 p. 21) describe research methodology as an “*ethical, systematic and theoretical analysis of the approaches applied to a field of study*”.

This chapter deals with the philosophical paradigm which acted as a lead for the researcher by laying out the philosophical foundations and fundamental expectations upon which the research was constructed. The chapter discusses the philosophical paradigm, research approach and research design which framed the premise of data assortment methods, population and sampling, and data analysis methods in the study. Finally, data trustworthiness, delimitation of the research study, and ethical considerations are also discussed.

2.2 PHILOSOPHICAL RESEARCH PARADIGM

Collis and Hussey (2013) refer to a philosophical research paradigm as a framework that outlines philosophical underpinnings and underlying scientific knowledge that is to be produced. Various research studies refer to the research paradigm as a model that seeks to develop and verify theories about how the research project should be conducted (Bissict, 2016; Collis, & Hussey, 2013). This ensures that thorough and rigorous research is being performed. Thus, it facilitates a set of assumptions about the nature of reality (*ontology*) and also how that reality is understood (*epistemology*) (Saunders, Lewis, & Thornhill, 2007).

Valizadeh and Vaezi (2016), put forward the view that research studies provide other philosophical perspectives such as pragmatism and axiology. In the context of Information Systems and Technology (IS/IT) studies, two main philosophies are presented, positivism and interpretivism (Collis & Hussey, 2013). However, Oates (2006) acknowledges three philosophical paradigms and refers to them as positivism, interpretivism, and pragmatism. To ensure thorough and rigorous research, the use of a chosen paradigm would contribute to the integrity of this study. The following section discusses all three paradigms respectively and thereafter states the paradigm that aligned with this research study and which was thus selected.

2.2.1 Positivism

The positivist paradigm is traditionally used in natural science research studies and amongst others is found to be the oldest research paradigm (Igwenagu, 2016). Bryman and Bell (2015) say this paradigm seeks to help the researcher to make a common, universal generalisation when a bigger sample is investigated. Chuang and Tsao (2013), agree with the notion saying that the positivist paradigm's main objective is to find theories making use of experimentations and observation. Oates (2006) posits that the positivist approach considers reality to be external and objective, and if large samples are investigated by different researchers, they will produce results that are generalisable.

Based on the objective of this study, the positivist paradigm was deemed not appropriate for this research study. The study did not seek to prove or disprove hypotheses, but rather to understand the factors that would result in patient information being stolen by cyber criminals. The following section examines an interpretivism paradigm.

2.2.2 Interpretivism

Within the social sciences, the conflict between positivism and interpretivism dates back to the 19th century and started in the field of education research (Gage, 1989). The interpretivism approach, according to Graff (2014), begins with the assumption that there are many realities, and the researcher is seeking to understand perspectives from participants. In an interpretive research project, the aim is not to prove the hypotheses as is the case with positivist research, but rather, it pursues to identify, explore and explain how related and interdependent factors are in a social setting (Oates, 2006; Klein & Myers, 1999).

Furthermore, Rowlands (2003 p. 22) posits that “*variables are not predefined and independent but the emphasis is to produce an understanding of the social context of the phenomenon and processes whereby the phenomenon influence and is influenced by social context*”. This paradigm explains and understands how actions influence a phenomenon, producing a reproducing social order for an organization (Nunu, 2019).

Therefore, using the interpretive perspective will aid researchers in understanding of critical, social, and organisational issues in line with the adaptation and acceptance of IS/IT in organisations. The following section discusses the third paradigm to assess its relevance to the study.

2.2.3 Pragmatism

Pragmatism is the third paradigm that Oates (2006) acknowledges. According to Leech, Barrett, Morgan, Clay, and Quick (2004), pragmatism regards knowledge as the reality of the world we live in and is constructed on reality. The literature on pragmatism presents researchers with the opportunity to use both qualitative and quantitative data collection methods or both as the importance is on ‘*what works best to address the phenomenon in question*’ (Denzin, 2010; Morgan, 2014). Dewey (2008) refers to this paradigm as mixed-method research (MMR), with consideration that it is an expansive and creative form of research, interesting researchers to take a different approach to method selection to produce the best results.

In social research, the advantage of pragmatism, according to Morgan (2014), is that it can serve as a philosophical programme regardless of the method used being qualitative, quantitative, or mixed-methods. This allows researchers an opportunity to indicate their research question and be able to define a framework that would be better used to respond to the research question. However, the intentions of this study were purely focused on using qualitative methods to understand how cybersecurity threats can compromise EHRs in public healthcare in South Africa. Additionally, the researcher had no intention to prove the hypothesis nor required any precise measurement to answer to research questions, and hence quantitative method was not used and pragmatism was not suitable for this study. In the next section, the appropriate research paradigm that was selected for this research study is justified.

2.3 SELECTING AN APPROPRIATE RESEARCH PARADIGM

Interpretivist researchers view reality as social constructs and they seek to identify, explore and explain how the factors in a social setting are related and interdependent (Oates, 2006). As discussed in Section 2.2.2, interpretivism within the social sciences has become more widely adopted as the standard for IS/IT research projects. As a matter of fact, this paradigm emerged in response to criticism of positivism and seeks to construct and develop the social context in IS (Oates, 2006).

In order to determine which paradigm best suits a research study, researchers select an appropriate paradigm depending on the nature of the research question as well as their personal beliefs or values of the research (Oates, 2006; Collis & Hussey, 2013). Thus, the important issue is not whether the research should be philosophically informed, but rather the manner in which research can reflect philosophical choices and be able to defend them in alternative philosophy. Figure 4 below depicts Collis and Hussey's (2013) Continuum of Core Ontological Assumption.

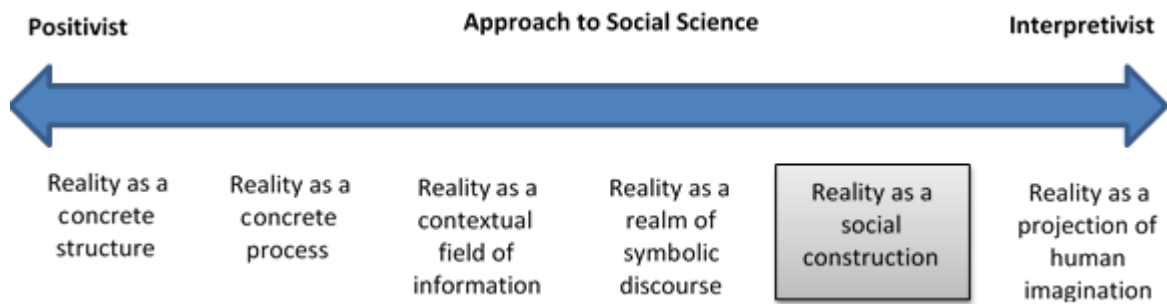


Figure 4: Continuum of Core Ontological Assumption

(Collis & Hussey, 2009)

As depicted in the figure above, the study aligns with the fifth stage of the Continuum: “*Reality as Social Construction*”. Collis and Hussey (2009) state that positivist researchers are objective in their nature and as a result, they view reality as a concrete structure whereas interpretivist researchers’ approach to social science is that they view reality as a social construct.

In this research study, the ontological stance required a deeper understanding of cybersecurity threats in the healthcare sector, and no experimentations, numerical quantities, and observation were used. Additionally, the researcher viewed reality as a social construct as it intends to develop a conceptual framework with no intention to produce large sample results.

Therefore, the research study leans more towards interpretivism as its objective was to develop a contingency management framework (CMF) to safeguard the information to EHRs against cybersecurity threats in the healthcare sector in SA. Furthermore, the interpretivist paradigm requires a qualitative method because it allows the research to ask the questions what, how, and why (Collis & Hussey, 1942).

Thus, the qualitative data was gathered from various sources that included journals, articles, books and cases studies in order to identify these concerns. Consequently, a comparison among various international frameworks, models, strategies, and policies was conducted in order to address issues of cybersecurity in the healthcare sector.

Table 2: Applying research philosophical paradigm to the study

Paradigm	Positivist	Interpretivist	Pragmatism	Application to this study
Ontology	Reality is objectively supplied, uncertain, but knowable	Multiple realities from socially different human experiences which may be true	Knowledge is the reality of the world we live in and is constructed on reality	Literature review was used as the data collection method in the research study. Expert reviewers were employed in the study to describe the nature of reality concerning the proposed conceptual framework
Epistemology	Research carried out independently of research	Participatory interaction exists between the subject of research and the researcher	Participatory interaction exists for the researchers through research questions and can define a framework	The method of data collection used was literature review Researchers asked experts to review the proposed conceptual framework for the SA healthcare sector for objectivity, and this led to their interaction.
Methodology	Mainly quantitative methods, observatory, manipulative, and thorough verification of hypotheses	Mainly participatory, qualitative, explanatory, and rationalistic	Mainly mixed-method research (MMR), with consideration that it is an expansive and creative form	Literature review was used as the data collection method Qualitative research methods were adopted to understand the subjective narratives and discourses of cybersecurity to the patient record in the healthcare sector

(Adapted from Collis & Hussey, 2013)

The following section explains the research approach to be adopted by the research study.

2.4 RESEARCH APPROACH

When conducting a research study, two approaches can be applied – the inductive and deductive approaches. In Chapter 1 (Section 1.6.4) a conceptual structure was described as a creative process of assembling, developing concepts, constructs, and components built in a qualitative method (Ameen et al., 2020). Furthermore, the theoretical structure was described as a group of theories that combined to provide information for explaining, viewing, or

contemplating a phenomenon (Ngxabane & Cilliers, 2020). The approaches are further discussed in the following section.

2.4.1 Inductive approach

Saunders et al. (2007) posit that the inductive approach is a hypothesis made from the perception of empirical reality and it gives a better comprehension of the nature of the problem. A qualitative approach integrates both the description and interpretation of phenomena within their context, which is known as the inductive approach (Liu & Zhang, 2015). Ma (2015) posits that the inductive reasoning approach differs from deductive reasoning in that it starts from being specific and moves to generalisation.

Golden-Biddle and Locke (2007) further put more emphasis on this saying this approach allows the research to construct new theories in order to arrive at generalisation. This study made use of an interpretive paradigm that employs an inductive research approach where collected data was used at the start to derive theory about the phenomenon of interest. In line with the objective of the study, the theories were tested and refined to formulate a conceptual framework to be used by the healthcare sector in SA.

2.4.2 Deductive approach

Collis and Hussey (2013) described the deductive approach as the creation of conceptual and theoretical structures which are tested by empirical observation. Through deductive reasoning, theories can be tested through the application of pre-existing or pre-developed propositions to a situation (Rahman, 2015). Kothari (2004) explains this by saying when a researcher starts from theory, deriving a hypothesis from it, testing the hypothesis, and revising that theory, that is referred to as a deductive approach. Igwenagu (2016) concludes this clarification saying because this approach tests a hypothesis and is concerned with experiments, it is generally associated with quantitative methods.

The ontological stance in this research study required a deeper understanding of cybersecurity threats in the healthcare sector. As explained in the previous section, the positivist approach requires experimentations, numerical quantities, and observation to test its theories, and in this study, there was no hypothesis to be tested. As such, this study did not use the deductive approach as there were no numerical quantities to work on and there was no hypothesis to prove.



University of Fort Hare
Together We Advance

2.5 RESEARCH METHODS

In research, the tools used for collecting and analysing data, according to Collis and Hussey (2009), are referred to as research methods. Although there are several discussions of issues regarding the appropriate research modes that can be applied in a study, Mkhomazi and Iyamu (2013), in their research study, present three methods that are normally used in research, namely qualitative, quantitative and mixed methods. The following section discusses these methods further, beginning with qualitative.

2.5.1 Qualitative research methods

Brannen (2017) posits that the qualitative method influences the natural scientific method in the human behavioural study which is exclusive to what can be measured and observed objectively. McCusker and Gunaydin (2015) refer to qualitative methods as a detailed description to be obtained about what is being observed. Various research studies have explained qualitative research as a method that seeks to describe and explain, explore and interpret how people perceive phenomena (Blumberg, Cooper, Schindler, 2014; Cassell & Symon, 2014).

This study applied a qualitative research approach that is consistent with the interpretive paradigm. The focus of the research was on understanding and interpreting factors that influence cybersecurity threats in the healthcare sector in SA. As a result, the qualitative approach that was used allowed the interaction between the researcher, a literature review, and expert reviewers on how to refine a proposed conceptual framework to be used in the sector.

2.5.2 Quantitative research methods

Quantitative methods are generally popular in the research field for testing a theory and hypothesis and are specifically used in the positivist paradigm (Collis & Hussey, 1942). Furthermore, Murshed and Zhang (2016) posit that quantitative methods are concerned with numerical values and require precise measurements of constructs. Thus, studies conducted quantitatively generally use statistical, computational, or mathematical techniques to determine the relationship between variables in a controlled environment. This method was found to be not suitable for this research study as the study planned to use an open-ended questionnaire for data collection which is suitable for the qualitative method.

2.5.3 Mixed methods

Kothari (2004) explains that both qualitative and quantitative approaches are commonly used in IS/IT studies. However, once the two methods are used in combination they are referred to

as mixed methods. Oates (2006) posits that the mixed method approach encompasses both quantitative and qualitative data collection methods in a research study. The objective of combining both techniques (qualitative and quantitative) is not to dispose of either technique which will minimise their inherent weaknesses (R. B. Johnson & Onwuegbuzie, 2004). When both methods are used, they allow the research question to be responded to in a varied fashion of perspectives leading to greater authenticity of the research outcome (Wiid & Diggines, 2013). This method was not adopted in this research as the researcher applied qualitative research methods by means of a literature review. The following section presents the research design of the study.

2.6 RESEARCH DESIGN

Research design “*is the conceptual structure within which research is conducted, constituting the blueprint for the collection and analysis of data*” (Gill & Chew, 2018, p. 251). In this way, it facilitates the smooth implementation of the various research operations by providing an outline for the research (Gill & Chew, 2019). According to Mouton (2001), the research design must be constructed enough to respond to the research problem or research question. According to Creswell (2009), the design of a research project is an association between the research question and its execution.

A literature review was selected as the research design best suited to answer the question presented in this research study. According to Armitage and Keeble-allen (2008), the literature review has taken its historical development in medical sciences where research studies based on meta-analysis have been long established. Furthermore, the literature review is recently found in social sciences as contributing to the development of review methodology through approaches to qualitative research. The literature review method that was used is discussed in the following section below.

2.6.1 Data collection methods

A literature review was consulted in order to collect information on existing knowledge to develop a conceptual framework for mitigating cybersecurity threats in public health, in accordance with the study's objectives. According to Woo, Pettit, Kwak, and Beresford (2011), the literature review can be useful when drawing from existing literature that could apply to the research question (Munyarandzi, 2018). To identify the gap in cybersecurity literature, existing knowledge related to cybersecurity and electronic health records was used to develop

a conceptual framework. Figure 2 below presents the literature review process adopted in this research study.

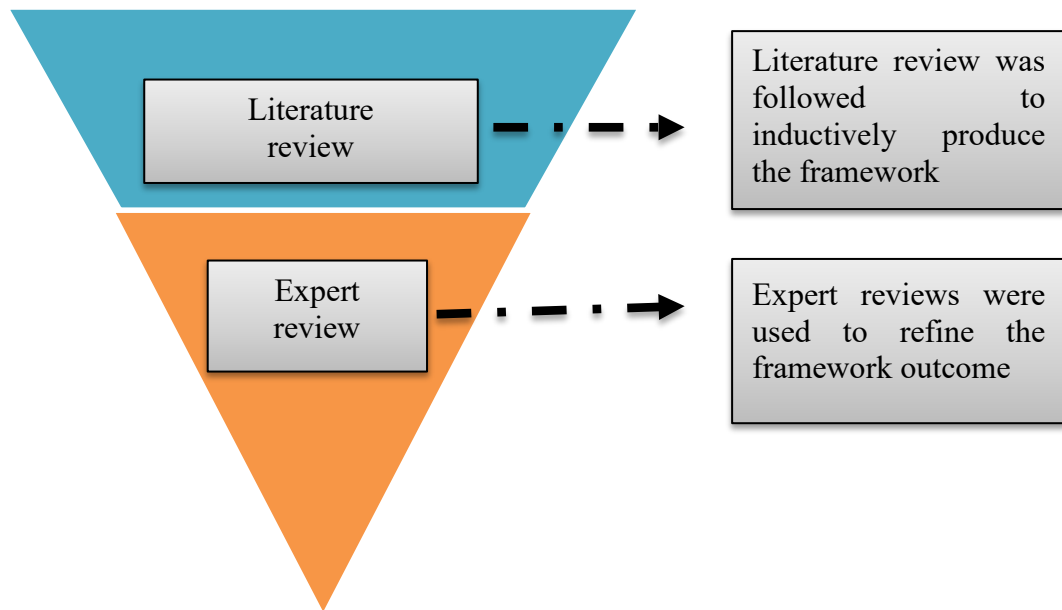


Figure 5: Literature review

This research investigates the possibility of collecting either primary or secondary data in a research project, respectively. In the following sections, we examine both data collection methods extensively.



2.6.2 Secondary data

According to the Management Study Guide (2013), secondary data is referred to as data collected for a purpose other than the study in question and is data that can be obtained from other sources. In this study, secondary data was obtained by conducting a literature review. Massaro, Dumay, and Guthrie (2016) state that most researchers use a literature review to draw and evaluate the existing information to identify future research needs. A literature review can yield better results when it is done thoroughly and follows a predetermined protocol (Armitage & Keeble-Allen, 2008). A literature review can thus be broken down into three main phases, *i*) planning, *ii*) conducting, and *iii*) reporting the results of the literature review (Dumay et al., 2016).

a) Phase 1 – Planning

According to Salkind (2010), planning in research is an applied investigation designed to respond to an inquiry using empirical observation. The first phase for this study involved planning the review and this was further broken down into the five-step approach as follows:

- i) *Identification of the need to review* – literature specific to both the domain of cybersecurity and that of EHR in the public healthcare sector in SA was reviewed with the objective to develop a conceptual framework for use in mitigating cybersecurity threats to electronic health records in the public health sector in South Africa. The list of sources that was searched traditionally contains the relevant online digital libraries offered at the University of Fort Hare.
- ii) *Commissioning a review* – the goal of this step was to use the investigated literature review from step one to develop a conceptual framework that was to mitigate cybersecurity threats to electronic health records in the public health sector in South Africa.
- iii) *Specifying the research questions* – attempting a literature review was mostly aligned to a research problem. Section 1.3.1 of this research study was a formulation of a research question that seeks to respond to the research study. The research question was further broken down into individual components that were investigated in order to respond to the main research question of the study.
- iv) *Developing a review protocol* – this step was very important as it outlined exactly how each step would be carried out. This step was also beneficial in ensuring the researcher's bias was minimised as well as documenting each step of the process which is vital for the replicability of the study was ensured.
- v) *Evaluating the review protocol* – at this step, in order to ensure the effectiveness of the collected sources, the review document was shared amongst colleagues for evaluation.

b) Phase 2 – Conducting the review

With the developed plan in hand, it was now possible to conduct an actual review of the literature. This phase consists of five steps: *i)* identification of research, *ii)* selection of primary studies, *iii)* study quality assessment, *iv)* data extraction and monitoring, and *v)* data synthesis (Armitage & Keeble-Allen, 2008).

- i) *Identification of research* – the goal of this step was to retrieve all the literature relevant to the research study. The researcher accessed the following online resources: the ACM digital library database, IEEE Xplore database, ISI web of knowledge database,

ScienceDirect database, as well as the university online book lending facility, the OPAC system, to gather information. The review protocol document was used to maintain the ledgers for all the online databases, search terms, and phrases for purposes of replicability and validation of the study.

During the identification process of research, literature relevant to the defined research question was retrieved. There were several different categories of terms in each group, including synonyms, different forms and search terms, as well as similar or related terms within each domain, as shown in the Search Key Terms Table below.

Table 3: Search key terms

	Group 1	Group 2	Group 3	Group 4	Group 5
Term 1	Electronic health record	electronic-health	cybersecurity	Contingency Management	Public healthcare sector
Term 2	Patient health record	EHealth	Cyber security information systems	Incident Management	Public healthcare sector
Term 3		Electronic Health	Cybersecurity information systems	Emergency management	Public hospitals
Term 4			Cybercrime	Uncertainty management	Government clinics
Term 5					Public health facilities

ii) *Selection of primary studies* – at this step, process efforts were made to eliminate some literature that was irrelevant to the research study. This was the exclusion criteria process the study assumed. According to Kofod-petersen (2014), the purpose of this step is to filter away irrelevant studies to the area chosen. The protocol assists in describing exactly which criteria were used to select the primary studies. The range of primary studies to be utilised would further be filtered to a range of five years (2015-2021).

iii) *Study quality assessment* – the purpose of this step was to remove irrelevant research studies to the area of the study, and as such vetting of the literature against the criteria was carried out to ensure quality. Furthermore, the secondary screening was conducted based on full-text inclusion and quality screening (Armitage & Keeble-Allen, 2008).

- iv) *Data extraction and monitoring* – using primary sources, data extraction was conducted making use of the key terms and phrases. From the source document, both the key terms and phrases were defined as any phrase or term that relates to a question under scrutiny.
- v) *Data synthesis* – synthesis of the extracted data was conducted using a thematic content analysis using the qualitative data analysis measures available. Subsequently, the identification of themes and observation of recurrent trends from the literature results were communicated at the reporting stage.

c) Phase 3 – Reporting the review

The designed nature of the reporting phase was to report the findings of the review and discuss the results concerning the problem statement. The result filtered from the ACM Digital library between 2016 and 2021 yielded only seven publications that were related to information security and not e-health or electronic health records. The result filtered from Science Direct Digital library gave better results to those of ACM library in that 102 results were found that were related to the first research question of the study “*How can cybersecurity threats compromise electronic health records in the public health sector in South Africa?*”. However, most of these results were either “*Information Management*” or “*Information Systems*”. The identification process of research proceeded to the second sub-research question “*How can contingency management safeguard information in electronic health records against cybersecurity threats?*”, and the narrowing of the search resulted in 58 publications that could be used. The last and final sub-research question “*How can a framework assist with the contingency management to secure electronic health records against cybersecurity threats in the public health sector in South Africa?*” yielded only nine publications. A total of 234 publications from the University of Fort Hare were retrieved from digital libraries, including ACM Digital library, SAGE Research Methods, SAGE Journals, ScienceDirect online and SpringerLink.

Furthermore, discussions in this phase informed how the conceptual framework was to be formulated. Experts reviews were used after this phase to refine the conceptual framework.

2.6.3 Primary data

Sarstedt, Bengart, Shaltoni, and Lehmann (2018) posit that data collection is a process of collecting information about a particular topic to be examined using a systematic approach.

However, data collection can be conducted in two forms, primary and secondary. Wiid and Diggins (2013) compare secondary data and refer to primary data as data collection whereby an individual collects data from the original source to find a solution to a specific objective. Likewise, de Kleijn and Van Leeuwen, (2018) present primary data collection as the process of gathering data at sources to answer a specific research question.

The Management Study Guide (2013) agrees with the above definitions of primary data, saying that when adopting a qualitative research method, primary data may be collected utilising various methods including observation, interviews, active participation, and expert reviews. Various research studies describe primary data as information at first hand, compared to secondary data which is used by the researcher, but was collected by someone else, for instance from previous literature (Mack, Woodson, MacQueen, Guest, & Namey, (2005); Englander, (2012). Additionally, in a primary data method, the process used to collect and survey the opinions of experts on a particular subject is referred to as expert review (Simon, 2011). The following section discusses the population and sampling.

2.6.3.1 Population and sampling

Groves (2004, p. 49) refers to the population as including a group of people, events, groups, or objects that are the representation one wishes to understand. Flick (2015) posits that a population can be referred to as a description of the study group under scrutiny. In this study, the targeted population for this research was defined to include individuals who were subject matter experts in security and had at least conducted threat analysis in the field of cybersecurity.

Therefore, the subject matter experts in information security and the healthcare sector were regarded as the population sample of this study. Nwogu (1991) describes a sample of the population as a portion of a population that is studied in a research project. However, according to Denzin and Lincoln (1994), a population constitutes a large number of potential participants, and the design of this research study did not require a large number of participants. Eubank et al. (2016) and Mbokane (2001) posit that a smaller grouping of people drawn to present the entire population can be referred to as a population sample.

WBI Evaluation Group (2007) describes expert reviews as people who are subject matter experts; they have the ability to provide new ideas that can be used for developing a CMF. At least two of these individuals must have conducted and published within the subject of EHR implementation in South Africa together with two more individuals who worked in the public

sector in South Africa. The expert reviewers were asked to provide comments on the CMF developed as a result of this research study.

Therefore, in this research study, the smaller grouping that was identified as a population sample comprised six subject matter experts that were adequate for the task presented. Furthermore, all six experts were required to respond to open-ended questionnaires to elicit their opinion on the understanding of the conceptual framework. The research developed the questionnaire which was sent by email to six experts in order to refine the CMF developed as a result of this research study. The table below illustrates how the six subject matter experts were selected.

Table 4: Details of Expert Participants in the Study

No.	Subject matter expert	Description
1	Expert in EHR	<i>conducted and published EHR implementation in SA</i>
2	Expert in EHR	<i>conducted and published EHR implementation in SA</i>
3	Expert in EHR	<i>conducted and published EHR implementation in SA</i>
4	Expert in Cybersecurity	<i>worked in the public sector in South Africa as CISO</i>
5	Expert in Cybersecurity	<i>worked in the public sector in South Africa as CISO</i>
6	Expert in Security	<i>worked in the public sector in South Africa as CIO</i>

In this research study, primary data was collected through expert reviews, and the experts that were approached for reviews were subject matter experts in cybersecurity and had at least conducted threat analysis in the field of EHRs. The literature drawn from secondary data specific to both the domain of cybersecurity and that of EHR was reviewed and evaluated by all six experts nominated.

2.6.3.2 Data analysis methods

Ma (2015, p. 566) defines data analysis as a “*process of moving from the collected data into manageable components in an attempt to achieve understanding and/or interpretation of the investigated results*”. Male (2016) agrees with the notion above by suggesting that the researcher should be able to understand the data collected from the participant's perspective, categorizing themes and regularities, and identifying the pattern. Furthermore, Male (2016) states that the acquisition of data must occur concurrently with the process of analyzing it.

In this research study, data analysis was conducted in one iterative session by the nominated expert reviewers. Eubank et al. (2016) refer to this technique as a method for collecting data from experts with the aim to achieve a convergence of opinions or ideas in a specific domain. Through this technique, experts were provided with a proposed solution to the research question which they were expected to review and comment on areas that need to be improved respectively. A conceptual framework and open-ended questions were sent to experts to draw information regarding improving the framework. The feedback from the reviewers were incorporated into the framework as discussed in Chapter five.

2.6.4 Data trustworthiness

The findings of the research should be as trustworthy as possible. Nowell, Norris, White, and Moules (2017) state that trustworthiness is a method that can be used by researchers to encourage themselves and readers to see the importance of their research findings. It is evident from many researchers that qualitative research has become increasingly recognised and valued and as such, it has become important that it is conducted methodologically with useful results (Sinkovics et al., 2008). Nowell et al. (2017) further explain how the concept of trustworthiness was refined, where four techniques were introduced including credibility, transferability, dependability, and confirmability. These techniques are based on persistent observation, contextual description, case analysis, and transparency (Kothari, 2004).

Lincoln and Guba (1989) posit that in a qualitative study the concept of *credibility* is compared or parallel to internal validity and is about ensuring the confidence of the truth in the study. Graneheim and Lundman (2004), in their research study, put forward the view that credibility is concerned with the emphasis of the research study and refers to confidence in how aspects are processed to address the intended focus. In this study, the responses collected from expert reviewers were analysed to improve the conceptual framework. Polit and Beck (2014) state that credibility is the most important criterion and speaks to the confidence of the study.

Trustworthiness also refers to *transferability* in qualitative research as external validity that is concerned about the usefulness of findings to the person in other settings (Miller & Brewer, 2015). Graneheim and Lundman (2004) posit that transferability is the extent to which the research findings can be transferred to other groups or settings and can be delayed by superficial examination of the study.

Another technique of trustworthiness, according to Lincoln and Guba (1989), is *dependability* which finds means to account for both issues of instability and design. Connelly (2016)

describes dependability as the steadiness of data and its state during the course of the study. Connelly (2016) further asserts that dependability is similar to reliability in a qualitative research study.

The final criteria in a qualitative research study is *confirmability* and Amin et al. (2020) find this criterion to be comparable with the objectivity of the study and posit that it is concerned with the degree of consistency with emerging data and interpretations of information. Graneheim and Lundman (2004), in their study, confirm the notion of confirmability as being a question of verification. Connelly (2016) also affirms these theories saying confirmability is the degree to which findings are consistent and neutral.

2.7 DELIMITATION OF THE RESEARCH PROJECT

The study focused on mitigating cybersecurity threats to EHRs in South Africa. Neither private nor public sector hospitals formed part of the investigation. The research study focused on the cybersecurity technological aspect as well as its governance. The next section discusses ethical considerations. The scope of the research study was restricted to developing a conceptual framework to mitigate cybersecurity threats to EHRs in South Africa.

2.8 ETHICAL CONSIDERATIONS

Research study ethics approval was sought from the University of Fort Hare's Ethics Committee (CIL021SNGX01 see Appendix A). Resnik, (2013) describes ethics in research as a standard manner to differentiate between acceptable and unacceptable conduct. Saunders, Lewis, and Thornhill (2003) posit that factors relating to ethics and how a researcher should be conducting research in higher education require consideration, , and these were adhered to in this research as follows:

Anonymity and confidentiality: Nominated participants to perform expert reviews were kept anonymous to other participants performing reviews in the study. The personal information of participants that includes their identity and names was kept anonymous, pseudo names were used to represent the participants (Saunders et al., 2015).

Wilful participation and withdrawal: The voluntary nature of participating in the study was explained to the expert reviewers. Participants were given the option not to participate in the study at any point should they wish to withdraw (Saunders et al., 2015).

Risk of harm: Even though it is envisaged that there would be no risk in conducting this study. all participants contributing to the study were informed of any hazards and risks that could be encountered in the study (Saunders et al., 2015).

2.9 CONCLUSION

A comprehensive description of the methodology applied to this research study is discussed in this chapter. The discussion outlined the research paradigm, methodology, strategies as well as design applied in the project, including data collection and analysis methods.

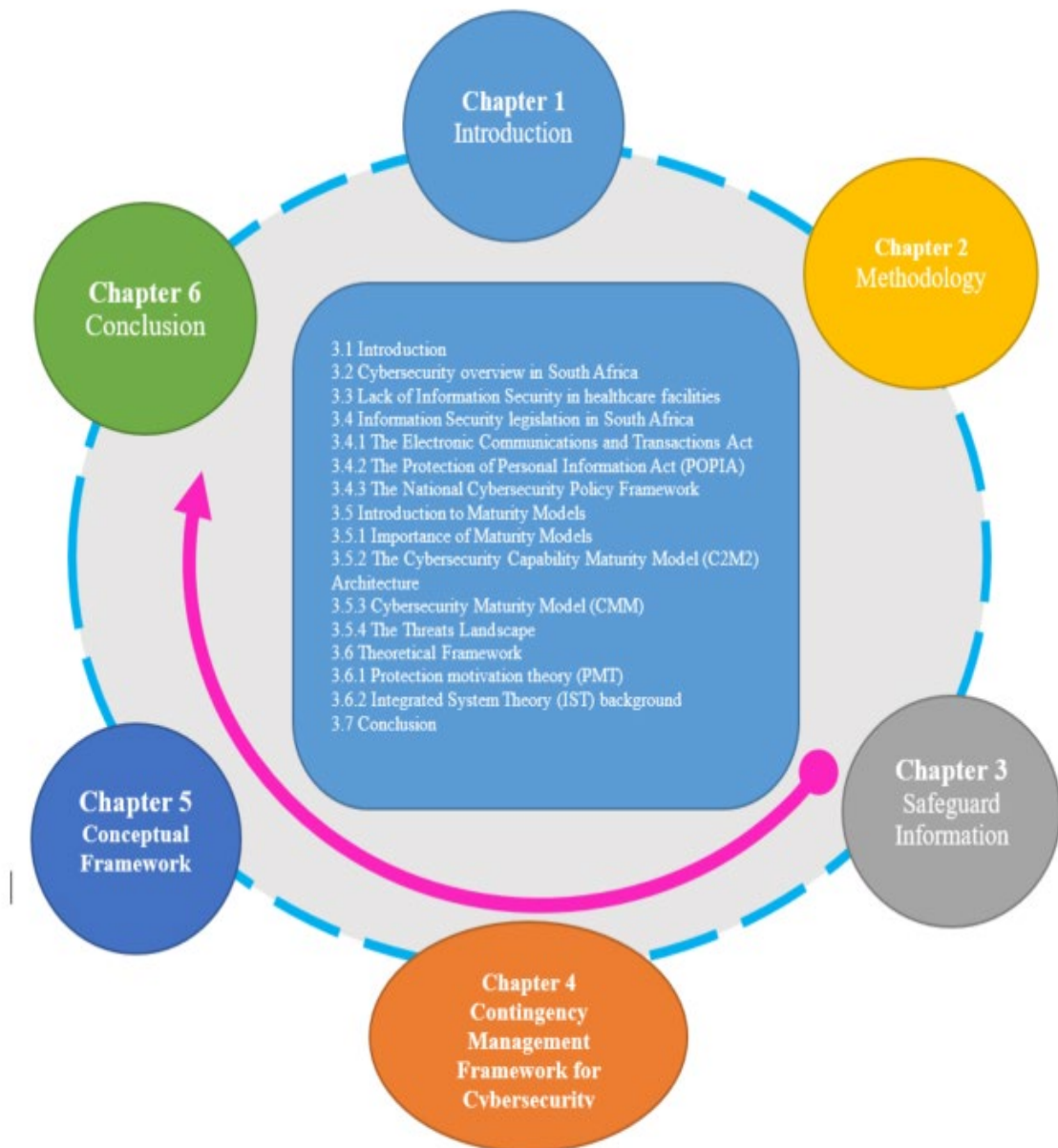
As stated above, philosophical paradigms were discussed, namely the three paradigms – interpretivism, positivism, and pragmatism. The interpretivist paradigm was employed as it was deemed fit to solve the research problem of the study. Literature review was the optimal research design used to answer the question posed in this research study. Both primary and secondary data collection methods were used to collect the research study information. Furthermore, three iterative sessions were conducted by the nominated subject matter experts together with open-ended questionnaires to elicit their opinion.

After reviewing the ethical considerations used to guide the research process, this chapter concludes.



University of Fort Hare
Together in Excellence

CHAPTER 3: LITERATURE REVIEW



3.1 INTRODUCTION

Electronic health records (EHRs) have become increasingly popular in the South African health sector as discussed in the previous chapter. However, the growth of the information society and the increased cybersecurity breaches in the healthcare sector have revealed a need for information security measures (Bissict, 2016). The World Health Organisation (WHO) recognised that when EHRs are not implemented in a healthcare facility, health outcomes, and care efficiency are negatively impacted (Zayyad & Toycan, 2018). Within the healthcare facility, EHRs are so important that Wright, O'Mahony, and Cilliers, (2017) consider it to be essential to sustain patient safety and care while providing better efficiency. However, the safeguarding of patient-sensitive information, according to the 2018 Cyber-Security Breaches Survey, has in recent years become a major challenge (Ursillo & Arnold, 2019).

This challenge has led the South African government to announce the National Cybersecurity Policy Framework (NCPF) in 2012 with the aim of providing a coherent and integrated approach to address cybersecurity threats (Sutherland, 2017). Further to that, the e-health strategy for South Africa 2012 – 2016 was also developed to address the foregoing challenges in health information systems (Katuu, 2018). Thus, over the years, the information systems have been described as disintegration with a lack of automation, interoperability, lack of collaboration, and prevalence of manual systems (Katuu, 2016). This research focused on the relationship and interaction between EHRs and cybersecurity to develop a framework that can be used to circumvent cybersecurity threats in the public health sector in South Africa. This chapter provides answers to the remaining research sub-question.

How can contingency management safeguard information in electronic health records against cybersecurity threats?

Because of the growing reliance on information security, there are numerous risks that must be considered, the first section of this chapter discusses the overview of cybersecurity in South Africa (SA) followed by a discussion of implemented Information Security legislation in SA. The second section discusses the Cybersecurity Maturity Model (CMM) to ascertain the cybersecurity level of preparedness in SA healthcare organisations. This is followed by the theoretical framework section that includes the protection motivation theory (PMT) and integrated system theory (IST) used to identify gap areas that result in increased cybersecurity incidents in the South African healthcare sector. The IST was used in this study to evaluate information security management of public healthcare organisations through making use of the

results of previous studies found in the literature. Finally, the chapter presents the literature reviewed on contingency management in the healthcare sector.

3.2 CYBERSECURITY OVERVIEW IN SOUTH AFRICA

In today's digital world, we are living in cyberspace that is expanding rapidly due to the volume of information collected and processed (Le & Hoang, 2017). EHRs are becoming more prevalent on the African continent and have the potential to stay longer, protect and enhance patient lives (Coventry & Branley, 2018). However, the prevalence of healthcare technologies intertwined with cyberspace has increased patients' concerns over the security of their EHR (Burke, Taiwo, Alireza & Gondal, 2019). Additionally, advancements in technology are also continuously threatened by many risks that can have adverse effects on the security of healthcare data and medical devices.

Cybercrime has become a lucrative business with a specific focus, according to the Cybersecurity Breaches Survey 2018, on the healthcare sector (Ursillo & Arnold, 2019). Both public and private healthcare in South Africa have become an attractive target for cybercrime for two fundamental reasons:

- lack of legislation that governs and protects healthcare technologies and;
- weak defences for valuable information (Coventry & Branley, 2018).



Together in Excellence

A well-developed cybersecurity framework is essential to ensure the protection of information in healthcare facilities (Kruse, Frederick, Jacobson, & Monticone, 2017). The following section will deliberate on the impact of the absence of information security in the healthcare sector.

3.3 LACK OF INFORMATION SECURITY IN HEALTHCARE FACILITIES

Both large and small organisations, private or public, connected to the internet are at risk of being targeted by hackers daily (Ursillo & Arnold, 2019). The Data Breach Report and Mimecast "The state of Email Security" report released in 2019 found that many hospitals in South Africa have weak defences to prevent and protect the cybersecurity breach to healthcare medical data (Nathan & Scobell, 2012; Ponemon Institute, 2019). Ponemon Institute (2019) Cost of Data Report states that more than a 30% chance exists that organisations across the board will be experiencing an increase of major data breaches annually due to cybersecurity breaches.

Jaquire (2015) argues that it is cyberspace that has initiated many information security breaches and has become a place of cybercrime originating from outside the borders of our country. Many of these attacks and data breaches, amongst other criminal acts, according to the Mimecast “*The state of Email Security*” report, were perpetrated making use of email spoofing by forging the sender’s address (Oliver, 2019). Further, according to Connelly Lynne (2016), the increased connectivity of medical devices to the internet has resulted in the exposure and vulnerabilities of healthcare technologies. Flahault et al. (2018) concur with this notion adding that health facilities’ exposure is due to weak information security defences and the introduction of these interconnected medical devices.

Coventry and Branley (2018) posit that the lack of security infrastructure designed to protect medical devices, such as the Intrusion Detection and Prevention System (IDPs), Firewalls, and Virtual Private Networks (VPN), can result in health facility medical devices being vulnerable to external intruders. As a result in 2017, IBM Frequency Data Breaches 2019 report, predicted that public healthcare organisations will be amongst the top targeted by cyberattacks due to lack of cyber protection (IBM, 2019). Whitman and Mattord (2018, p. 387) define an Intrusion Detection and Prevention System (IDPS) as a technology system that is designed to detect and modify its environment to protect an organisation from threats and intrusions. A firewall is a software or hardware that prevents intruders from stealing information (Hamidi, 2019). Both Hamidi (2019) and Whitman and Mattord (2018) posit that a Virtual Private Network (VPN) is an extension of a public network using private communication with certain protocols to enable users to send and receive information.

Meanwhile many other authors blame the cybersecurity challenges on infrastructure, email spoofing, and many other weak defences that lead to the cybersecurity breach in healthcare data (Burke et al., 2019; Commonwealth of Australia, 2016; Kure, Islam, & Razzaque, 2018). Flahault et al. (2018) put the blame on the human element, arguing that people are the weakest link in the organisational information management cycle. It is also common knowledge, according to Hamidi (2019), that at the healthcare facilities nurses, doctors and physicians are working with sensitive clinical data. Thus, the Health Insurance Portability and Accountability Act (HIPAA) in America forced healthcare organisations to maintain the availability, confidentiality, and integrity of a patient’s medical and health information by implementing a robust and reliable electronic healthcare system. A report written by Coventry and Branley

(2018) presents the high degree of emotional harm in the event of theft of patient data which results in medical identity theft and financial identity theft.

Indeed, Whitman and Mattord (2018) agree with this notion saying technical hardware failure and technological obsolescence can lead to a system performance being out of expected normal working conditions, untrustworthy and unreliable, resulting in unavailability of service. The unavailability of healthcare services has led to the Global State of Information Security Survey (GSISS) suggesting that there is a need to revitalise privacy risk management and merge it with cybersecurity (Burke et al., 2019). The following section discusses the information security legislation in SA to identify key factors in any national cybersecurity protection of healthcare data.

3.4 INFORMATION SECURITY LEGISLATION IN SOUTH AFRICA

Generally, it is common cause that countries regulate their cyber environment through policy; however, with the lack of international cyber laws, it is difficult to resolve cross-border cyber issues impeding the cybersecurity efforts (Jaquire & Von Solms, 2015). In this section, the discussion centres around the policy and legislation designed to govern the information exchange amongst various organisations locally and abroad.

Even though the South African National Development Plan 2030 (NDP) states that "*All people living in South Africa feel safe and have no fear of cybercrime*", the rate of cybercrime has increased over the years (Kempen, 2017). The available evidence seems to suggest that government legislation is unable to address the issue of cybersecurity threats (State Security Agency 2015; Coventry & Branley, 2018; Flahault et al., 2018). Most developing countries on the African continent, including SA, according to Kempen (2017), seem to be lagging in both research and policy development in order to prevent cybersecurity threats. A third of organisations in SA currently have no cybersecurity plan or strategy with only a quarter having a fully functional plan or strategy (Leppan, 2017). The 2018 Global State of Information Security Survey (GSISS) reports that 44% of the organisation did not have an overall information security strategy (PWC, 2018). In order to foster cyber-security, a growing number of African countries are enacting or establishing policy and legislative frameworks to facilitate it. (Mohammed and Bade, 2019).

In response to these global attacks, the South African government collaboratively established policies and structures that govern the exchange of information between public and private sector retaliation to cybersecurity vulnerabilities and attacks (State Agency, 2015). Kempen

(2017) posits that the establishment of information security policies, regulations, and laws is a strategy to mitigate the instances of threats and vulnerabilities to healthcare technologies and patient data. The South African legislative context that relates to information security and privacy is found to be growing extensively (Van Niekerk, 2017).

The following sections, in general, introduce initiatives and essential aspects of how information in the internet space in SA is governed through legislation and will include, Electronic Communications and Transactions Act (ECTA), Regulation of Interception of Communications Act (RICA), Protection of Personal Information Act (POPIA) and the National Cybersecurity Policy Framework (NCPF).

3.4.1 The Electronic Communications and Transactions Act

To prevent, react, combat, and mitigate abuse of information systems and yet to encourage the use of e-government services that include the healthcare system, the South African government developed the Electronic Communications and Transactions Act 25 of 2002 (Republic of South Africa, 2002).

The ECT Act is the foundation for moving South Africa towards universal access to electronic communications, providing a human resource with the electronic transaction and forming the source of all other acts (Republic of South Africa, 2002). For example, the South African National e-health strategy makes reference to this act where it puts emphasis on preventing abuse of information exchange in various organisations.

3.4.2 The Protection of Personal Information Act (POPIA)

Post the development of the Electronic Communications and Transactions Act 25 of 2002, according to Sutherland (2017), the flow of personal information outside the borders of the country was still unregulated. In order to regulate information to ensure privacy, SA developed the Protection of Personal Information (POPIA) in 2009 which was enacted on 26 November 2013, and commenced on 1st July 2020 with organisations given until July 2021 to comply and implement.

Many countries adopted similar legislation as strategies to safeguard personal information, including rules and regulations for cross-border transfer and exchange of patient data (Van Niekerk, 2017). In 2011, the national assembly of the Republic of Angola passed a law on the protection of personal data, which outlines principles for data processing, such as transparency, lawfulness, proportionality, accuracy, and the length of retention period (Kurth, 2019). Similar

to SA, their fundamental objective was to approve international (cross-border) data transfers to countries with no adequate level of data protection (Kurth, 2019).

In South African law, POPIA legislation is found to be referenced in most policies; however, Sutherland (2017) posits that our country still falls behind advanced economies in cybersecurity legislation. The Government Gazette (2013) indicates that the act is designed to ensure all South African organisations in the private and public sector including the healthcare sector are accountable when collecting, processing, storing, and sharing someone's personal information should they be abused or compromised. The consensus seems to be that the healthcare sector is found to be progressing in transforming physical patient files to electronic patient information despite the immense security challenges. This has taken place to the extent that cybersecurity has continued to be a growing concern for governments. The POPIA is found to be well thought out and it borrows from the best of other similar international regulations like Angola, learning from their mistakes and shortcomings (Katurura & Cilliers, 2016). The next section will narrow the discussion to cybersecurity legislation.

3.4.3 The National Cybersecurity Policy Framework

According to a research study conducted by Bissiet (2016), compliance moves from best practice to mandatory. The development of the POPIA was considered as a compliance strategy that is meant to provide for the formation of a privacy regulator so to enforce certain controls and perform particular functions in terms of the act. However, given the seriousness of cybersecurity threats in the country, Broeders and Khanna (2015) consider the development of the National Cybersecurity Policy Framework (NCPF) as not just a mandatory requirement but a security measure that will be used to address both the intentional and local incidents and attacks.

Even though it was a slow process to develop the NCPF, the State Security Agent (SSA) supported by the Department for Telecommunications and Postal Services (DTPS) and together with the Department of Communications (DoC) developed the NCPF (South African Government, 2015a). The NCPF was released at the end of 2015 to ensure the confidentiality, integrity, and availability of (CIA) computer data and systems (South African Government, 2015a). The development of this policy, according to Sutherland (2017), was based on foreign experiences which have faster-moving policy formulation and are more advanced in the use of technology.

The extensive coordination to implement the NCPF was driven by various role players that included the state, private and public sector, and community at large (Lejaka, Da Veiga, & Look, 2019). In the public sector, the development of security-related policies is normally carried by the Department of Justice, Crime Prevention chaired by the State Security Agent (SSA) director-general. Their main objective in their agenda was to identify and prioritise areas for intervention and address strategy and decision-making based on assessments of possible threats (Van Niekerk, 2017).

Like many other laws, various policies and strategies that include e-government strategy, ECTA, POPIA, and the State Information Technology Agency (SITA) act were considered in the development of the NCPF; however, critical strategy documents that include e-government strategy, Cyber Warfare Strategy, were either incomplete or not updated (South African Government, 2015). As a result, these critical documents in the formulation of the NCPF framework were not considered. Chaired by the State Security Agent (SSA), a decision-making body known as (JCPS) Cybersecurity response committee was established to prioritise areas of intervention and identify focus areas of attention regarding cybersecurity-related threats (Sutherland, 2017). As mentioned earlier, despite the intense coordination to implement the regulatory framework presented above, cybercrime which is mainly related to the healthcare sector in South Africa has continued to increase (Department of Telecommunications and Postal Services, 2017).

Notably, none of the implemented regulatory frameworks and legislation has either reduced or stopped the continued cybercrime in SA. Presentation of reports from various institutions including IBM and the Ponemon institute Report: “*Cost of a Data Breach Report 2019*”, Verizon Report: “*Data Breach Investigations Report 2019*”, Gartner Report: “*The Urgency to Treat Cybersecurity as a Business Decision*” and the PWC Report: “*2018 Global State of Information Security Survey (GSISS)*” have confirmed that cybercrime in South Africa is on the increase at an alarming rate. These reports support Gartner's (2015) predictions that organisations would lose close to 25% of their strength as a result of not joining the trend of digital transformation in three years (Rojas, Muedas, & Mauricio, 2019).

The next section provides a detailed theoretical framework, which includes the CMM and IST. The contingency factors affecting the effectiveness of healthcare organisations are also discussed

3.5 INTRODUCTION TO MATURITY MODELS

There are many frameworks, models, methods, and checklists that can be used to address common cybersecurity barriers in healthcare organisations, all with their strengths and weaknesses. These frameworks, models, and methods are developed by researchers to guide organisations and to provide a structured approach when responding to concerns. Yet, few can be used to develop a contingency management approach to safeguard information in EHRs (Blair, Pagano, & Burns, 2019).

Murire (2016) posits that theoretical models are in their nature designed to be the anchor of a research project and define its boundaries. This research study explored a few cybersecurity-related models that included Cybersecurity Capability Maturity Model (C2M2), Community Cybersecurity Maturity Model (CCSMM), and Cybersecurity Maturity Model (CMM) which were briefly discussed in Chapter 1 (Section 1.6.3.1).

Additionally, the Protection Motivation Theory and IST were reviewed and the IST was noted as a preferred framework for this study. The IST was briefly discussed in Chapter 1 and was used as a guiding framework to compare the capability of maturity models using its components. This section commences with the importance of the models in a research study followed by each of the models to determine the state of cybersecurity level in the South African healthcare sector.

3.5.1 Importance of maturity models

Maturity models are useful in guiding an organisation's readiness for any proposed state of maturity that can lead to a secured state which an organisation prefers (White, 2007). The United States Department of Defense (2020) defines maturity models as a range of industry standards, patterns, characteristics, indicators, and attributes that determine a company's capability to defend itself against cybersecurity threats. An organisation can use a maturity model as a benchmark to evaluate its current level of capability of methods and practices and use the results to define priorities for improvement. Many of these models take on a similar form of evaluation steps used to assess the level of capability for improvements. Figure 6 below depicts a common structure of maturity models used today.

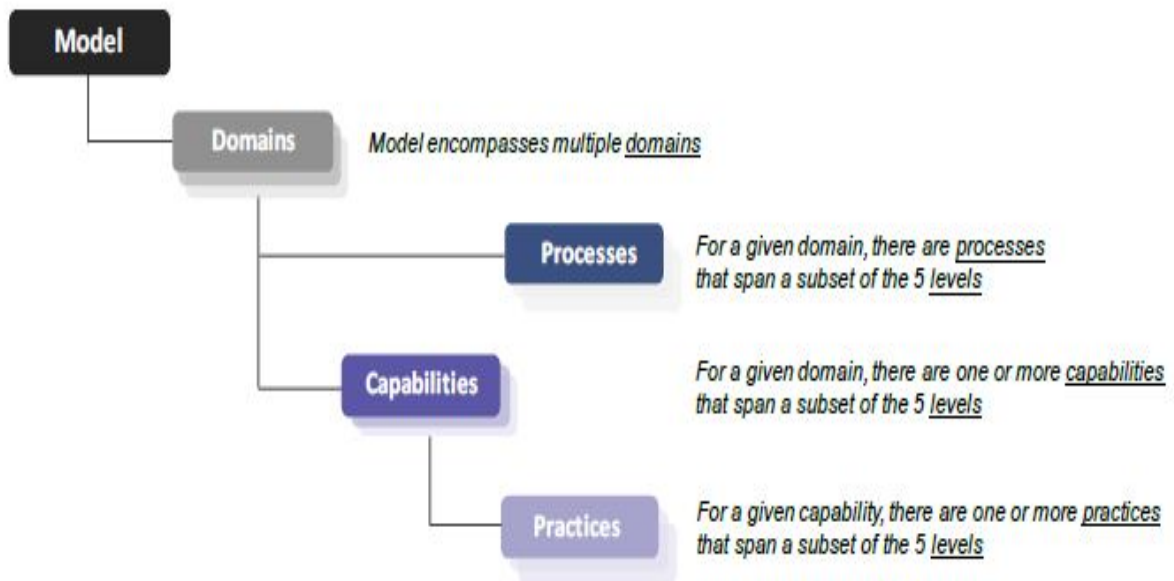


Figure 6: Model and domain elements

(NICCS, 2014)

As mentioned earlier in Chapter 1 Section 1.6.1, two examples of maturity models were chosen because they were able to classify organisation cybersecurity maturity into distinct levels. Both these models encompassed multiple domains or categories that provide an overarching organisational structure of the model (Almuhammadi & Alsaleh, 2017). The models also entailed processes that span as a subset of identified domains designed to act as a step-by-step guide to be used by an organisation. These processes are followed by one or more capabilities that respond to each of the processes. Burke et al. (2019) refer to capabilities as a method of measuring the security preparedness of an organisation.

According to Whitman and Mattord (2018), to address issues of cybersecurity capability, an organisation feasibility study is required, where the maturity of information security is examined through a process of examining existing patterns, characteristics, indicators, and attributes that define the state of cybersecurity capability. According to Whitman and Mattord (2018), ensuring continuous availability of information security systems requires the cooperation of both managers in information technology (IT) and information security. Finally, some practices are derived from each of the capabilities or categories that can be used in an organisation as a standard guideline to be followed in the implementation process. The following section discusses the first model, Cybersecurity Capability Maturity Model (C2M2).

3.5.2 The Cybersecurity Capability Maturity Model (C2M2) architecture

In the previous section, the importance of the maturity models to guide an organisation's readiness to prevent, protect and guide against cybersecurity threats was discussed (White, 2007). A capability maturity model (CMM), according to Aliyu et al. (2020) and Mohammed and Bade (2019), investigates the maturity of the business and improves the controls employed to secure the information. The C2M2 was developed in 2012 and later updated in 2014 and 2019 (HITRUST Alliance, 2016).

The model in the United States of America's Department of Energy (DOE) programme supports businesses to voluntarily evaluate their cybersecurity capability consistently. This model was developed by a group of government experts together with advisors from the industry, academia and was headed by both the Departments of Energy and Homeland Security (Gourisetti, Sri, Mylrea, & Patangia, 2020). The model was originally designed to respond to critical infrastructure setting; however, it was later updated in 2014 to accommodate most of the sectors including the cybersecurity sector.

In the healthcare sector, the EHRs that are designed to improve the quality, efficiency, and safety of patient life are increasingly vulnerable to cyberattack (Onuiri et al., 2015). Electronic health records were defined as technology means to patients' safety; however, the dawn of cyberspace has resulted in these records being vulnerable to cyberspace and increased criminal, hostile action, and potential threats (Kruse et al., 2017). The healthcare industry as a result, according to CISA (2020) has turned to cybersecurity maturity models to provide means to assess and report the state of affairs concerning cybersecurity readiness. The following section shows components of the C2M2.

3.5.2.1 C2M2 components

The C2M2 consists of two components according to Mohammed and Bade (2019),

- i) methodology of measuring and describing object evolution in a sequential manner; and
- ii) criteria for evaluating the capability of objects, e.g. conditions, processes, or application targets.

According to Karabacak, Yildirim, and Baykal (2016), these components together will provide a sequential structure of maturity levels categorised in the form of a list of domains that are organised into objectives. Gourisetti, Mylrea, and Patangia (2020) agree with the previous author, the conceptual framework of C2M2 contains ten domains with each domain organised

by objectives. This is followed by evaluation steps that are used to assess the level of capability for improvements of the business. Each of the objectives in a domain consists of a set of practices that are grouped by the maturity indicator level (MIL). Figure 7 below summarises the elements of each of the domain.

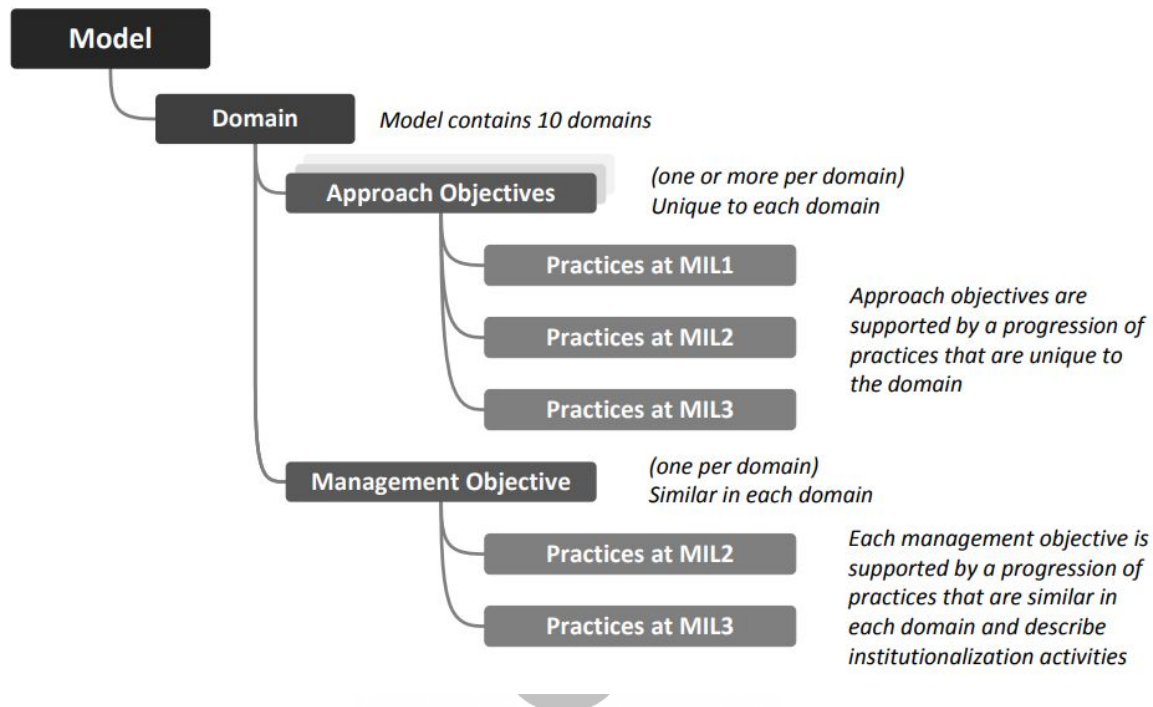


Figure 7: C2M2 Domain elements

(NICCS, 2014)

3.5.2.2 The C2M2 maturity indicator levels

An important question that has to be asked concerning the safeguarding of information in the EHR is whether the maturity model will cover all the requirements of the business. Indeed, the C2M2 represents an anticipated, desired evolution path of objectives shaped as maturity levels (Gourisetti, Sri, et al., 2020).

The C2M2 model interprets four maturity indicator levels, from MIL0 to MIL3 which uniquely apply to each of the domains. These MILs according to Christopher et al. (2015) interpret a dual progression of maturity including an approach progression and an institutionalisation progression as illustrated by the C2M2 maturity levels in Figure 8 below.

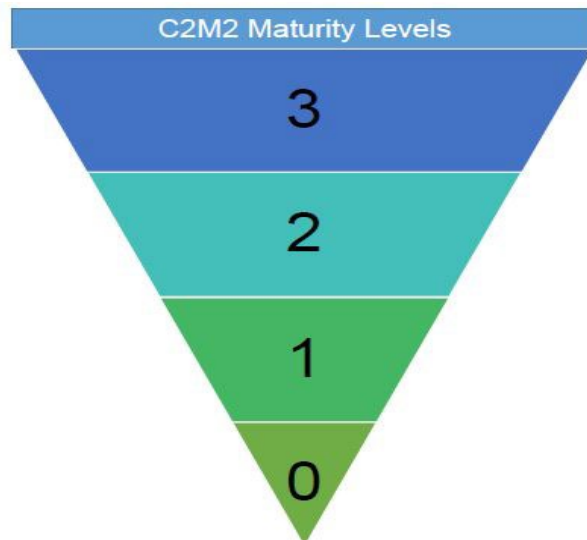


Figure 8: Cybersecurity capability maturity model levels

(C2M2, 2014)

i) MIL0 Level

The C2M2 at the maturity indicator level 0 contains no practices (Gourisetti et al., 2020). This reflects an organisation that has no strategy in place or risk mitigation plans and that the performance in a given domain has not been achieved.

ii) MIL1 Level

The MIL 1 indicates that the business has established a strategy programme for the cybersecurity environment (Gourisetti, Sri, et al., 2020). At this level, risks are identified and documented, at least in an ad hoc manner. Documented risks are mitigated following a strategy programme, accepted, avoided, or transferred at least in an ad hoc manner (Gourisetti, Sri, et al., 2020). According to a baseline study on cybersecurity readiness conducted by the Department of Telecommunications and Postal Services (2017) present, 37% of the respondent organisations have discussed a cybersecurity plan or strategy and will implement in future, meanwhile over 29% of respondent organisations have fully functional plans in place. The 37% of organisations can be categorised as those that are in MIL1 Level of the C2M2 model.

iii) MIL2 Level

At this level, activities in a particular domain represent an initial level of institutionalisation with at least four management practices present (Ursillo & Arnold, 2019). The four management practices according to Ursillo and Arnold (2019) include the following:

- Practices are documented;

- Stakeholders of the practice are identified and involved;
- Adequate resources are provided to support the process (people, funding, and tools); and
- Standards and/or guidelines have been identified to guide the implementation of the practices.

According to Christopher et al. (2015), the cybersecurity strategy programme defined in the MIL2 level of the C2M2 model includes an objective of the organisation's cybersecurity activities. The cybersecurity priorities of the strategy programme are documented and aligned to the organisation's strategic objectives and risk to medical records. The oversight and governance of cybersecurity activities are provided through a cybersecurity programme oversight and are defined in the cybersecurity programme strategy. Furthermore, the structure and organisation of the cybersecurity programme are defined in the programme strategy. The approval of the cybersecurity programme has followed the established governance structures through the senior management.



iv) MIL3 Level

At this level, activities have been further institutionalised in a specific domain (Ursillo & Arnold, 2019). The cybersecurity strategy programme on maturity indicator level 3 is updated to reflect organisation changes, changes in threat profile, and changes in the operating environment (Christopher et al., 2014). The progression of this level is supported by five management practices, including:

- activities are policy driven and governance structured;
- compliance requirements are specified in policies and include specified standards and/or guidelines;
- to ensure conformance to policy, activities are periodically reviewed;
- responsibility and authority for performing the practices are assigned to personnel; and
- personnel performing the practices have adequate skills and knowledge.

Although the C2M2 maturity indicator includes health as a benefit, it does not explicitly include this sector in the cybersecurity capacity maturity model (Burke et al., 2019). The maturity model for a nation as it is called by Burke et al. (2019) has exposed many drawbacks when compared to the CMM. Therefore, it is argued in this study that the C2M2 is not yet developed

enough in order to address the entire scope of contingency management and the magnitude of cyber threats facing the healthcare sector in South Africa.

3.5.3 Cybersecurity Maturity Model (CMM)

The global increase of cyber intrusion into the healthcare sector demonstrated the need for improved cybersecurity. Worldwide, cybersecurity has become a shared responsibility and a priority that requires adequate motivation to develop a comprehensive CMM (Le & Hoang, 2017). However, one of the main problems is how to assess the level of cybersecurity to mitigate the increasing risks associated with cyber threats. As a result, many security models have been developed to lead the way in safeguarding cyberspace (Le & Hoang, 2017). Escalated realisation of cybersecurity threats to patient records has realised the need to assess and report on the readiness of the healthcare sector using cybersecurity maturity models (Al-Matari, Helal, Mazen, & Elhennawy, 2021).

In recent years, maturity models were intended to help organisations to evaluate and make improvements to their cybersecurity programmes. Mohammed and Bade (2019) posit that maturity models are designed to offer a point of reference in an organisation using their set of characteristics, attributes, patterns, and indicators. To assess organization readiness to monitor and respond to potential breaches, Nemertes Research, based on their four-level cybersecurity maturity model (Till, 2019), developed a model similar to the United States National Institute of Standards and Technology (NIST) cybersecurity framework. The CMM model is designed to protect sensitive customer and proprietary data, as well as comply with legislation to ensure the best services to customers (Le & Hoang, 2017).

The CMM model focuses on operational metrics Till (2019); specifically, the time required to do the following:

- Distinguish that something potentially unsafe has occurred;
- Comprehend whether the incidence represents a breach; and, if so
- Contain the breach.

These metrics were used as a measure to validate the cybersecurity maturity model to distinguish if the higher level of maturity can correspond to better operational security (Till, 2019). Figure 9 below presents the Cybersecurity Maturity Model.

Cybersecurity maturity model



Figure 9: Cybersecurity Maturity Model

(Till, 2019)

The model uses NIST and ISO standards to define maturity level and baseline for the implementation of best security practices (Almuhammadi & Alsaleh, 2017a; Henriques, Pereira, Almeida, & Mira da Silva, 2020). As was indicated in Chapter 1 (Section 1.6.3.1), the approach to use CMM model levels to evaluate the organisation's maturity is based on its simplified version of the National Institute of Standards and Technology (NIST) cybersecurity framework.

The model will use its metrics levels (*Unprepared, Proactive, Reactive, and Anticipatory*) as a guide to identifying healthcare organisations' (HCOs') information security maturity and develop improvements to address the contingency factors that are affecting the effectiveness of HCOs. The growing aggressiveness of these attacks caused an increasing difficulty in HCOs to achieve their objectives (Feix & Procházka, 2017). In addition to healthcare facility cyberattacks, according to Rojas et al. (2019), is the result of a lack of maturity models that allow facilities to perform post evaluation monitoring. Thus, the nature and designs of these models do not address the risk factors.

Olden (2016) agrees with this opinion saying the organisation's success will be limited if they mostly depend on policies and have not implemented maturity models. The application of CMM, according to Akinsanya, Papadaki, and Sun (2019), to assess healthcare organisations fortunately result in domain precise problems when mapping healthcare specific processes. The reason for this is because its narrow properties and comprehensive assessment of the processes concerned with the maturity level (Ross, 2017) are very strong (Ross, 2017).

3.5.1 *The CMM maturity levels*

Even though the importance of the CMM model was presented with four maturity levels assigned with names that are indicative of the threat types and activities they are to address, most healthcare institutions use each maturity level of a chosen model as an objective and look for their objective to get to the next maturity level of a model (Akinsanya et al., 2020). As presented in Figure 9 above, each of the maturity levels in the model has a predefined set of characteristics, as follows:

- i) *Level 0*. This level is characterised by the healthcare organisations that have no defined policies or procedures to safeguard the institution (Akinsanya et al., 2020). In Figure 9, this level is referred to as the *Unprepared level* because of its elementary practical implementation in security systems, being unreliable, and unable to respond to current or emerging attacks. The Department of Telecommunications and Postal Services (2017) presents a report on cybersecurity readiness in South Africa in which 53% of the organisation had no cybersecurity policies, plans, and procedures.
- ii) *Level 1*. In Figure 9, this level was referred to as the *Reactive level* where its elements are designed to help an organisation establish, maintain and improve upon the security processes required to address cybersecurity challenges (White, 2007). Healthcare organisations are found with basic security mechanisms, platforms, and structures to respond to and handle organisational cybersecurity threats; however, they can't protect the organisation effectively against future threats (Akinsanya et al., 2020). The focus at this level results in the perception that systems are protected, with protection of essential systems. The Department of Telecommunications and Postal Services (2017) presented 37% of healthcare facilities to have discussed basic requirements for cybersecurity like a cybersecurity plan/strategy, security infrastructure; however, these are not implemented. According to Mohammed and Bade (2019), the levels require healthcare facilities to

establish and document practices and policies, and resource plans demonstrating the management of activities that will ensure proper implementation of security measures.

iii) *Level 2.* of the model is the *Proactive Level* and demonstrates that organisations in the healthcare sector are aware of the cybersecurity issues and have the processes and mechanisms in place to detect security incidents (Akinsanya et al., 2020). According to White (2015), the model supports organisations lacking the necessary information to develop strategies to move from an ‘*Unprepared*’ state of maturity to where an organisation has defined processes, platforms, and structure to proactively address issues of cybersecurity. As an additional concern, the majority of cybersecurity metrics are measured using qualitative approaches, in order to provide organizations with compliance instead of motivating security improvement (Henriques et al., 2020). The main objective of this level is to promote existing legislation as far as an information sharing mechanism is concerned within the healthcare sector to enable hospitals to share patient information (Feix & Procházka, 2017).

iv) *Level 3.* of the model is the top-level and referred to as an *Anticipatory level*. At this level, healthcare organisations have implemented real-time monitoring of cybersecurity risk and cybersecurity threats, making use of risk assessment tools as the driver of security investment (Akinsanya et al., 2020).

The next section presents the threat landscape in SA where the hospital systems are compromised by different types of attacks. The section describes examples of threats and gives detailed incidents that occurred in various healthcare facilities in South Africa.

3.5.4 The threats landscape

According to the KPMG (2015) report, the frequent growth of healthcare organisations that are under attack by cyberattackers is alarming in SA. Indeed, the report presented that over the past 12 months, on average, healthcare facilities have been victims of at least one cyberattack per month. In chapter 1 (Section 1.6.4), threat types that concerned healthcare information were identified; however, the model is not capable of categorising existing threats but rather characterising various incidents that can happen.

Van Heerden, Von Soms, and Mooi (2016) in their research paper posit that cybersecurity attacks can be classified according to the aggressors, hackers, or attackers' point of view or even from the victim's point of view. According to Akinsanya et al. (2019), the CMM model identification process to threats is based on several elements which include: *the time to set up*

the attack, who to attack, and what motivates the individual to attack. The model identified two categories of attacks: structured and unstructured threats.

3.5.4.1 Structured threat attack

In today's computerised world, businesses are under immense pressure to protect information assets, according to Whitman and Mattord (2018), with threat agents finding vulnerabilities in the healthcare systems. As discussed in previous sections, several research studies in recent years have observed cyber threats and attacks growing in huge percentages. Coventry and Branley (2018) in their research study indicated that the increased connectivity to the internet has resulted in the healthcare sector being an attractive target for cybercrime. Patient data (age, blood type, medical history, past surgeries, diagnoses, laboratory test results, immunization, radiology images, and contents of health status) is especially valuable to cybercriminals because of its unchangeable aspects (Malakoane, Heunis, Chikobvu, Kigozi, & Kruger, 2020).

In agreeing that various categories of threat attack exist, Land (2016) maintains that the structured threat attacks are used by threat actors to compromise organisation information focusing on most important areas such as confidentiality, integrity, and availability of information. Patient health data resides in a healthcare facility infrastructure over which a patient has no control. The case of Charlotte Maxeke Academic Hospital in Johannesburg, SA, where the hospital systems were compromised by a ransomware attack according to News24 (2019), was categorised as a structured attack. The attack compromised patient information and demanded a bitcoin as ransom. These attacks are found to be planned and organised, targeting the healthcare facility by a sophisticated group of criminals (World Economic Forum, 2019).

Security experts report that Life Healthcare Group, the country's second-largest private hospital operator, has seen most of its facilities across the country attacked by ransomware (Bottomley, 2020). Amid the COVID-19 pandemic, Life Healthcare was bringing cybersecurity experts and forensic teams from outside the country to assist internal employees and to advise in resolving the issue (Mungadze, 2020). Even though the group did not reveal the extent of the damage from the cyberattack, they claimed the attack concentrated on patient-sensitive data, and they further revealed that the security incident affected admission systems, business processing systems, and their email servers (Bottomley, 2020).

At the end of October 2020, during the COVID-19 Level 3 in South Africa, an unexpected 45% increase of ransomware attacks at clinics and in non-profit organisations was noticed,

according to a report published by Check Point Research on hospitals (Latham, 2021). The healthcare sector, being the most targeted in cyberattacks compared to other industries worldwide, experienced an increase of about 22% toward the end of the year 2020, bringing South Africa to an astounding 66%. With the South African healthcare sector under severe strain during COVID-19, cybercriminals exploited gaps in healthcare facilities' security software and increased their attacks by 626 in December 2020 from 430 in October 2020. In

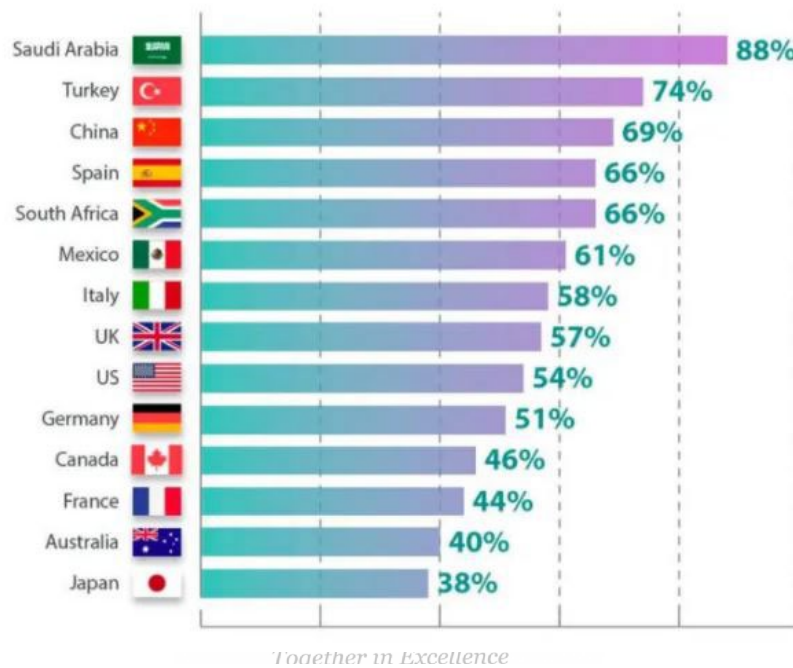


Figure 10: Ransomware attacks in 2020 around the world

(MSP, 2019)

Figure 10 above, the Cybersecurity and Infrastructure Security Agency present the ransomware activity targeting the private healthcare and public health sector.

According to Le Bris and Asri (2017), the major challenge of the health sector is the multiplicity of healthcare practitioners handling electronic health records resulting in multiple potential targets. Akinsanya et al. (2019) refer to threats in this category as those that are characterised by methodical attacks using a systematic approach to disrupt, corrupt or compromise patient information systems for financial gain. Yassine, Singh, Hossain, and Muhammad (2019) agree with this statement saying that structured attacks are usually an act of one or more individuals with an intent to harm one or more system of an organisation, which differs from unstructured threat attacks.

3.5.4.2 Unstructured threat attack

Unstructured threat attacks are said to be committed by individuals with limited or developing skills and are unfocused to assault one or more network systems (Park, 2018). The attackers' main focus is to maximise their gain of recognition in the field of attackers or their financial cost. For example, when the attackers gain access to EHRs, they select data that is especially valued like blood type, surgeries, and diagnoses because of the unique personal health information (Flahault et al., 2018). In that way, the attackers will generate high profits with the least effort. The Southern African Fraud Prevention Service (SAFPS) has released a statistic showing that cybercriminals have become less interested in the theft of large amounts of personal information (Business Tech, 2019). Cybercriminals target bad consumer behaviour to commit cybercrimes to an organisation making use of their credentials to authenticate to organisation networks.

According to Van Heerden, Von Soms, and Mooi (2016), large businesses in SA refuse to declare cyberattacks and release their identity in fear of being attacked again. The assertions of the previous writers are also found in the “*Major spike in SA cyber-attacks*” malware report by Kaspersky 2019, where there report presented 22% of South African organisations are experiencing malware attacks (C. Smith, 2019). In the next section, the theoretical framework of the study is discussed.

 University of Fort Hare
Together in Excellence

3.6 THEORETICAL FRAMEWORK

To gain a better understanding of the reasons why the healthcare sector is under immense attack by cybercriminals, this study relied on existing theories, including the PMT and IST. These theories have interesting views of security protection and prevention. In many of them, if not all, their central focus is to provide defensive mechanisms to protect people and organisations. Studies in Information Systems (IS) are increasingly relying on sociological theories such as PMTs and ISTs, according to Nunu (2019). They were used mainly to direct the collection and analysis of data and to comprehend why IS deployments are implemented in the manner they've been. Each of these sociological theories are discussed in detail below.

3.6.1 Protection motivation theory (PMT)

The everlasting interest of criminologists is responding to actual and perceived threats of victimisation (Clubb & Hinkle, 2015). The protection motivation theory (PMT) which was originally postulated by Ronald Rogers in 1975, is by far the most widely used, and was designed to provide conceptual clarity to the understanding of fear appeals (Clubb & Hinkle,

2015). Rogers (1983) improved and extended the theory to a more general theory of persuasive communication, putting more emphasis on cognitive processes to better understand how and why individuals respond to potential threats to their health and safety (Clubb & Hinkle, 2015). While researchers noticed an increase in the development and implementation of EHRs, according to Izaara, Ssembatya, and Kagwa, (2018), there has been a behavioural change noticed through an increased number of attacks in the healthcare sector. For example, in the last decade, there has been a gradual change in the increase of cybersecurity attacks in both public and private hospitals. Some authors accuse the increase in medical devices connected to the internet, others point fingers to a lack of governance implementation, while others say the lack of skills in the field of security is the reason for behavioural change. Figure 11 below depicts the basic components of the PMT as detailed by Rogers (1983).

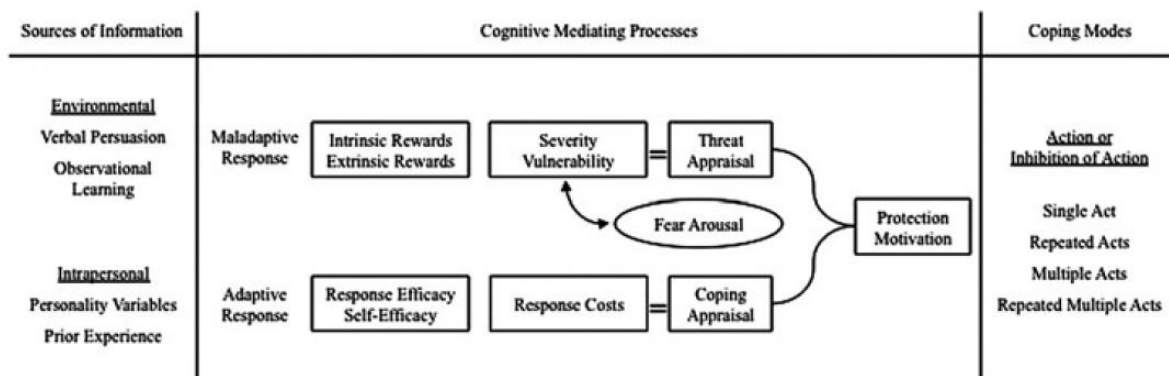


Figure 11: Protection motivation theory

(Rogers, 1983)

Protection motivation adopts a similar strategy to that of risk management found in the IST and is the result of threat appraisal, according to Rogers (1983), with its design partially based on the work of both Lazarus (1966) and Leventhal (1970). The following section provides the limitations of the PMT.

3.6.1.1 Limitations of protection motivation theory

Depicted in Rogers' (1983) diagram of the protection motivation theory, the contextual characteristics associated with the use of the theory has revealed some limitation (Clubb & Hinkle, 2015). The PMT theory has shown two factors in its structure, the individual and environmental factors which can either provide encouragement or discouragement for getting into protective behaviour. According to Diesch, Pfaff, and Krcmar (2020), recent studies have shown engagement measures that can be employed by businesses to protect their assets:

- *Threat appraisal process* – cognitive mediating process where an organisation assesses the extent to which they are to be affected by a given type of criminal threat. In this process, the severity, vulnerability, and fear arousal are considered.
- *Coping appraisal process* - while a threat appraisal process gives a cost-benefit analysis for potential benefit, the coping appraisal process provides a subjective analysis for projected protective measures to mitigate and or prevent criminal threats. In this process, response efficacy, self-efficacy, and response cost are also considered to prevent or mitigate a potential criminal threat.

In summary, it can be concluded that constructs of the theory variables are appealing, in that the protective measures are a response to criminal victimisation and can protect individuals and their property (Clubb & Hinkle, 2015). Furthermore, the theory has been recognised in the healthcare sector in explaining the use of specific protective methods. However, the theory lacks a contingent management aspect that deals with multiple processes such as information audit, internal control, and risk management that respond to organisation objectives. The next section discusses in detail the integrated system theory.

3.6.2 Integrated system theory (IST) background

Since the popularity of electronic commerce, many businesses are experiencing unprecedented security challenges (Olden, 2016). The biggest challenge is maintaining the security and privacy of the protected health information that is transmitted within an organisation (Anderson, Baskerville, & Kaul, 2017). Management tools and security techniques have apprehended a lot of attention from both academia and practitioners (Kessler & Hitt, 2016). However, according to Alqurshi (2020), this is a result of a lack of a theoretical framework for information security management.

Based on contingency management, the IST incorporates information security policy, risk management, internal control, and information audit theories to construct information security architecture that is compliant with organizational objectives (Anderson, Baskerville, & Kaul, 2017). While the integration of various theories is also important to enhance clinical, operational, and managerial outcomes in the healthcare sector, audit, security, and privacy have been a crucial impediment to adoption (Anderson et al., 2017). The following section describes how the IST is constructed.

3.6.2.1 The construction of a theory

The construction of a theory is a creative process of assembling, developing concepts, constructs, and components of theory (Du, Vidal, & Markovsky, 2019). To respond to unprecedented challenges, IST was developed on the basis of contingency management, and it incorporates five different theories related to information security management, which are discussed further in this chapter. These theories include security policy theory, risk management theory, control, and audit theory, contingency theory, and lastly the management systems theory which take a dissimilar course in the process of information security management (Anderson, Baskerville, & Kaul, 2017). The result of this amalgamation is constructing an information security architecture that is reconcilable with organisational objectives. Furthermore, while the integration of information systems is also important to enhance clinical, operational, and managerial outcomes in the healthcare sector, audit, security, and privacy have been significant barriers to adoption (Anderson et al., 2017).

Figure 12 below presents the IST framework commencing from the environment which is being addressed, followed by contingency management, five different theories relating to information security management, and finally the organisational objectives.

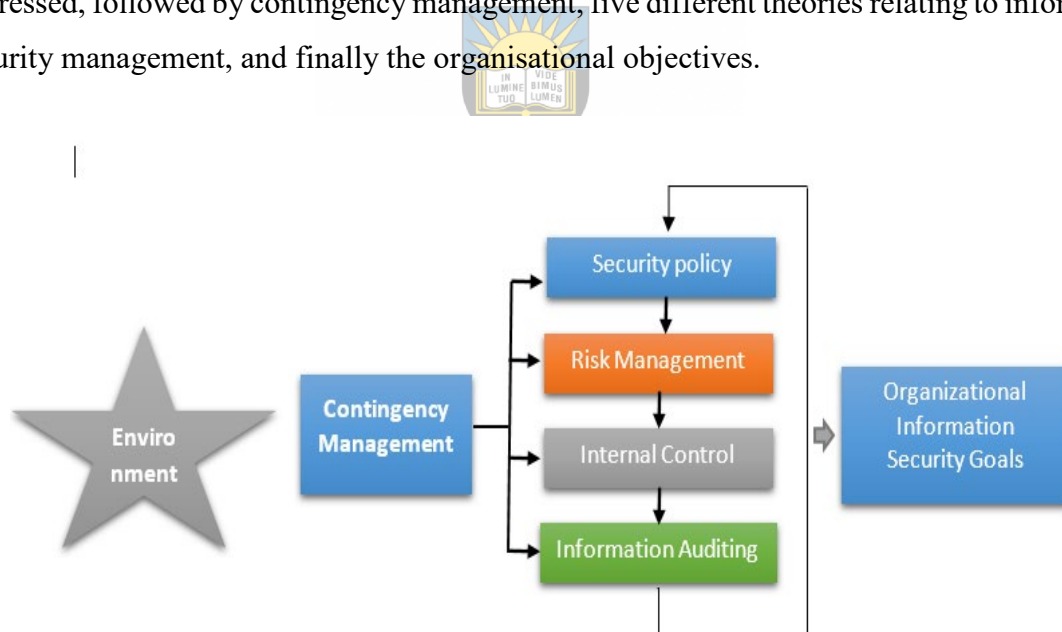


Figure 12: Integrated System Theory

(Hong et al., 2003)

Information security management, according to Diesch et al. (2020), is mostly developed based on international standards and best practices. Similarly, the IST is based on contingency management and five sequential management process in order to respond to and be able to

meet the ever-changing environment (Diesch et al., 2020). As a result, in an organisation, any component of managerial activities could be the focus of contingency management.

The five different theories were transformed to organisational sequential management processes which start from security policy, and then to risk management, internal control to information auditing with contingency processes (Anderson, Baskerville, & Kaul, 2017). Anderson, Baskerville, and Kaul (2017) cite a procedure for contingency management that originates from any security management activity and moves sequentially into each of the forms and processes cycles. Using an example of sequential processes, contingency management could begin at risk management, internal control, and then information auditing and go back to security policy.

Thus, information security management implements a periodic management cycle which could also be independent from other managerial activities (Diesch et al., 2020). Furthermore, Diesch et al. (2020) suggest that managerial activities can happen sequentially, and that each activity can provide input or output for the next one.

The conversation contained in this segment reached at few key elements related to how the IST was constructed. As was indicated earlier, the IST is founded from several theories and is categorised in terms of main security managerial activities, managerial procedures, characteristics, and literature. These theories that created the IST are presented in the following section.

3.6.2.2 Contingency management theory

National and international governance regulations have been challenged with the steady increase of cybercrime (Flowerday & Tuyikeze, 2016). This is due to complex improvements in technology, large-scale increase in information security threats that continue at an alarming rate in the healthcare sector (Somepalli, Tangella, & Yalamanchili, 2020). Zastepa, Sun, Clune, and Mathew (2020) define contingency management as a subset of information security that is concerned with the prevention, detection, and reaction to the threats and vulnerabilities in an organisation. Based on the IST, Hong et al. (2003) proclaim that contingency management could include one or more management activities; however, to successfully achieve organisation objectives, an organisation including the health sector should consider developing information security architecture and following contingency management processes.

Zastepa, Sun, Clune, and Mathew (2020) suggest practitioners consider one or more forms of information security management in order to deal with the complexities of a rapidly changing environment. They suggests for example, security management measures, security policy actions, risk management actions, control and audit actions, or system management actions. The approach to contingency according to Hong et al. (2003) is to distinguish and answer to circumstances' variables to achieve organisational objectives. In essence, contingency management is to oversee environmental interaction inside an institution with a set of technology and other managerial activities so as to attain organisational objectives (Williams et al., 2017). The following section discusses how security policy theory fits within the five other theories.

3.6.2.3 Security policy theory

Currently there is no consistent security policy theory (Park, 2018). Instead, organisations are overwhelmed with policies, standards, and frameworks that do not address core challenges that affect the attainment of organisation objectives (Malakoane et al., 2020; Sutherland, 2017). Compared to other industries, healthcare sector is even more vulnerable to cyberattacks due to its inherent security vulnerabilities (Martin, Martin, Hankin, Darzi, & Kinross, 2017). Ngoqo and Flowerday (2015) suggest that it is important to have standards that define criteria for evaluating the effectiveness of security measures, techniques, the scope of security functions, and features needed for managing information security.

Diesch et al. (2020) posit that an information security policy is created by the organisation to ensure its employees, most importantly those who are using computers, follow security procedures and protocols. Bulgurcu et al. 2016 and Whitman and Mattord (2018) recommend four key components or procedures to be followed when developing an information security policy:

- a) assess and persuade top management;
- b) analyse information security;
- c) form and draft a policy; and
- d) maintain the policy.

However, the information security policy life cycle suggested by Kaušpadienė et al. (2019) addresses four parts:

- a) policy assessment;
- b) risk assessment;
- c) policy development and requirements definitions; and
- d) review trends and operation management.

Despite the available measures, Diesch et al. (2020) posit that in 53% of the attacks in 2019, the healthcare organisations were found to have implemented information security policies but lacked the underlying technology to secure against business harm. Whitman and Mattord (2018) suggest that an organisation should “*know the enemy*” by assessing, examining, and understanding the threats and vulnerabilities of its information assets to lower the risk.

Land (2016) further put forward the assertion that the objective of information security is detecting and preventing unauthorised acts performed by computer users. It is argued by Diesch et al. (2020) that information security is purely a technical concern within an organisation and hence it has become the most important challenge in the modern and global world. For example, to understand the complexity of information security in 2018, only Computer Emergency Response Team (CERT) technology experts were able to detect the abnormality activities in the Norway Regional Health Hospitals. The Norway authorities immediately reported that the EHRs of nearly 2.9 million citizens had been compromised by hackers. However, Reychav et al. (2019) claim a different perspective in this regard, saying that these types of attacks are not only a threat to information technology resources but also to patients and the financials of the organisation.

Ponemon Institute (2019) raised further concerns about the information risk and the consequences to patient safety. Additionally, Kaušpadienė, Ramanauskaitė, and Čenysd (2019) define information security as keeping information assets confidential, secure, and accessible.

To sum up, information security policy goals are planning information security requirements, creating consensus in the business, drafting and implementing a policy, and finally reviewing the policy regularly so as to attain the business demands (Diesch et al., 2020). The following section details the risk management theory.

3.6.2.4 Risk management theory

Part of information security governance is the establishment and support of effective risk management (Masum, 2018). Whitman and Mattord (2018) define risk management as a process of identifying, carrying, and assessing risk to carry out decision steps to reduce it to an acceptable level. According to IBM and the Ponemon Institute report, in the period between 2017 and 2019 the healthcare sector was amongst the highest attacked by cybersecurity which raised a need for better risk management in the public sector. According to Diesch et al. (2020), threats and vulnerabilities could be assessed and estimated through organisation risk and analysis as far as the risk management theory is concerned.

During the adoption of EHRs in South Africa, risk assessment was carried out to understand the factors that could affect the implementation of EHRs (Thomas, 2016). Thomas (2016) further put forward that some of these factors included lack of government backing to implement EHR, technology readiness, poor implementation. Le Bris and Asri (2017) posit that the criticality of patients' well-being and safety is a result of healthcare organisations' sensitive infrastructure. For example, hospitals' exposure to cybersecurity threats is due to connected medical devices that manage health plans, health records, and patients' critical information. Van Niekerk, (2017) suggests three major undertakings to manage and control organisational risk and protect information assets: *risk identification*, *risk assessment*, and *risk control*.

i) Risk identification

As mentioned previously in this research, the adoption of EHRs in the healthcare sector carried numerous risk challenges. One of the main challenges of the healthcare sector is many threat actors handling EHRs resulting in numerous potential targets (Le Bris & Asri, 2017). As a result, in recent years, the topic of risk management in healthcare organisations has moved up the agenda of both public and private sectors. The period between 2010 and 2016, according to Somepalli, Tangella, and Yalamanchili (2020), marked the publication of a series of reports that drew attention for better risk management within the healthcare industry.

Anderson and Williams (2018) refer to the identification of the risk as a standard risk management process performed by using several instruments such as internal records of the organisation, risk analysis questionnaires, and policy checklists. Whitman and Mattord (2018) define risk identification as a process in risk management that requires risk owners to document, enumerate and understand the current information and system in an or organisation.

ii) Risk assessment

Accordingly, the evaluation of risk involves measuring the potential size of the loss and the probability that it would occur (Quay-De La Vallee, Selby, & Krishnamurthi, 2016). Thomas (2016) posits that during the adoption of EHRs in SA, risk assessment was carried to understand the factors that could affect the implementation of EHRs. Determining the extent to which an organisation's information assets are exposed to risk is a process of risk assessment in risk management, according to Whitman and Mattord (2018). An important asset in healthcare centres, according to Cilliers and Katurura (2018), is the patient health record.

Flahault et al. (2018) warn that when the healthcare facility's patient health record is compromised criminals can have access to information such as date of birth, address, patient names, and healthcare provider information. In order to evaluate the impact on a healthcare facility, measuring the potential size of the loss of data and the probability that it would occur, a sequence of evaluation steps would need to be carried out (Diesch et al., 2020). Van Niekerk (2017) stresses that the effect of the cyberattack on patient health is regarded as the most critical and can affect the patient in many ways and organisations thus need to perform a proper risk assessment. For example, manipulation of surgical machines' data can result in invalid results of a patient during an examination.



University of Fort Hare
Together in Excellence

iii) Risk control process

Finally, the availability of healthcare service is also categorised as one of the most important and critical key assets that when hospital operations are affected by cyberattacks, they can place the health and well-being of the patient at risk (Flahault et al., 2018). The concept of risk control is defined by Whitman and Mattord (2018) as the use of controls that reduce the exposure of an organization's information assets to an acceptable level. Van Niekerk (2017) puts more emphasis on risk control saying that when it is not implemented, an organisation can suffer variabilities to its information asset.

The Life Healthcare hospitals in South Africa were attacked a cybercriminal attack on their information systems (Bottomley, 2020). This incident is similar to that of Charlotte Maxeke Academic Hospital in Johannesburg, South Africa, where the hospital systems were compromised by a ransomware attack, as reported by News24 (2019). However, according to Bottomley (2020), most of these healthcare hospitals refuse to share information on the nature of the attack as they are concerned about sensitive data. In the light of the nature and importance of managing and controlling organisational risk, risk identification, risk assessment, and risk

control were discussed and the next section discusses the control and audit of the integrated system theory.

As is evident the above, to place information security risk under an acceptable level, and actualise the control procedures, it is important to perform a risk assessment. The the primary risk assessment challenges in an organisation have already been examined and thus the following section explores the controls and audits.

3.6.2.5 Control and audit theory

Consequently, as experts state in de Kleijn and Van Leeuwen (2018), the aim of control and auditing theory is for businesses to implement information security control systems, and once implemented, auditing processes should be conducted to evaluate the effectiveness of these controls. Information Security Standard ISO/IEC 17799 suggests best practices of control objectives for information security management to be followed to mitigate issues of a security breach (Hong, Chi, Chao, and Tang, 2003). The following are recommended best practices for control objectives:

- i) Define a security policy;
- ii) Undertake organisational security;
- iii) Classify assets and control;
- iv) Ensure personnel security;
- v) Perform physical and environmental security;
- vi) Ensure communication and operation security;
- vii) Provide access control; and
- viii) Maintain and develop systems.



University of Fort Hare
Together in Excellence

From the previously mentioned best practices, note that it is important to note that control and audit are important components of the integrated system theory that are designed to mitigate issues of cybersecurity security breach and are designed to foster a cybersecurity culture in an organisation. It is patent in the above-mentioned best practices by the IST that information security is key in the healthcare sector and that to meet the demands of a fast-changing environment, it is necessary to discuss the contingency process. Based upon the above analysis, businesses should refer to information security standards and establish information security

strategies in order to form security control objectives. The following final section discusses the management system theory.

3.6.2.6 Management system theory

The process of securing information and information assets so that they remain confidential, their integrity is preserved, and their accessibility is maintained (Almuhammadi & Alsaleh, 2017). It is therefore a critical challenge for organisations, their clients, and the public. Out of 223 organisations surveyed, the healthcare sector is regarded as one of the most targeted globally, with cybercriminals targeting patient information (Martin et al., 2017). However, the management systems theory, according to Diesch et al. (2020), emphasizes that organisations should establish and maintain a document information security management (ISMS) to maintain confidentiality, integrity, and availability of information assets.

To circumvent this challenge, ISMS suggests six steps that organisations need to follow:

- i) Define the security policy;
- ii) Define the ISMS scope;
- iii) Assess risk;
- iv) Manage risk;
- v) Select appropriate controls; and
- vi) Create a statement of applicability.



University of Fort Hare
Together in Excellence

Al-Dhahri, Al-Sarti, and Abdul (2017) suggest that businesses should review the environment and current security standards to ascertain an information security policy, define the scope of information security and risk control to form an information security management system (ISMS). The next section makes concluding remarks on this chapter.

3.7 CONCLUSION

This chapter introduced and provided the background on public healthcare, electronic health records, and cybersecurity. The purpose of this chapter was to introduce the reader to the theoretical foundation of this research study. Technology has allowed interaction between the public sector and its citizens through the internet, thereby allowing even patients at the hospitals to view, read or sign their patient health records using their mobile devices. However, the increase of technology devices has increased patients' concerns about the security of their

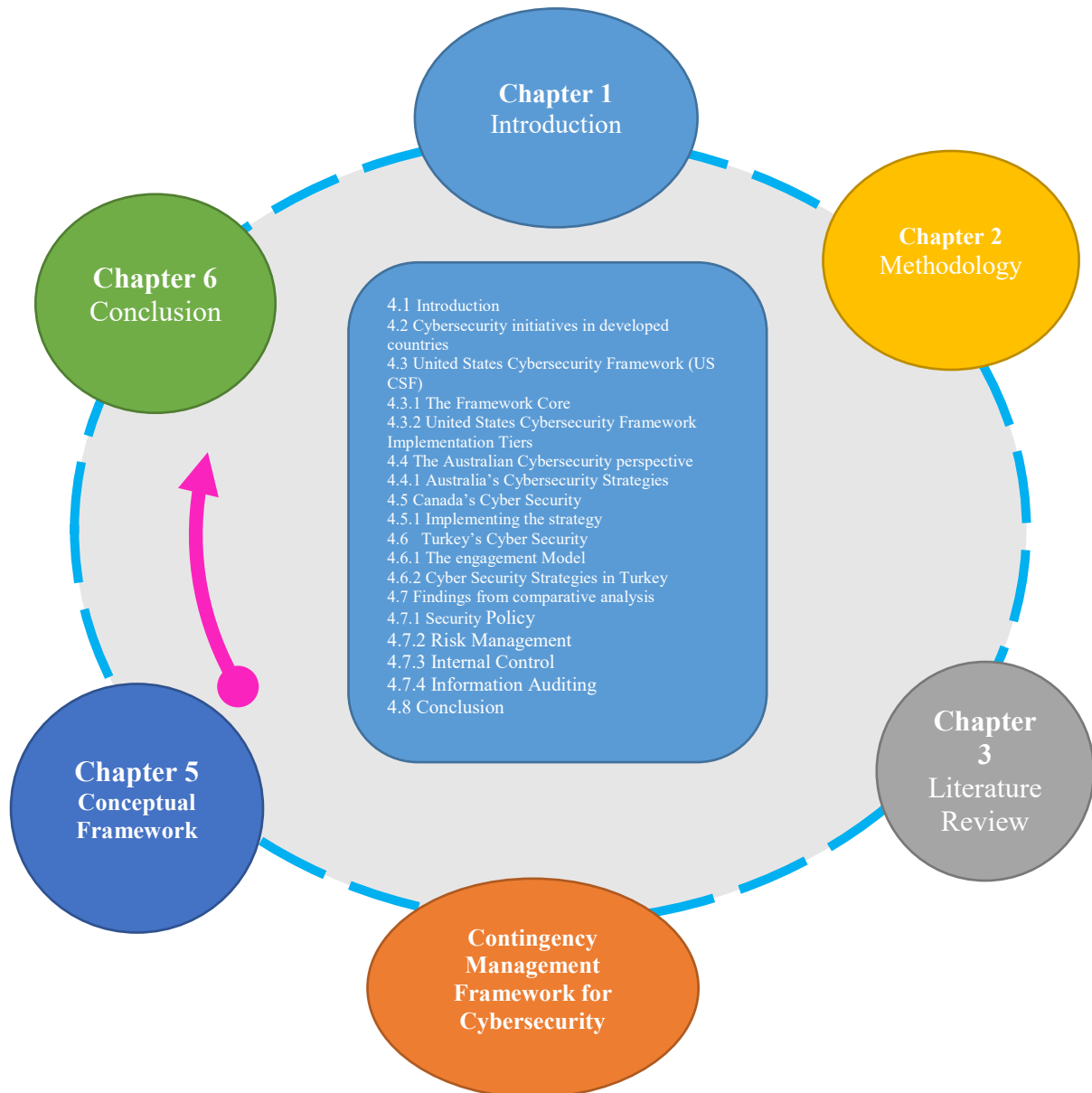
EHRs. The lack of cyber protection in healthcare institutions has resulted in the healthcare sector being regarded as one of the top targeted sectors.

South Africa is seen making strides in developing government legislation to prevent public healthcare and other sectors from cybersecurity threats. However, reports indicate about 44% of the organisations have overall information security strategies. This is in response to global attacks even though most of the African countries are said to be at their fundamental stages in implementing policies to guide the protection of their environment.



University of Fort Hare
Together in Excellence

CHAPTER 4: CONTINGENCY MANAGEMENT FRAMEWORK FOR CYBERSECURITY



4.1 INTRODUCTION

The discussion of the previous chapter provided an understanding of how contingency management safeguards the information in electronic health records (EHRs) against cybersecurity threats. In this chapter, the focus is on how a contingency management framework can secure EHRs against cybersecurity threats. This chapter compares, evaluates, and discusses various cybersecurity models, strategies, and frameworks chosen from various countries and introduces the IST.

As was indicated in earlier chapters, both the public and private sectors are vulnerable to cyberattacks. The protection of healthcare information in these organisations has become a significant issue. Even though there are plenty of frameworks, models and strategies developed to address issues of information security management, surprisingly there not much that addresses contingent management to safeguard EHRs (Chang & Coppel, 2020).

According to Shah and Khan (2020), the Health Insurance Portability and Accountability Act of 1996 (HIPPA) necessitated the United States Department of Health and Human Services (HHS) to develop regulations that safeguard the privacy and security of certain health information including patient information. In the same vein, the National Infrastructure Plan (NIPP) directed by Presidential Policy Directive 21 (PPD-21) required both the private and public sectors to improve information security and resilience of the nation's infrastructure in 16 critical infrastructures that include the healthcare sector.

4.2 CYBERSECURITY INITIATIVES IN DEVELOPED COUNTRIES

This segment gives a relative examination of how various countries promoted cybersecurity in the healthcare sector using models, strategies, or frameworks to safeguard EHRs. It furthermore analyses the cybersecurity originality of each of the countries in this area. The developed nations that were examined, and discussed here, are the United States (US), Australia, Canada, and Turkey.

The chosen countries are found to have either developed and maintained capability maturity models, strategies, and frameworks in compliance with the CIA (Confidentiality, Integrity, and Availability) triad and cybersecurity to protect healthcare information. The diversity of the countries as they have different economic, political, and healthcare-orientated backgrounds was considered to increase the richness of the discussion. These countries were selected amongst many based on the potential applicability or relevance of their models, strategies, or frameworks to the current study.

The US government, through the executive order (EO) 13636, requested the National Institute of Standards and Technology (NIST) to develop a healthcare framework. The “*framework for improving critical infrastructure cybersecurity*” in 2014 was developed and later updated in 2017 and 2018 respectively. Thus, through the Cybersecurity Enhancement Act of 2014 (CEA), the responsibility of NIST that includes the development of a cybersecurity risk framework was updated to better address the cybersecurity risk (Barrett, 2018a). However, the US doesn’t have a universal public healthcare programme, unlike other developed countries, and as a result, it relied on private programmes such as Medicare, Medicaid, the Children's Health Insurance Programme, and the Veterans Health Administration (Tikkanen & Abrams, 2020).

According to Burke, Oseni, Jolfaei, and Gondal (2019), Australia followed the United States’ example in 2016 and developed “*Australia’s landmark 2016 Cyber Security Strategy*” to protect, defend and investigate cybercrime including the dark web. The country went further to investigate the cybersecurity landscape using “*Cybersecurity Indexes for eHealth framework*” developed by the US NIST organisation to distinguish cybersecurity records that may be important to the healthcare sector. Sandison (2018) posits that Australia’s health system is strengthened by Medicare, a universal health insurance system similar to National Health Insurance NHI in South Africa. Australians conceded to public hospitals are ensured access to expense free treatment as public patients.



University of Fort Hare
Together in Excellence

Like in many other countries, the Canadian government in 2012 signed a Cyber Security Action Plan where amongst the objectives of the plan of action was the construction of a Canadian National Cyber Security Strategy. Taking a similar strategy to Australia, NIST (2017) published a National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework for Canada. The Canadian healthcare system is predominantly publicly financed through general tax revenues, with approximately 70% of health expenditures (Marchildon, Allin, & Merkur, 2020). The Canadian system is federated, with provinces and territories administered through a system known as Medicare and is legislated under the Canada Health Act.

The renewed interest in cybersecurity has found the Republic of Turkey’s Ministry of Transport, Maritime Affairs and Communications also following in similar footsteps and developing a 2016-2019 National Cyber Security Strategy to improve the cybersecurity ecosystem, strengthen the cyber defence and protect the critical infrastructure as the modern society depends on robust and resilient critical cybersecurity. The country of Turkey has

achieved remarkable improvements in terms of health status through health systems referred to as Social security schemes and Health Insurance schemes (Tatar et al., 2017). Both health systems are financed through employers and employees of the government and provide services to public and private sector facilities. The next sections discuss each of these countries' case studies in more detail.

4.3 UNITED STATES CYBERSECURITY FRAMEWORK (US CSF)

The United States Department of Health and Human Services reported more than one data break each day influencing in excess of 27 million patient records in 2016. By executive directive of the order (EO) 13636 issued by President Obama, the United States government authorised the National Institute of Standards and Technology (NIST) to construct a healthcare framework based on industry standards and best practices to assist businesses to mitigate cybersecurity risk (Barrett, 2018). In 2014 the “*Framework for improving critical infrastructure cybersecurity*” was developed, later updated in 2017 through 2018 (Barrett, 2018).

The US cybersecurity framework followed a standard framework design which consists of three elements: Framework core, the framework profile, and the framework implementation tiers (Akinsanya et al., 2020). These are discussed in detail in the following sections.

4.3.1 The framework core

The framework core, herein referred to as the “core”, is an industry standard, practices, and guidelines that serve the communication of cybersecurity-related activities between the organisation, executive level, and operational level (Swart, 2015). Francis (2016) refers to the core as the nucleus of the framework that acts at the organisation's strategic level. The core is not a checklist of action, according to Akinsanya, Papadaki, and Sun (2019), but a set of cybersecurity exercises or desired results that are normal across a certain critical infrastructure, which in this case is the healthcare sector.

According to Barrett and Matt (2018), the US Cybersecurity Framework (CSF) core component comprises of five simultaneous and consistent functions, i.e. Identify, Protect, Detect, Respond, Recover. The core uses categories, subcategories, and informative references to structure an identified function. Figure 13 below depicts the core components' subcategories and informative references.

Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Figure 13: Framework core structure

(NIST, 2014)

4.3.1.1 The five key elements of the core

Functions, according to Uppal (2020), represent key pillars of an end-to-end and successful cybersecurity program. As indicated above, they include Identify, Protect, Detect, Respond, Recover, and are there to support the organisation in articulating its cybersecurity risk management decision making (Akinsanya et al., 2020). Once all functions are combined, they form a strategic high-level view lifecycle of business management of cybersecurity risk (Uppal, 2020). The functions can also be aligned with existing policies and methodologies so as to ensure quick response to cybersecurity incidents. Other authors refer to these functions as key drivers that inform the management of an organisation about the risk appetite of cybersecurity (Rascado Sedes et al., 2020). The method in which all the functions are organised is essential to a well-operating security posture of an organisation and its successful management of cybersecurity (Uppal, 2020).

In classifying the key pillars of the core, La Fleur, Hoffman, Gibson, and Buchler, (2021) listed them as follows:

i) Step 1 – Identify

Cybersecurity in healthcare facilities is critical for patients’ medical information. The *identify* function is the step that kick-starts cybersecurity practices, recognises and helps the organisation with the process of managing cybersecurity risks and how systems apply, data, people, and capabilities (Uppal, 2020). Barrett and Matt (2018) agree with the previous author

saying the *identify* function improves the business capability and knowhow to manage cybersecurity risk to assets, data, systems, and capabilities. Both Barrett (2018) and Uppal (2020) mention that the *identify* function has foundational activities that are effective for the use of US CSF.

Understanding the context of the organisation enables the business to know how security affects and requires it to concentrate and prioritise its endeavours, consistency with risk management strategy and business objectives. Examples of outcomes facilitated with the *identify* function within an organisation are the following:

- Identifying asset management that includes software assets and physical assets;
- Identifying risk assessment that includes identifying weaknesses, dangers to both internal and outside organisation resources, and risk response activities as bases;
- Identifying risk management strategy to enable risk tolerance; and
- Identifying business environment that includes support in business rule in the supply chain and the business position within the critical infrastructure sector.

ii) Step 2 - Protect



The second function, *protect*, summarises the suitable safeguarding to guarantee the delivery of critical infrastructure services (Barrett, 2018). This function underpins the ability of the business to restrict or contain the effect of a potential cybersecurity assault. Examples of outcomes facilitated through the *protect* within an organisation function include the following:

- Implementing access control (AC);
- Instituting of data security protection regularly;
- Proactively managing information protection, processes, and procedures; and
- Implementing an information procedure.

iii) Step 3 – Detect

Uppal (2020) classifies the *detect* function as a step that defines exercises to distinguish the incidence of a cybersecurity event. At this step, continuous timely discovery of events is enabled. In the previous chapter, Coventry and Branley (2018) mentioned security infrastructure that can be used to protect medical devices, such as Intrusion Detection and Prevention System (IDPs). It is at this stage that such systems can be used to detect anomalies

and events within the business. Examples of outcomes categories established within the detect function in an organisation include the following:

- Ensuring anomalies and events that are detected and understood;
- Managing and maintaining security continuously, monitoring to track cybersecurity events; and
- Monitoring detection processes to provide alerts for potential threats.

iv) Step 4 – Respond

The *respond* function is designed to implement the appropriate activities that will take action regarding a detected cybersecurity threat event (La Fleur et al., 2021). This function will establish appropriate action in response to the adverse event and will support an organisation's ability to contain the impact of a potential threat (Mambo & Saeednia, 2003). Examples of outcomes categories established within the respond function are as follows:

- Response planning must be executed before and after the event;
- Communications are managed during and after the incident with all relevant stakeholders;
- Analysis to ensure the appropriate response to the event;
- A risk mitigation plan is developed in preparation for the unknown event; and
- The business must develop an improvements database using lessons learnt during the event.

v) Step 5 – Recover

Finally, the recovery step of the 5 key components of the US NITS framework assists to maintain plain though appropriate documented actions for security flexibility and re-establishing any capabilities or services that were hindered because of a cybersecurity threat (Barrett, 2018). Similar to the response function, this function upholds timely recuperation to typical tasks and makes sure there is a reduced effect from adverse cybersecurity threats. Examples of outcomes within the recovery function in an organisation include the following:

- Ensuring businesses implement recovery planning and procedure to restore current systems;

- Ensuring that improvements are based on current activities learned during adverse attacks; and
- Ensuring to keep the communications to both the organisation and the stakeholders about the recovery from a cybersecurity incident.

However, the five key components of the US CSF discussed above cannot be implemented without considering the implementation tiers discussed in the following section.

4.3.2 United States cybersecurity framework implementation tiers

The framework implementation tiers (Tiers) depict how much an organisation exhibits its risk management operations and provides mechanisms for businesses to understand and view the ways to manage cybersecurity risk (Uppal, 2020). According to Al-Matari, Helal, Mazen, and Elhennawy (2020), the tiers can support organisations to evaluate their performance of a particular core category using one of the four implementation “tiers” ranging from Partial (Tier 1) to Adaptive (Tier 4). Johnson (2020) posits that the tiers can build from each other and can be described as increasing the level of rigour and complexity in cybersecurity risk management operations.



The process of selecting a Tier is informed by an organisation’s present risk management operations, lawful and administrative requirements, organisational objectives, organisational constraints, and threats in the health sector (TechTarget, 2019). When an organisation is required to reduce cybersecurity risk to critical resources and assets to an acceptable degree, Francis (2016) posits that they should determine the desired Tier to ensure they meet the organisational goals. Information Sharing and Analysis Centres (ISACs) and maturity models are agencies from which organisations should leverage external guidance since they have capabilities to support organisations to determine the desired tier (Al-Matari et al., 2021).

Obar and Oeldorf-Hirsch (2020) posit that tiers do not signify or represent a maturity level; however, organisations are encouraged to consider moving to the next tier if they identify themselves in lower tiers. Furthermore, to reduce the risk of cybersecurity threats to patient records, healthcare sectors are encouraged to progress to higher tiers (Connelly, 2016). Successful implementation of the US CSF, according to Connelly (2016), depends on a comprehensive implementation of all the tiers, which are defined in the following paragraphs, and discussed in terms of risk management process, integrated risk management programme, and external participation.

Tier 1: Partial

Risk management process – there are risk-accepted standards that are popularly accepted in the industry such as ISO 31000. “*Risk management, principles and guidelines*” that provide guidelines for risk management in an organisation (Kure et al., 2018). The partial tier of the NIST framework recognises the risk management process as a method or technique. Connelly (2016) asserts that the high percentages in cybersecurity threats is as a result of organisation cybersecurity risk management practices not being formalised. These organisation risk objectives do not prioritise the cybersecurity activities and their risk is overseen in a specially appointed approach and at times in a receptive manner (Sutherland, 2017).

Integrated risk management program – is a combination of various components of a risk management approach that are independent and are necessary for successful risk management (Kure et al., 2018). Al-Matari et al. (2020) posit that organisations with integrated risk management programmes are found to have limited awareness of cybersecurity risk and there is no approach established to manage cybersecurity risk. At this level of the tier, an organisation executes cybersecurity risk dependent upon the situation due to a lack of skill and experience within the organisation.

External participation – at this level of the tier, most organisations are found not to have set up a processes in place to participate in a coordinated manner with other businesses (Kure et al., 2018).

Tier 2: Risk-informed

Risk management process – at this tier the risk management practices are authorised by management; however, they may not be established as organisational-wide risk practices or policies (Granja et al., 2018). Organisational risk objectives, threat environment, or business or mission requirements contain information about the prioritisation of cybersecurity activities.

Integrated risk management program – awareness campaigns have been conducted about cybersecurity risk at the organisational level but an organisation-wide approach to mitigate cybersecurity risk has not been established (Uppal, 2020). At this tier, the management has approved processes and procedures which are defined and implemented. It is assumed that staff have adequate resources to perform their duties related to cybersecurity.

External participation – the organisation is aware of its role in the larger cybersecurity environment; however, there are no formal documented capabilities to interact and share the information with external stakeholders (Le Bris & El Asri, 2021).

Tier 3: Repeatable

Risk management process – the organisation’s risk management at the repeatable tier is formally approved and expressed as practices or policies (Uppal, 2020). At this level, the business cybersecurity practices or policies are frequently kept up to date in line with the current application of risk management processes to changes in organisation requirements.

Integrated risk management program – at this stage, there is an existing programme to manage the cybersecurity risk. The previous level has informed the status of the repeatable tier with policies, processes, and procedures in place, implemented as intended, and reviewed (Uppal, 2020). Organisational employees retain credentials of knowledge and skills required in their position of employment to perform cybersecurity duties.

External participation – the business knows its stakeholders and partners and receives information from these stakeholders and partners that enables collaboration and risk-based management resolutions within the business in response to incidents (Uppal, 2020).

Tier 4: Adaptive



Risk management process – the organisation reviews its current cybersecurity practices and adjusts things based on the result presentation of both previous and current activities that include lessons learnt. In creating and maintaining a proactive standard, the business actively transforms to a changing technology landscape that can respond actively to sophisticated cybersecurity threats (Gourisetti et al., 2020a).

Integrated risk management program – the approach that is used is organisation-wide to manage cybersecurity risk making use of existing policies, processes, and procedures to respond to prospective events of cybersecurity (Al-Matari et al., 2021). The interrelation between the objectives of an organisation and cybersecurity risk is distinctly understood to make informed decisions. In Chapter 1 (Section 1.2), Van Niekerk (2017) presented ZAR 6.5 billion of direct cost in financial losses from cyberattacks that occurred in the healthcare sector. The huge financial losses from cyberattacks are a result of business senior management's shortfall in managing and monitoring cyberattacks. Organisational business units through existing governance that includes cybersecurity risk analyse system-level risk in the same

manner as the organisation risk tolerance (Uppal, 2020). Through an integrated risk management programme, according to Gourisetti, Mylrea, and Patangia (2020), organisations can efficiently take responsibility for changes to business objectives in the manner in which the risk is approached.

External participation – refers to the organisation understanding its part in the large ecosystem and how it will contribute to the healthcare sector's understanding of cybersecurity threats (Uppal, 2020). In this instance, the organisation uses technology tools like IDPS to understand real-time threats, and continuously acts on the cyber risk associated with the products it provides to its users. Constant, proactive communication is kept using formal or informal mechanisms to develop and maintain strong supply chain relationships.

The following section discusses the Australian perspective on safeguarding information in EHRs against cybersecurity threats.

4.4 THE AUSTRALIAN CYBERSECURITY PERSPECTIVE

Australians are also facing a range of cyber incidents that have affected the operations of health services. The Australian Strategic Policy Institute (ASPI) is an international cyber policy centre that endeavours to defend the Australian government on cybersecurity-related matters and is responsible for informing the public on a range of issues that include strategic issues (Feakin, Woodall, & Nevill, 2015). According to Australian legislation, all healthcare service providers are to ensure the protection of the security and privacy of patient health data (Australian Digital Health Agency, 2020).

Indeed, the commonwealth's Privacy Act of 1998 (Privacy Act) as applied to all government entities requires that all health service providers comply with reasonable steps to protect healthcare data from misuse, interference, and loss, including unauthorised access, tempering, or disclosure (Australian Digital Health Agency, 2020). However, Ponemon Institute (2018) Cost of a data breach survey reported 58% of healthcare victims due to system vulnerability. Due to the lack of framework in Australia, only about a third of healthcare institutions engaged in cybersecurity training and awareness in organisational policies and procedures (Alshaikh, 2020).

4.4.1 Australia's cybersecurity strategies

To grow the countries cybersecurity capabilities to be able to anticipate and respond to cyber vulnerabilities, the commonwealth of Australia developed and released 2009 Australia's

cybersecurity strategy (Commonwealth of Australia, 2016). However, despite the development of this document, the Australian government continued to be targeted by malicious threat actors (Australian Digital Health Agency, 2020). Research outcomes have demonstrated between the years 2009 and 2015, according to Onuiri, Idowu, and Komolafe (2015) issues of cybercrime especially in healthcare increased targeting of medical or health information that includes medical reports, patient discharge, drug information and were mostly compromised.

4.4.1.1 The 2016 cyber security strategy

Following these cyber incidences, the Australian government invested more than \$230 million for a period of four years to enhance Australia's cybersecurity capability and in 2016 developed a new strategy that is more focused on growth, innovation, strong cyber defences, and national cyber partnership (Gill & Chew, 2019). The intention that underpins the development of this strategy was drawn from a classified Cyber Security Review guided by the Department of the Prime Minister and Cabinet (Commonwealth of Australia, 2016).

However, according to Martin, Martin, Hankin, Darzi, and Kinross (2017), in the same year of the development and implementation of the strategy, 1.28 million records from the Australian Red Cross Blood Services that contained a massive amount of delicate information was posted on a public website to expose security flaws.

In this strategy, five themes of action were established, which according to the Commonwealth of Australia (2016) needed to assist the country to deal with cybersecurity challenges over the next four years to 2020:

- a) A national cyber partnership;
- b) Strong cyber defences;
- c) Global responsibility and influence;
- d) Growth and innovation; and
- e) A cyber smart nation.

i) A national cyber partnership

The strengthening resilience of cybercrime in Australia and other Asia-Pacific countries necessitated a good partnership amongst driving cybersecurity, setting the strategic agenda through annual cybersecurity meetings (Commonwealth of Australia, 2016). The Commonwealth of Australia (2016) posited that this structure would be composed of leaders

from business and the research community with key objectives to tackle emerging cybersecurity issues. Furthermore, this structure would streamline the cybersecurity governance for commonwealth government agencies and clearly identify responsibilities.

ii) Strong cyber defences

Due to the history of the vulnerability of healthcare to cyberattacks globally, the Australian government in its cybersecurity strategy promised to increase its network and systems resiliency to attack and make them hard to compromise. Mohammed and Bade (2019) posit that poor cybersecurity also has a major reputational risk for the healthcare sector. The Australian government made promises to expand the capacity of the national Computer Emergency Response Team (CERT) to work with other industries within the country particularly those providing critical services including the healthcare sector (Commonwealth of Australia, 2016).

In the process of increasing the bar on cybersecurity performance, the country further promised to tackle cybercrime by increasing the number of employees specialising in threat detection and awareness, technical analysis, and forensic fields (Commonwealth of Australia, 2016).

iii) Global responsibility and influence

The Australian cybersecurity strategy promised to partner with internationals to champion an open, free, and secure internet to improve the cyber proficiency of the country (Commonwealth of Australia, 2016). The cybersecurity strategy 2016 posited that this work would be enhanced through the appointment of a Cyber Ambassador, whose responsibility would be to identify opportunities for practical internal cooperation to guarantee the cooperation and influential voice of the country.

Indeed, according to Nakajima et al. (2017), Australia made good strides in implementing its cybersecurity strategy in 2016-17, in which amongst other things was the appointment of its Cyber Ambassador, Dr. Tobias Feakin. This appointment resulted in Australia's mandatory data breach notification law being passed and effected in the same year (Feakin et al., 2015).

iv) Growth and innovation

The internet has become a better tool for all Australian organisations, it presented enormous opportunities (Chang & Coppel, 2020). According to the Commonwealth of Australia (2016), the Asia-Pacific region can create up to US\$625 billion in economic activity per year by 2030 making use of disruptive business models and technologies including cloud computing, mobile Internet, Internet of Things, and big data analytics. The commitment of the Australian

government to cybersecurity will support developing businesses to diversify new markets, laying the foundation for a prosperous future (Chang & Coppel, 2020).

v) A cyber smart nation

Cybersmart is a national cybersecurity initiative dating back to Australia's Cyber Security Strategy 2009 (Ameen et al., 2020) and was developed to support the prerequisites of Australian culture by developing information, assets, and guidance to encourage secure online conduct. According to the Commonwealth of Australia (2016), Australia is suffering from a cybersecurity skills shortage. The Commonwealth of Australia (2016) further posits that Australian organisations are unaware of the risk they face in cyberspace. To address this predicament and raise national cybersecurity awareness, Australians have vowed to educate their citizens on the genuine effects of cyber risk and how cybersecurity affects the current and future prosperity of the country (Commonwealth of Australia, 2016).

4.4.1.2 The 2020 Cyber Security Strategy

The Australian government places much importance on cybersecurity, as the COVID-19 pandemic featured the developing nature of cyber threats, the commonwealth of the country developed a new Australian Cyber Security Strategy 2020 (Department of Home Affairs, 2020). The Australian Cyber Security Strategy 2020 builds on the 2016 Cyber Security strategy, which invested US\$230 million to protect and advance citizens of the country's interest online (Department of Home Affairs, 2020).

In this strategy, more emphasis was put on the Australian government to instruct and enable its citizens with the necessary awareness and knowledge about secure online activities (Ameen et al., 2020). The importance of secure online connectivity was Australia's response to the COVID-19 pandemic (Department of Home Affairs, 2020). However, according to Martin, Martin, Hankin, Darzi, and Kinross (2017), cybercriminals are exploiting the COVID-19 pandemic invading systems from anywhere in the world, stealing identities, money, personalities, and information from unsuspecting Australians including in health and medical research information.

The Coalition government in Australia invested \$1.67 billion over 10 years in cybersecurity in developing the 2020 strategy (Australian Digital Health Agency, 2020). This is considered the largest ever financial commitment to cybersecurity worldwide. The 2016 Cyber Security Strategy set out the Australian government's plans and has been a catalyst for change,

dispatching a progression of government and private sector cybersecurity activities and responses. The 2020 Cyber Security Strategy focused on the following activities:

i) The threat environment

The healthcare sector is accountable for collecting and keeping sensitive and confidential data whilst at the same time it is responsible to share such information with medical staff, patients, and other organisations (Offner, Sitnikova, Joiner, & MacIntyre, 2020). As a result, the rapid and national engagement in digital technology by businesses in Australia following the COVID-19 pandemic underscores the importance of digital technology (Dave, Boorman, & Walker, 2020).

Due to the COVID-19 pandemic, the threat environment widens as millions of Australians work from home and keep a connection to their organisational systems (Department of Home Affairs, 2020). A small scale of cyber events that threatens the integrity, availability, or confidentiality of digital information was recorded from June 2019 to July 2020. Figure 14 below illustrates cybersecurity incidents recorded during this period organised by the affected sector.

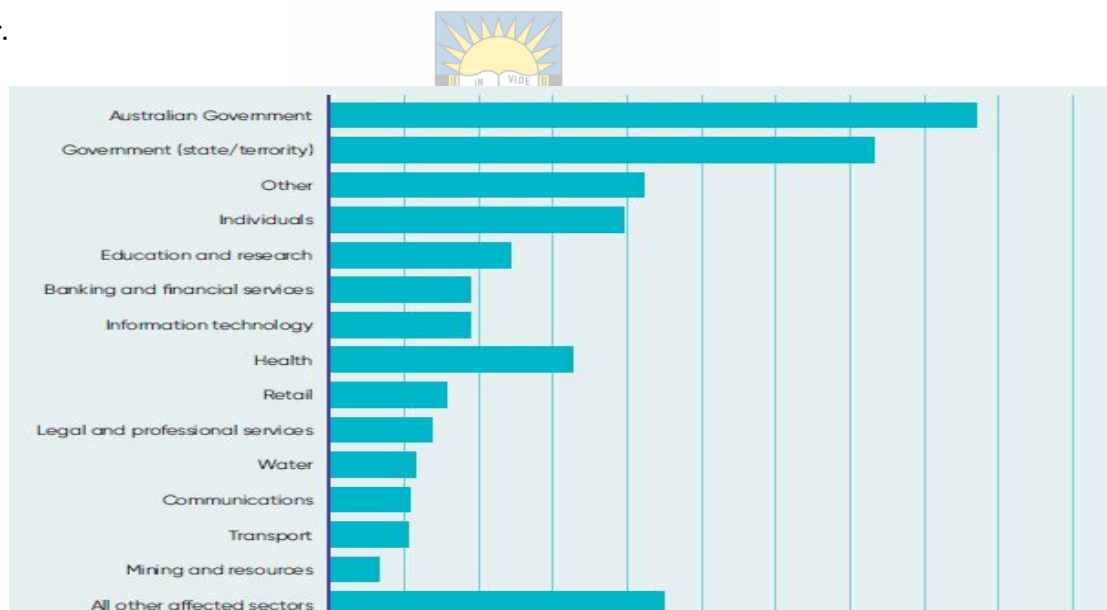


Figure 14: Cybersecurity incidents

(Australia Cyber Security Centre, 2020)

ii) Consultation

The transformation of healthcare from centred service design, specialist-focused approaches to distributed, patient-centred care has been a result of vast consultation through a government publication discussion paper “*A call for views*” that gave all Australians a platform to provide

their views. According to the Commonwealth of Australia (2020), the government of Australia received 215 submissions which resulted in identifying the following shortfall:

- a) The threat environment is worsening;
- b) Roles and responsibilities need clarification;
- c) Government and industry partnerships should be strengthened;
- d) Improved two-way information sharing is essential;
- e) Standards and regulations are necessary to get the basics right;
- f) The growth of cybercrime is outstripping our ability to respond;
- g) Many threats can be addressed at scale;
- h) Human behaviour is almost always part of the problem;
- i) Australia needs more trusted and skilled cybersecurity professionals;
- j) Small businesses are particularly vulnerable; and
- k) Australia needs to be better prepared, especially for a national-scale incident.

The shortfall from the Australians 2020 Cyber Security Strategy 2020, has propelled our discussion to look at the concerns that have affected the country of Canada.

4.5 CANADA'S CYBERSECURITY

According to Canada's National Cyber Security Strategies, digital technologies are now an integral part of Canadians' lives, with innovations emerging every day (Public Safety Canada, 2018). The new approach reflects the extent to which digital technologies are used and a record of more than 80% of organisations in Canada have accepted the chance to conduct business on the internet (Hegde, 2018). Moreover, the Canadians invested \$431 million over ten years focusing on three objectives including Security Government Systems, collaborating to get imperative cybers systems and assisting Canadians with being secure online.

However, criminals and other malicious cyber threats take advantage of the security gap. According to Zelmer (2018), the healthcare sector in Canada is not alone in experiencing cyberattacks. The rapid revolution of connected medical devices to the internet or other networks is growing exponentially with more people getting health devices in their homes, for

example blood pressure and sugar diabetes machines are a result of this dependence (Hegde, 2018).

With this in mind, the National Research Council of Canada's (NRC) Medical Devices Research Centre, in association with the Ministers of Defence, Innovation, Infrastructure, Public Services, and the Treasury Board, according to Public Safety Canada (2018), released a national effort to defend against these threats and developed Action Plan 2014-2017 for Canada's Cyber Security Strategy (the Action Plan) (Canada, 2013). In 2018, the renewal of existing Canada's Cyber Security Strategy 2010 was undertaken to:

- a) introduce the protection and safety of Canadians and critical infrastructure;
- b) promote and protect online freedom;
- c) encourage cybersecurity for business, economic growth, and prosperity; and
- d) proactively adapt to changes in the cybersecurity landscape.

4.5.1 Implementing the strategy



In the past few years, the healthcare sector has remained a subject of cybercriminals since medical identity fraud remains gainful and simple for hackers to take advantage of (Experian, 2017). Some cybersecurity groups predicted that as the attackers shift their focus, an increase in healthcare facilities breaches is the result of healthcare organisations that are not properly managed and this risk is said to increase (Zelmer, 2018).

In Canada, the number, significance, and intricacy of cyberattacks are expanding according to Experian's 2017 Fourth Annual Data Breach Industry Forecast report (Experian, 2017). Of the potential sources for a breach, EHRs are most likely to be a primary target for hackers. Experian (2017) further envisaged that of the many threats healthcare institutions face, ransomware would continue to be a top challenge in the year 2017. Moreover, it is recorded that disruption of healthcare system operations could be catastrophic.

As a result, the initiative to develop the strategy and the process followed in the development of the strategy was in consultation with Canadians and key stakeholders about how to best serve their security needs and mitigate the foreseen disruptions (Hegde, 2018). The implementation of the strategy, as indicated above, followed three Canadian objectives in an effort to safeguard cyberspace according to Public Safety Canada (2018) as follows:

i) Securing government systems

Like in many other countries, the government of Canada is entrusted with safeguarding electronic databases, providing services to the private sector through electronic systems. However, the increase in Canadians using online services has resulted in frequent cyberattacks in the health sector. It was recorded in May 2017 that over 86% of respondents to HealthCareCAN's 2016-2017 survey indicated that they either detected a breach or narrowly avoided cyber threat incidents (Coucke, 2020). More than eight in ten health leaders in Canada during May 2017 said the health sector is vulnerable to the WannaCry ransomware cyberattack. Moreover, the Canadian government has also received complaints from many organisations other than the health sector about detecting probes for vulnerabilities in their firewalls (Coucke, 2020). Most of these organisations complained about Canada's current Cyber Security Strategy lacking safeguarding processes. The recent high-profile ransomware attack that affected health sector organisations in the United Kingdom has proved that Canadian organisations are not alone in experiencing these cyberattacks (Strekalova, 2019).

As expressed, the Canadian Cyber Security Strategy is based on three pillars, among which is securing government systems. Concerning securing the government systems pillar, the ultimate goal is to transmit highly classified information while providing privacy and confidentiality to electronic processing systems (Kitts, 2017). Boucherville (2020) further posits that while the Canadian government is in the process of deploying cyber technology to advance the economy, it also reinforces its capacity to distinguish, discourage, and shield against cyber occurrences. The HealthCareCAN steering committee has played a big role in detecting, deterring, and defending critical infrastructure of the Canadian government which includes the health sector (Kitts, 2017).

ii) Partnering to secure vital cyber systems

According to Zelmer (2018), a strengthening of partnership amongst private and public sectors is necessary in order to produce a complete cybersecurity strategy for Canada and its citizens. Thus, the likelihood and impact of cyber incidents are shared amongst private and public sectors respectively.

In 2017, a HealthCareCAN steering committee was formed to support the creation and implementation of a Health Sector Critical Infrastructure Network as well as strengthening the cyber resilience of Canada's health sector (Zelmer, 2018). The committee engaged more than 25 national and international businesses about their programs and activities in cybersecurity.

This was because of the impact on the health sector that came in the different types of events. From the information obtained toward the end of 2017, from more than 25 national and international organisations pertaining to cybersecurity activities according to Boucherville (2020), the cooperation amongst the public, private, and citizens of Canada was achieved.

iii) Helping Canadians to be secure online

According to the government of Canada (2017), the ultimate goal of the last objective focused on giving Canadians data to secure themselves, and by doing that the capacity of law enforcement organizations to combat cybercrime would be strengthened. In the same year, the Canadian government cybercrime increased with breaches affecting more than 27 million patient records (Zelmer, 2018). Over 42% of the breaches were the result of actions by insiders, human errors, and those caused by wrongdoing.

These and many other attacks with similar events indicated that health organisations can be specifically targeted for a variety of reasons including personal information health organisations hold about patients, substantial financial resources, and large employers with significant payroll.



4.6 TURKEY'S CYBERSECURITY

Over the last years, the number of cybersecurity incidents in the health sector reported by ICT-CERT, Gartner Report, Ponemon Institute, World Economic Forum, and various other security companies revealed that Turkey is not immune to cybersecurity threats (Daskin, 2019). The Republic of Turkey has taken cognisance that cyberattacks have reached extraordinary levels (Gasiba, Lechner, & Pinto-Albuquerque, 2021). The Republic of Turkey (2019) went further to indicate that they believe the tireless and progressive cyberattacks focusing on information systems and data are being financed but it is difficult to detect their financiers. So instead, the Turkish government looks at keeping cybersecurity risk at manageable and acceptable levels.

In light of this situation, the Republic of Turkey Ministry of Transportation, Maritime Affairs, and Communications, following in similar footsteps to the likes of Canada and Australia, were tasked with adapting the policy, methodology, and activity plan for providing National Cyber Security Strategy (Cyber Security National Strategy, 2019). The objective is to improve the cybersecurity ecosystem, strengthen the cyber defence, and protect the critical infrastructure as a modern society depends on robust and resilient critical cybersecurity (Gasiba et al., 2021).

4.6.1 The engagement model

The Republic of Turkey National Cyber Security Strategy 2016-2019, comprehensively articulates two main objectives, namely:

- a) Acknowledge cybersecurity as an integral part of national security; and
- b) Acquire competency for administrative and technological precautions (Cyber Security National Strategy, 2019).

The main vision of the strategy according to the Republic of Turkey (2019, p. 11) is

“the formation of an eco-system that has international competitive power in the field of cybersecurity, in which all stakeholders related to cybersecurity manage risks at cyberspace in a competent manner in cooperation with each other in order to benefit from information and communication technologies in the most efficient way to contribute to wealth and security of society, as well as national economic growth and efficiency”.

The strategy also aims to determine and implement efficient and sustainable policies to guarantee national cybersecurity. On the other hand, the strategy is budgeted for an amount of about \$650 million to fuel the Republic of Turkey's cybersecurity initiatives (Cyber Security National Strategy, 2019).

However, according to Daskin (2019), despite so much investment into cybersecurity, it ought to be noticed that the Turkey National Cyber Security Strategy, legislation, and administration structures included are extremely new and not fully developed. The development of the strategy was supported by many including the Association for Information Security and the Union of Turkish Bar Associations (Daskin, 2019).

4.6.2 Cyber security strategies in Turkey

In the 21st century, cybercrime and ensuring the protection of cyberspace is evidently a top strategic priority (Şentürk, Çil, & Sağiroğlu, 2016). Although several methods exist to deal with cybersecurity threats, like maturity models, policies, and frameworks, the Republic of Turkey in June 2012 developed the first Cyber Security Strategy draft. Building from the draft strategy published in 2012, the Republic of Turkey introduced its first National Cyber Security Strategy and Action Plan 2013 -2015 by the Ministry of Transportation, Maritime, and Communications.

In this strategy, according to Karabacak, Yildirim, and Baykal, (2016), Turkey admitted that cyberattacks can never be completely eradicated or secured against and accordingly, the goal was to limit the number of cyberattacks and their effect on IT systems (Cyber Security National Strategy, 2019). Furthermore, several strategic actions were mandated in order to defeat deficiencies and carry out the national cybersecurity strategy with an initial deadline of 2014 (Daskin, 2019).

All nations, in particular third world countries are occupied with a series of exercises in order to ensure their security in cyberspace (Daskin, 2019). According to a survey conducted in 2016, it was found that there was an increase of 42% of households with internet access in Turkey (Karabacak et al., 2016). Following multiple meetings, workshops, seminars, and conferences, a process of developing a new National Cybersecurity Strategy 2016-2019 was required to contain the following objectives to respond to current challenges:

- a) Developing a national critical infrastructure inventory, that suggests security requirements of the health sector with supervision by a relevant regulatory board;
- b) Developing legislation that observes international standards which also contain cybersecurity auditing standards;
- c) Ordering to defend information systems of health sector organisations not only from attacks as well as from human mistakes;
- d) Developing training skills for personnel in cybersecurity and inspiring personnel to specialise in the cybersecurity field (Cyber Security National Strategy, 2019).

4.6.2.1 Cybersecurity challenges in Turkey

As was previously stated, the government of Turkey is not immune to cyber threats, it is during the 21st century when it witnessed multiple cyber occurrences and attacks on a phenomenal scale (Daskin, 2019). Amongst these multiple incidents are also incidents related to espionage to fraudulently impact the economy of the country. The hacking of HSBC Turkey resulted in credit card accounts' information of more than 2.7 million customers being stolen (Daskin, 2019).

The health sector is amongst the list of cyber incidents related to the political aspect, explicitly referred to as hacktivism, which has been a difficult issue for the Turkey government. According to Daskin (2019), these political groups are hacktivist groups who perform cyberattacks in accordance with their political conviction. Şentürk et al. (2016) posit that it

ought to be noted that the hacks of the Security Directorate were more serious than was disclosed according to some experts' claims.

Cyberattacks against the health sector have taken creative forms to access the infrastructure in Turkey. In 2019, management staff sent out an alert to the medical practitioners about online games that were used for cyberattacks (Bottomley, 2020). Many other institutions in government are also found to be regular targets of cyberattacks. As a result of the increased threats and actual attacks, the government of Turkey has taken multiple measures to safeguard its government departments and citizens respectively. Following are cyber defence mechanisms the country has followed to mitigate multiple incidents indicated above.

i) Safeguarding Turkey through cyber defence

To comprehend and act toward lowering the risk that may influence the state and public economy, health sector, and society is prepared in line with the ambit of this strategic action.

ii) Combating cyber crimes

To comprehend and act toward lowering the risk that may influence the health sector and patients causing the material loss is planned within the strategy.

iii) Improvement of awareness and human resources

The extent of the strategy incorporates bringing the cybersecurity culture to all portions of society from the management of the institutions to simple computer users and making them computer specialists.

iv) Developing a cybersecurity ecosystem

To comprehend and act to determine and implement prerequisites from legislations to technology innovations with the corresponded commitments of the general society, public sector, and other partners is also in the planning of the strategy.

v) Integration of cybersecurity to the national security

To comprehend and act toward lowering the misfortune caused by attacks performed by well-organised threat actors that might impact the state and public economy.

Thus, Turkey has progressed immensely in implementing its strategic objectives for cybersecurity and addressing critical security concerns in the country.

In all the cases presented above, it goes without saying that the government has committed to the safeguarding of its organisations and citizens from cybersecurity threats. Many initiatives

have been put in place to protect their environment and enormous amounts invested toward the protection and prevention of information. The following section provides a discussion on the comparative analysis making use of the IST organisational sequential management processes.

4.7 FINDINGS FROM COMPARATIVE ANALYSIS

It is clear that the United States, Australia, Canada, and Turkey have made unmistakable strides toward preventing information and information assets, preserving confidentiality, integrity, and availability of information. The previous sections presented each countries state of affairs pertaining to safeguarding cybersecurity and the initiatives taken to mitigate challenges that were found. Based on the analysis of these cases, this section provides a comparison and conclusion thereof. The format of the conversation will adjust to the structure of the IST organisational management processes as listed below:

- a) Security policy,
- b) Risk management,
- c) Internal control, and
- d) Information auditing.



However, in an organisational format, according to Anderson, Baskerville, and Kaul (2017), contingency management could begin at any of the organisational sequential management processes and form cycles.

4.7.1 Security policy

Having realised that the US was incapable to guarantee the secrecy, honesty, and security of medical information of its patients at their healthcare facilities, the Health Insurance Portability and Accountability Act of 1996 (HIPPA) brought forth various recommendations to the United States Department of Health and Human Services (HHS) to safeguard the protection and security of specific health information including patient information (Shah & Khan, 2020).

Among these recommendations was the development of a healthcare framework that must address issues of security policy. Furthermore, the US government developed a computer security guidance framework for how private medical services sector institutions can survey and improve on their capacity to prevent, detect and respond to cyberattacks (L. Johnson, 2020). The Australians, Canadians, and Turkish took on a different stance in curbing cybersecurity to that of the US framework and developed the National Cyber Security Strategy

and Action Plan (Commonwealth of Australia, 2016; Daskin, 2019; Public Safety Canada, 2018).

4.7.2 Risk management

Although the framework was developed and implemented to address risk-related issues, the Federal agencies in October 2020 raised alerts to the healthcare sector that is facing elevated and fast approaching cyberattacks and indicated that the cyber criminals have unleashed a wave of destruction to lock up health facilities' systems during COVID19 nationwide (The Guardian, 2020). The alert carried a warning about a group of cybercriminals targeting credible information from US hospitals and healthcare providers.

This malicious group was using ransomware which scrambles the patient information into gibberish that can only be decrypted using a specific type of software key provided once the targets pay up. In point of fact, in the US, the Department of Health and Human Services in 2016 reported more than one health information break each day influencing in excess of 27 million patient records (Zelmer, 2018). Zelmer (2018) further reports that two in five of the breaches (42%) were the results of actions by internal employees.

Similar to the US, even though the Australian government, Canadians, and Turkey did not use a framework to control the probability of cybersecurity threats, they used their strategies to single out the high-risk areas. According to Barrett (2018) when comparing the use of strategy versus implementing a framework, it is said that the strategy is a short-term document focused on certain process development while a framework provides a structure over a long period.

4.7.3 Internal control

According to de Kleijn and Van Leeuwen (2018), control and auditing theory recommends that businesses should institute data security control system, and subsequent to being implemented, examining processes ought to be controlled to find out the control performance. Amid the list of reported breaches in the US are those associated with human error and those caused by wrongdoing (The Guardian, 2020). The Guardian (2020) concludes its report by saying that the cyberattack from cybercriminals compromised all 250 US hospital chain Universal Health Service, necessitating healthcare practitioners to rely on the manual system (paper and pen) to record patient information.

Charlese Carmakal, the senior technical official of the cybersecurity organisation known as Mandiant spoke to the public and said, "*We are experiencing the most significant cybersecurity threat we've ever seen in the United States*" (Jalali & Kaiser, 2018 p. 12). The CEO of Hold

Security, Alex Holden supported the statement made by Carmakal saying he has been intently following the ransomware being referred to for over a year and that this attack has unfolded offensive unprecedented attacks in magnitude in the US (The Guardian, 2020).

Since in the US, Australia, Canada, and Turkey it is evident that there is a high lack of internal control, the Canadians proposed they would enrol computer training to their citizens to make them experts in cyberspace.

4.7.4 Information auditing

To sum up the state of cybersecurity in the United States healthcare sector, Herjavec Group (2020) predicted that the industry will spend more than \$65 billion incrementally over five years on cybersecurity products. Health Care Industry Cybersecurity Task Force, a group formed in line with the Cybersecurity Act of 2015, according to Zelmer (2018), released a report which identified several key challenges in the US which included the following:

- Shortage of security talent;
- Shortage of audit management skills;
- Premature/over-connectivity;
- Vulnerabilities impacting patient care; and
- A large number of known vulnerabilities.



University of North Hare
Together in Excellence

In contrast to Australia, Canada, and Turkey, the US has not distributed any activity plans in addition to their United States cybersecurity framework (US CSF). Having inspected some of the public cybersecurity issues in various countries using organisational sequential management processes, it can be concluded that there is a lack of contingency management for information security that is concerned with the prevention, detection, and reaction to the threats and vulnerabilities in an organisation. Zastepa, Sun, Clune, and Mathew (2020) suggest to practitioners that they should consider at least one information security management aspect to fulfill the needs of a dynamic environment. The following section concludes the discussion of the chapter.

4.8 CONCLUSION

In this chapter, the cybersecurity frameworks and strategies from four developed countries using IST were compared, evaluated and discusses. This refers to the United States

Cybersecurity Framework, the Australian Cyber Security Strategy, Canadian National Cyber Security, and the Turkey 2016-2019 National Cyber Security Strategy.

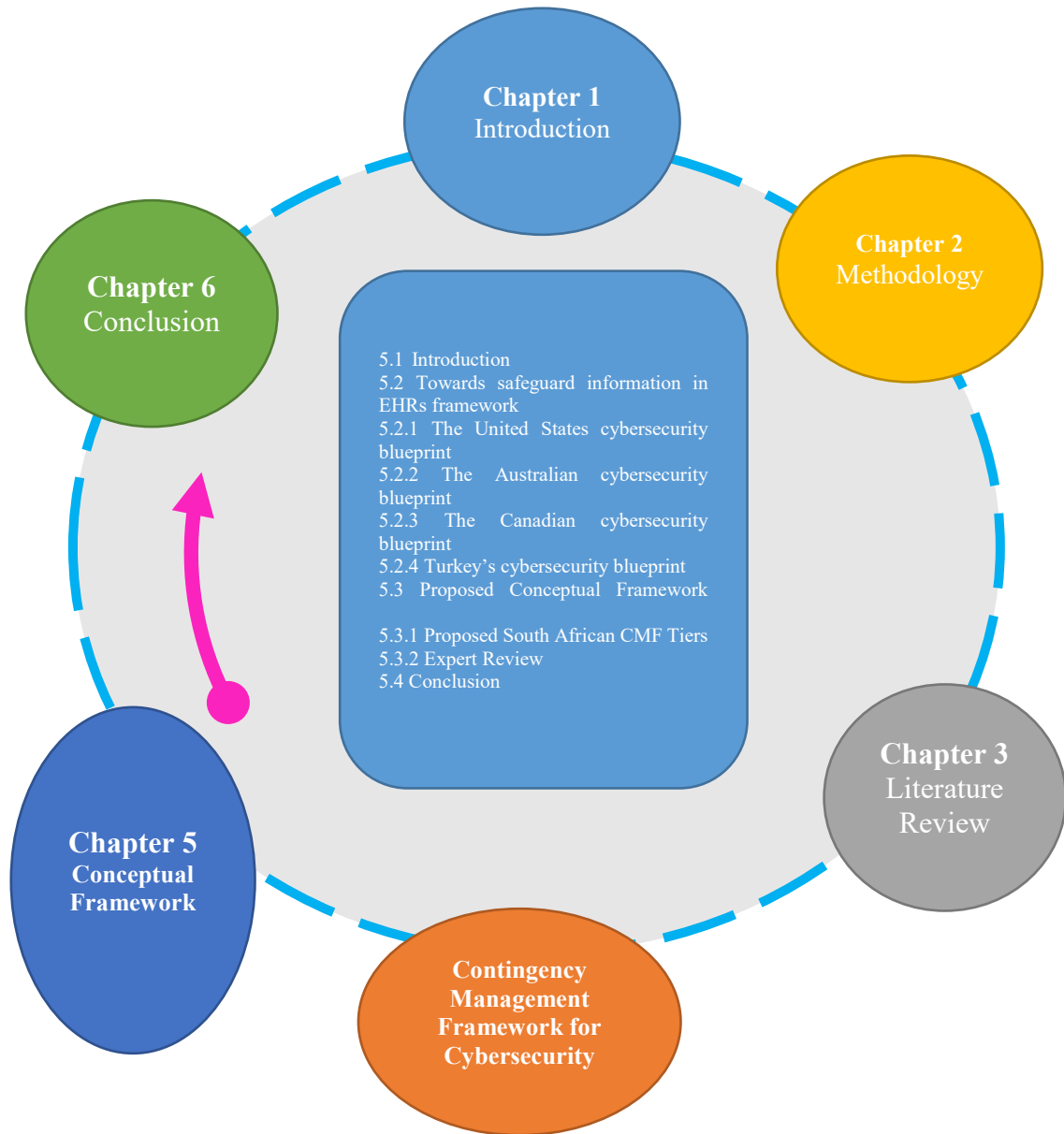
The US government developed a healthcare framework. The “framework for improving critical infrastructure cybersecurity” was later updated in 2017 and 2018 respectively. The framework is an industry standard, practices, and guidelines that serve the communication of cybersecurity-related activities between the organisation, executive level, and operational level. As explained, the framework has a core component consisting of five simultaneous and continuous functions i.e. Identify, Protect, Detect, Respond, Recover. The core uses categories, subcategories, and informative references to structure an identified function.

Following numerous cyber incidents, the Australian government invested more than \$230 million for a period of four years to upgrade Australia’s cybersecurity capacity and in 2016 developed a new strategy that is more focused on strong cyber defences, growth, and innovation, and a national cyber partnership was developed. The country went further to investigate the cybersecurity landscape using “Cybersecurity Indexes for eHealth framework” to identify cybersecurity indexes that may be relevant to the healthcare sector.

The Canadian government, on the other hand, invested \$431 million over ten years, focusing on the development of a Canadian National Cyber Security Strategy. Their approach reflects the extent to which digital technologies are used and it was recorded that more than 80% of organisations in Canada have accepted the chance to conduct business on the internet. The Canadian National Cyber Security Strategy contained three objectives including Security Government systems, partnering together to get crucial cyber systems, and assisting Canadians with being secure on the internet. Taking on similar steps of the Australians, NIST (2017) published a National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework for Canada.

The intense interest in cybersecurity has found the republic of Turkey Ministry of Transport Maritime Affairs and communications also following in similar footsteps and developing a 2016-2019 National Cyber Security Strategy to improve cybersecurity ecosystem, strengthen the cyber defence and protection of the critical infrastructure as the modern society depends on robust and resilient critical cybersecurity.

CHAPTER 5: CONCEPTUAL FRAMEWORK



5.1 INTRODUCTION

“South Africa has a huge responsibility to ensure all people living in it feel safe and have no fear of cyber-crime” (NDP, 2016, p. 320).

This chapter has the objective of providing a solution to this responsibility by developing a contingency management framework that will help the SA healthcare sector to secure EHRs against cybersecurity threats. Having studied developed countries like the US, Australia, Canada, and Turkey in the previous chapter, this chapter combines the strategies used and restructures components of existing cybersecurity policies, models, strategies, and frameworks from each of these countries. As was indicated in the previous chapter, these policies, models, strategies, and frameworks were chosen dependent on their potential applicability and significance to cybersecurity and healthcare orientation. The proposed contingency management framework of this study was developed according to the best information security architecture deemed most suitable for the healthcare sector in SA.

The repeated cyber intrusions into the healthcare sector environment demonstrated the need for improved cybersecurity in SA (Zelmer, 2018). According to Verizon (2019), about 67% of these intrusions have also influenced this study to research measures for safeguarding information in patient health records. In order to circumvent the increase in healthcare data breaches, the Health Insurance Portability and Accountability Act (HIPPA) of 1996 was introduced by the United States to implement physical and technical measures to safeguard sensitive information (Kruse, Frederick, Jacobson, and Monticone, 2017). However, according to Van Niekerk (2017), SA has not invested in implementing physical and technical measures to safeguard sensitive information.

The contingency management framework proposed in this chapter focuses on information security management implementation. It should also be noted that the framework was developed for this study based on the IST by focusing on key components discussed in Chapter 3 of this study.

Therefore, the aim of this chapter is to present a contingency management framework for the SA healthcare sector. This framework was constructed based on five different constructs that were used to develop the IST as was established in Chapter 3 of this study.

These constructs included:

- Security policy,

- Risk management,
- Control and audit,
- Contingency theory, and
- Management systems theory.

The following section presents the current approach of the US, Australia, Canada, and Turkey used to protect EHRs against cybersecurity threats. Thereafter, the proposed framework of this study is presented.

5.2 A RECAP OF CYBERSECURITY AND EHR INITIATIVES

A comparative analysis of how various countries promoted cybersecurity in the healthcare sector using policies, models, strategies, and frameworks to safeguard EHRs was presented in Chapter 4 (Section 4.2). As such, this section briefly summarises the cybersecurity initiatives of each of the countries and thereafter presents the proposed healthcare Contingency Management Framework in order to safeguard information in the EHRs in the South Africa healthcare sector.



5.2.1 The United States cybersecurity blueprint

The majority of developed countries, if not all studied, have an ultimate vision regarding promoting and protecting their cybersecurity environment. The healthcare sector environment is facing fast-changing demands. This vision is based on the respective perspective of the National Cyber Security framework, National Cyber Security policy, and/or the relevant document like action plan (Kure et al., 2018). In the case of the US, as mentioned in Section 4.2 of the previous chapter, President Obama, through the executive directive of the order (EO) 13636 mandated the National Institute of Standards and Technology (NIST) to develop a healthcare framework based on industry standards and best practices to assist businesses to mitigate cybersecurity risk (Barrett, 2018). Enhancing the cybersecurity of critical infrastructure was developed in 2014 and later updated in 2017 through 2018 (Barrett, 2018).

The framework design comprised of five concurrent and constant functions i.e. Identify, Protect, Detect, Respond, Recover. These functions were further defined to respond to categories, subcategories, and informative references to structure an identified function (Uppal, 2020). In this framework, as was further revealed in Chapter 4 (Section 4.3.2) by Al-Matari, Helal, Mazen, and Elhennawy (2020) that in order to fully support organisation and mitigate cybersecurity risk, one of four implementation tiers (Partial, Risk-Informed, Repeatable and

adaptive) can be used to evaluate its performance of a particular core category. Obar and Oeldorf-Hirsch (2020) encouraged organisations to consider moving to the next implementation tier if they were in the lower tier of the framework in order to reduce the risk of cybersecurity threats to patient records.

5.2.2 The Australian cybersecurity blueprint

Similar to many other countries, the Australian healthcare sector has also experienced a range of cyber cases that have affected the operations of health services (Zelmer, 2018). As indicated by Chapter 4 (section 4.4), Australia considers cybersecurity in their current legislation, where it is mandated that all healthcare service providers protect the privacy and security of patient health information (Australian Digital Health Agency, 2020). In the same section of Chapter 4, it was further revealed that the Commonwealth's Privacy Act of 1998 (Privacy Act) applied to all government entities and required all health service providers to maintain reasonable measures to protect healthcare information against abuse, obstruction, and loss, including unauthorized access, alteration, and disclosure (Australian Digital Health Agency, 2020).

Focusing on implementing strong cyber defences, growth, innovation, and national cyber partnership, according to Gill and Chew (2018), the Australian government committed more than \$230 million over four years to improve Australia's cyber security capacity and developed a new National Cyber Security Strategy 2016. In this strategy, five themes of action were established, to assist the country to deal with cybersecurity challenges until 2020 (Commonwealth of Australia, 2016):

Theme 1 - A national cyber partnership,

Theme 2 - Strong cyber defences,

Theme 3 - Global responsibility and influence,

Theme 4 - Growth and innovation, and

Theme 5 - A cyber smart nation.

As such, through a comprehensive strategic plan, the Australian government places much importance on cybersecurity as the COVID-19 pandemic report featured the developing nature of cyber threats (Department of Home Affairs, 2020). Despite the adjustment of the countries to adopt and use the established themes from the new National Cyber Security Strategy 2016, it was noted that Australian society suffered from cybersecurity skills and was supported

through the Cybersmart initiative (Ameen et al., 2020). The proposed CMF intends to address this shortfall from the Australian 2016 National Cyber Security Strategy. The following section briefly details the Canadian cybersecurity blueprint.

5.2.3 The Canadian cybersecurity blueprint

Similar to Australia, the Canadians invested \$431 million over ten years focusing on three objectives including security government systems, partnering to secure vital cyber systems, and helping Canadians to be secure online (Public Safety Canada, 2018). Amongst others, Canada regards securing government systems against cybersecurity threats as an integral part of its National Cyber Security Strategies (Public Safety Canada, 2018).

Cybersecurity threats to the healthcare sector are the focus of both a national strategic plan and a national action plan in Canada and Australia, respectively. Furthermore, both these countries carried similar initiatives that include the Australian Cyber smart initiative, and the Canadian HealthCareCAN initiative that is designed to protect and promote cybersecurity in those respective countries. However, it should be noted that Australia's National Strategic Plan 2020 focuses exclusively on educating and empowering its citizens to participate in secure online activities and acquire the relevant knowledge and skills, while the Canadian Cybersecurity Strategy is more about the protection and safety of Canadians and critical infrastructure.

Despite these initiatives, it was revealed in Chapter 4 of this study that criminals and other malicious cyber threats took advantage of the security gap in Canada. It was recorded in May 2017 that over 86% of respondents to HealthCareCAN's 2016-2017 survey indicated that they had either detected a breach or narrowly avoided cyber threat incidents (Coucke, 2020). More than eight in ten health leaders in Canada during May 2017 said the health sector is vulnerable to the WannaCry ransomware cyberattack. The support function that is proposed in the CMF will cater for the incident response and business continuity plan to mitigate these adverse events. The next section presents a brief cybersecurity blueprint implemented in Turkey.

5.2.4 Turkey's cybersecurity blueprint

According to Chapter 4 (Section 4.6), the National Cyber Security Strategy of Turkey, one of the country's primary objectives is to secure the healthcare sector through cybersecurity (Cyber Security National Strategy, 2019). As a result, Turkey has been busy with a series of activities in order to protect its security in cyberspace (Daskin, 2019). Some of these activities include the development of Turkey's National Cybersecurity Strategy and Action Plan over the years since 2012 (Cyber Security National Strategy, 2019). According to the Republic of Turkey

(2019), the Republic of Turkey Ministry of Transportation, Maritime Affairs, and communications followed in similar footsteps to the likes of Canada and Australia and developed its recent National Cybersecurity Strategy 2016-2019.

Turkey acknowledged in the strategy that cyberattacks can never be completely eradicated or avoided (Karabacak et al., 2016). As a result, the Republic distinctively articulated its objectives as follows:

- a) Acknowledge cybersecurity as an integral part of national security; and
- b) Acquire competency for administrative; and technological precautions (Cyber Security National Strategy, 2019).

Through these objectives, the government of Turkey reserved approximately a \$650 million budget to fuel the Republic of Turkey's cybersecurity initiatives (Cyber Security National Strategy, 2019). Karabacak, Yildirim, and Baykal (2016) posit that intention was to minimize the number and impact of cyberattacks on IT systems.

However, the Republic has taken cognisance of cyberattacks that have reached extraordinary levels and published them in the media (Gasiba et al., 2021). Through a thorough investigation, the country also discovered that persistent and advanced cyberattacks targeted at data and information systems were being financed; however, it is difficult to detect their financiers (Gasiba et al., 2021). It was revealed in Chapter 4 (Section 4.6.2.1) that the hacking of HSBC Turkey resulted in credit card accounts' information of more than 2.7 million customers being stolen which was one such financial event (Daskin, 2019). Bottomley (2020) further revealed that cyberattacks against the health sector have taken creative forms to access the infrastructure in Turkey.

As a result of the key issues raised in these approaches from various countries, the US framework seems to have merit compared to its international counterparts. Given its comprehensiveness and exclusivity in terms of approach to cybersecurity, it is argued that this framework could be adopted for the outline in the development of this study's conceptual framework – as opposed to the Australians that only relied on their National Cybersecurity Strategy of 2016 which provided five themes of action to assist the country to deal with cybersecurity challenges.

Likewise, Canada and Turkey also relied on their similar National Cybersecurity Strategy and Action Plan that are similar in structure to that of Australia. The US initiatives related to

strengthening cybersecurity in the healthcare sector further included a critical infrastructure cyber community voluntary programme also known as C Cubed, American Hospital Association's Cybersecurity, and the Postmarket Management of Cybersecurity in Medical Devices (Hegde, 2018). The following section discusses the proposed contingency management framework for the healthcare sector in SA.

5.3 PROPOSED CONCEPTUAL FRAMEWORK

A summary of healthcare cybersecurity initiatives and challenges was presented in the previous section using the US, Australia, Canada, and Turkey as examples. Following are the principles that guided the development of the framework for this study:

- The integrated system theory (IST) focusing on key components discussed in Chapter 2;
- The outline of the US framework for Improving Critical Infrastructure Cybersecurity; and
- The best information security architecture that is deemed most suitable for the healthcare sector in SA.



Moving ahead, in this section elements of the proposed Contingency Management Framework (CMF) for the healthcare sector in SA are discussed. However, as a prerequisite to discussing the proposed framework, it is necessary to first describe its type.

A theoretical framework and a conceptual framework are two types of frameworks found in research. According to Adom, Hussein, and Adu-Agyem (2018), a theoretical framework refers to a combination of multiple theories that are put together to provide an explanation, perspective, or basis for considering a phenomenon. Els and Cilliers (2017 p. 79) characterise a conceptual framework as “*a written or visual presentation that explains either graphically, or in narrative form, the main things to be studied, the key factors, concepts or variables and the presumed relationship among them*”.

Ameen et al. (2020) further clarifies the difference between a theoretical and a conceptual framework, by expressing that a conceptual framework as a structure that represents concepts borrowed from a particular phenomenon, while a theoretical framework describes and elaborates the concepts relating to the phenomenon. The proposed framework of this study is, therefore, a conceptual framework.

Tungpantong, Nilsook, and Wannapiroon (2021) posit that a conceptual framework is a creative process of assembling, developing concepts, constructs, and components built in a qualitative method. Consequently, a comparative analysis of concepts and elements was performed in the previous chapter to identify those to include in the proposed framework. As shown in the conceptual framework, the proposed framework is divided into four (4) implementation tiers, starting at the bottom tier, progressing to the fourth tier, which provides how an organisation views its cybersecurity risk as follows: -

- **Tier 1** – Support Function
- **Tier 2** - Process Management
- **Tier 3** - Governance Management
- **Tier 4** - Contingency management

The above-mentioned tiers respectively illustrate the four elements of IST. All these tiers could be applied in a healthcare environment such as community clinics, hospitals facilities, and health support centres. Furthermore, this conceptual framework was designed to work with both public and private healthcare in SA.



The diagram in Figure 15 below is a graphical representation of the proposed Healthcare Contingency Management Framework.

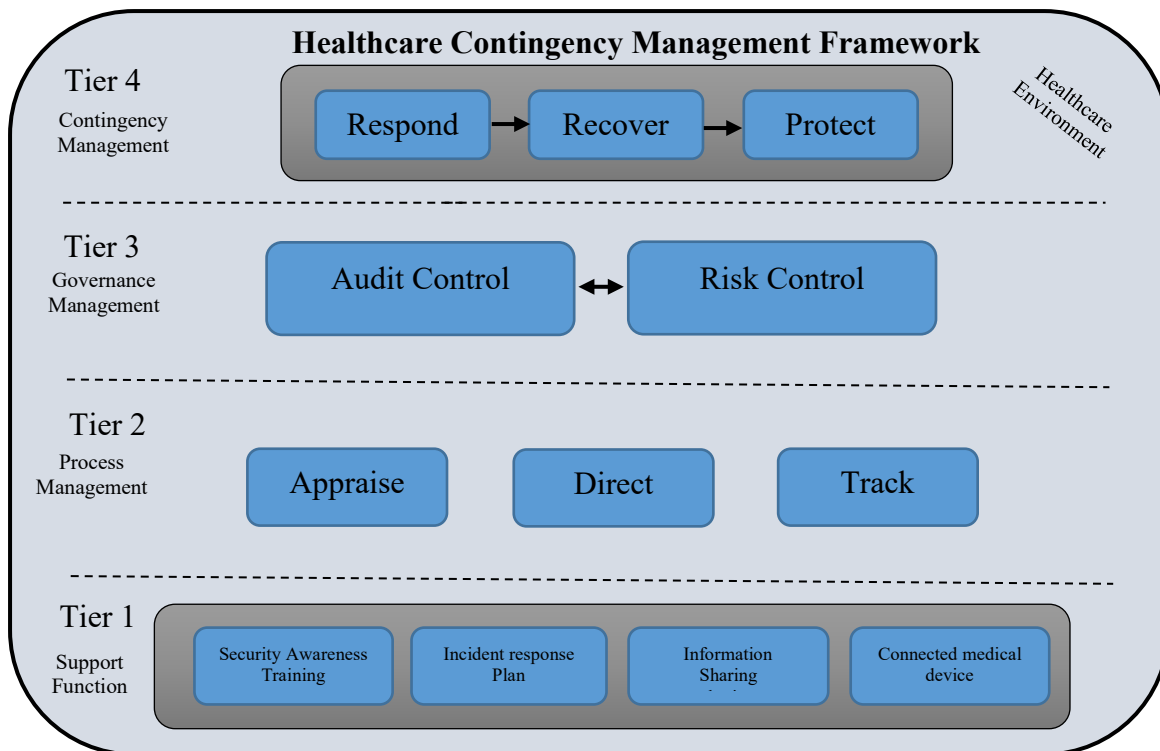


Figure 15: Proposed Healthcare Contingency Management Framework (HCMF)

5.3.1 Proposed South African HCMF Tiers

The organisation will engage in a selection process to consider its current risk management practices when using this proposed framework. The first tier of the proposed framework deals with the support functions of the organisation focusing on security awareness training, incident response planning management, information sharing management, and connected medical devices pillars. The second tier is a process management tier and is considered to be the three supporting processes of the HCMF and consists of Appraise, Direct, and Track pillars.

The third tier serves as the governance management tier of the HCMF, which deals with audit control and risk control of cybersecurity in the healthcare sector. The third tier of the healthcare contingency management framework provides governance management functional support to the organisation, ensuring the establishment of relevant structures like audit management committees and risk management committees. The fourth tier is referred to as a contingency management tier of the HCMF and the three pillars respond, recover and protect contingency management. The following section discusses each of the tiers of the HCMF sequentially starting from Tier 1 up to Tier 4 in further detail.

5.3.1.1 Tier 1 – Support function

Chapter 4 (Section 4.6.2) stated that when Turkey developed its new National Cybersecurity Strategy (2016-2019), one of its main objectives was to develop training skills for personnel in cybersecurity. In Chapter 4 (Section 4.5.1), Canada is also noted proposing to enrol computer training to its citizen making them experts in cyberspace. It is further noted in the Australian 2016 Cyber Security Strategy that the main challenges were those of cybersecurity awareness and training in organisational policies and procedures. Australia suffers huge losses from cybersecurity attacks due to a lack of framework (Alshaikh, 2020).

Given the various challenges and objectives of each country discussed, security awareness and training were noted as major challenges resulting from cybersecurity threats and is thus discussed first.

i) Security awareness training

Security awareness and training is an individual pillar within the Support Function of the HCMF. This pillar is not dependent on any other pillar in the HCMF. The main objective of this pillar is to provide healthcare institutions' employees with security-related training.

According to Chowdhury and Gkioulos (2021), humans are the weakest link in cybersecurity. Subsequently, healthcare facilities need to raise awareness among health providers (i.e. physicians, physician assistants, nurses, pharmacists, technicians, dietitians, physical therapists, etc.). Leppan (2017) posits that limited awareness of cybersecurity at a healthcare organisation has been a result of increased cybersecurity attacks.

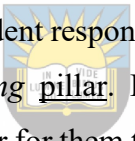
Even though raising awareness does not guarantee the security of medical information, it is nevertheless considered a critical step in a controlled environment. Chapter 2 (Section 2.1) presented the human element where people intentionally or unintentionally threaten the cybersecurity of the health facility. Many research studies have presented numerous efforts of mitigated risk, amongst which is security awareness training to healthcare providers. Security awareness training is a strong requirement to reduce cybersecurity attacks and increase the level of security in the SA healthcare sector (Alshaikh, 2020; Flahault et al., 2018).

According to Flahault et al. (2018), security risks in the patient record can be minimised if more health providers are knowledgeable about best practices and essential precautions within a healthcare facility. While beginner training is useful for entry-level workers like nurses, pharmacists, physician assistants, and administrators, more advanced, intermediate, and hybrid

training should also be provided to doctors, physical therapists, and a specialist from different health institutions is needed to help educate them about patient record cyber risks and threats. This will help to ensure that more health providers are knowledgeable of their respective work domains and the levels required to secure clinical data.

In this framework, healthcare institutions are required to frequently *Track* and *Appraise* gaps in knowledge to offer relevant and effective training (Flahault et al., 2018). Health providers should have a concrete understanding of the potential threats in their environment. For example, what is password sniffing, its effect, and what could happen if you release your information to strangers? The following section discusses how organisations should respond when detecting an incident in the healthcare system.

ii) Incident response planning

The incident response planning pillar can be regarded as an individual pillar to its function within the Support Function of the HCMF. However, the pillar can be dependent on others for the perfection of its function. The main objective of this pillar is to proactively prepare the institution for adverse events. The incident response planning pillar is directly connected to its counterpart *security awareness training* pillar. For a healthcare facility to have a strong information security posture, it is proper for them to prepare an incident response and business continuity plan (Latham, 2021).  University of Fort Hare
Together in Excellence

La Fleur, Hoffman, Gibson, and Buchler (2021) posit that this could be difficult to achieve in healthcare facilities because of a lack of skilled health providers, and challenges that are related to the budget. However, Flahault et al. (2018) posit that information security can never be achieved without a proper ICT management foundation. Malakoane, Heunis, Chikobvu, Kigozi, and Kruger (2020) define ICT management as a discipline in information communication and technology whereby all resources of an organisation are directed, governed, and monitored according to their needs and priorities.

Incident response and business continuity plans according to La Fleur et al. (2021) should involve an agreed-upon process with business top management. For a healthcare facility to properly manage its environment better, it is advisable to have agreements depicting incident management and escalation processes (Coucke, 2020). For example, in order for a healthcare facility to have a stable base of software applications, management of incidents through a service desk call logging system is required. An incident response plan should endorse system notification, post-incident steps, enforcing institution-wide password resets when attacks have

happened or been detected (Malakoane et al., 2020). Once an incident is detected either through server devices or through a software application, an organisation should immediately take drastic steps to limit such a breach (Dave et al., 2020). The following section discusses the information-sharing management of the proposed framework.

iii) Information sharing

The *information-sharing* pillar can be regarded to be similar to the *incident response planning pillar*, in that it is an individual pillar to its function within the Support Function of the HCMF. However, the pillar can be dependent on others for the perfection of its function. The main objective of this pillar is to allow the institution to securely share information amongst other healthcare institutions, doctors, nurses, patients through secure medical devices. The Cybersecurity Maturity Model (CMM) introduced in Chapter 3 (Section 3.5.3) is designed to protect sensitive customer and proprietary data, and comply with legislation to ensure the best services to customers (Le & Hoang, 2017). It was further indicated that the CMM makes use of metric levels to identify healthcare organisations' information security maturity. These metrics levels were presented as follows:

- *CMM Level 0 - Unprepared,*
- *CMM Level 1 - Reactive,*
- *CMM Level 2 - Proactive, and*
- *CMM Level 3 - Anticipatory.*



University of Fort Hare
Together in Excellence

The 2nd metric level of the model (*Level 1 - Reactive*) is specifically designed to promote existing legislation as far as the information-sharing mechanism is concerned within the healthcare sector to enable hospitals to share patient information (Feix & Procházka, 2017). Thus, the HCMF framework will promote the exchange and collaboration of healthcare patient information amongst health facilities throughout SA.

Most patients have their health information dispersed in various health facilities. However, the healthcare sector finds the exchange of information as an indicator of compromise and potential threat to patient information (Flahault et al., 2018). Information sharing facilitates situational awareness and a firm understanding of threat actors, their motivations, tactics, and techniques. Obar and Oeldorf-Hirsch (2020) posit that there are better ways to introduce information sharing in the healthcare sector, including collaboration, and sharing of information with considerable ease.

When the e-health introduced the EHRs initiative, it presented it as able to be shared amongst healthcare facilities. Information sharing approaches became the most important with the increase of EHRs in the healthcare sector, and the most vulnerable (Nalin et al., 2019). Some organisations are specifically designed to facilitate information sharing and collaboration between institutions including the National Health Information Sharing and Analysis Centre (NH-ISAC) in the United States (Ameen et al., 2020; Barrett, 2018). Such healthcare facilities that have adopted the National Health Information Sharing and Analysis Centre (NH-ISAC) policy support the interlinking of patient files and the collaboration thereof (Barrett, 2018). The following section discusses the interconnection of medical devices.

iv) Connected medical device

The *connected medical device* pillar can be regarded to be similar to its predecessor, the *information pillar*, in that it is an individual pillar to its function within the Support Function of the HCMF. However, the pillar can be regarded as dependent on others for the perfection of its function. The main objective of this pillar is to allow the institution (medical) to securely connect via an organisation network to provide service to patients. Research findings have revealed that the healthcare sector is fully dependent on information communication and technology (ICT) to transect its business (Mungadze, 2020). This is influenced by the increased variety in health devices that include equipment such as electronic beds, in-house treadmills, monitors, intravenous pumps, and insulin pumps (Flahault et al., 2018). Furthermore, wearable devices that monitor and record health and lifestyle data, for example, Fitbits, which can be available to clinicians have also contributed to the dependency of the healthcare sector on technology.

However, the diversification of these devices has brought along challenges in cybersecurity and requires a strict security policy. This is due to these devices being in direct contact with patient information and this has proved to be an increased risk to hospital operations and patient safety (Ursillo & Arnold, 2019). Advances in technology such as the Internet of Things have facilities to connect medical devices remotely. Both public and private sectors have a direct responsibility to protect patients' rights arising from cybersecurity threats (Alali, 2018).

5.3.1.2 Tier 2 – Process management

The goals and priorities of a healthcare organisation are to ensure consistent methods are in place to respond effectively and efficiently to cybersecurity threats (Anderson & Williams, 2018). Most organisations are overwhelmed with policies, standards, and frameworks that do

not address core challenges that affect the attainment of organisation objectives (Malakoane et al., 2020; Sutherland, 2017). The second tier of this proposed framework intends to ensure every activity that is performed in Tier 2:

- Appraised to determine elements of cybersecurity threats and ensure no anomalies or a breach in the information system.
- Direct information obtained from an organisation and ensure health providers follow relevant guidelines.
- Track the effectiveness and performance of cybersecurity to ensure a continuously improved safe environment.

i) Appraise

The *appraise pillar* is designed to detect the correctness of the Tier 1 functions to ensure how well the healthcare facility within an organisation operates. Cybersecurity threats are not only affecting patient files but also impede hospital operations (Flahault et al., 2018). The approach to managing cybersecurity is to analyse and identify activities that are performed in Tier 1 to ensure the internal and external environment is safe from cybersecurity threats. Additionally, organisations should evaluate their current policies regularly to ensure a cyber-resilient environment (Sobers, 2019).

The appraise pillar evaluates the availability of security awareness training in healthcare facilities and makes necessary recommendations such as the development of guidelines and policies that will aid the organisation to perform required pieces of training. Health facilities should frequently conduct awareness training for their computer users. The pillar moves to evaluate the implementation of incident response and business continuity plans. Each healthcare facility within the domain of the healthcare sector is required to prepare an incident response plan in line with the existing business continuity plan derived within the sector.

Roles and responsibilities should be made clear within the team responsible to respond to incidents. The appraise pillar further moves to evaluate the potential of cybersecurity threats during the exchange of data between the healthcare facilities. Recommendations of best practices, lessons learnt, mitigation strategies are then developed for the resilience of healthcare systems. Finally, the pillar looks into the connected medical devices to determine if they are included in strict security policies. The following section discusses the direct pillar of the proposed HCMF.

ii) Direct

The *direct pillar* of the proposed HCMF requires an organisation to develop policies, processes, and practices to address the everlasting challenges in health information systems. The literature identified that employees are regarded as the weakest link in the information security chain in many organisations but can also be a great asset in the effort to reduce risk related to information security (Anderson, Baskerville, & Kaul, 2017; Katurura & Cilliers, 2018). Since employees who comply with information security and regulation of the organisation are the key to strengthening information security, the pillar requires that developed policies, processes, and practices be workshopped with internal and external stakeholders.

To further ensure compliance, the healthcare sector is required to allocate responsibility, authority, and accountability of information systems to the management of the healthcare facility to ensure relevant guidelines for ethical and professional behaviour are enforced. The pillar further requires that in each healthcare facility, a security manager is appointed who will ensure information security policies are presented, be responsible for decision making, and managing the environment (Diesch et al., 2020).

In Chapter 3 (Section 3.4) it was indicated that the SA government is required to collaboratively establish policies and structures that direct the exchange of information between the public and private sector in response to global attacks. To prevent and mitigate abuse of information systems to encourage the use of e-government services, the SA government developed multiple policies (Ameen et al., 2020). The following pillar, which responds to tracking of activities within the framework, is discussed.

iii) Track

The continued cyberattacks in the healthcare sector are the result of a lack of consistent monitoring (Feix & Procházka, 2017). Almuhammadi and Alsaleh (2017) posit that to verify the existence of compliance and the efficiency of controls to mitigate risk, tracking of activities is essential. In Chapter 2 (Section 2.3), Till (2019) presented the Cybersecurity Maturity Model (CMM) with four maturity levels that were used as a measure to validate cybersecurity position in an organisation. The 3rd maturity level of the model specifically requires real-time monitoring of cybersecurity risk and cybersecurity threats, making use of risk assessment tools as the driver of security investment (Akinsanya et al., 2020). Flahault et al. (2018) posit that information security requires amongst others that change management, configuration management, and logging and monitoring mitigate risk.

Furthermore, Chapter 3 (Section 2.1.1) lists step 3 of the five key elements of the core of the US Framework with the outcome categories established within the detect function in an organisation as follows:

- Managing and maintaining security continuously;
- Monitoring to track cybersecurity events; and
- Monitoring detection processes to provide alerts for potential threats.

The *track pillar* of the proposed HCMF requires organisational business units through existing governance regulation that includes cybersecurity risk to assess the effectiveness and performance, analyse and track malicious activities of cybersecurity. For example, an organisation can implement a call logging and monitoring system that records all adverse events. Strict audit logs and monitoring of logging records, according to Flahault et al. (2018), are information and communication technology functions; however, they are also critical to recognise attacks sooner and devise solutions. It is further necessary to periodically assess and maintain oversight to ensure use of standards and guidelines by health providers.

5.3.1.3 Tier 3 – Governance management

The highest level of security measures is required to manage cybersecurity and a risk-based approach through enterprise risk management is necessary (Flahault et al., 2018). Masum (2018) posits that part of information security governance is the establishment and support of effective enterprise risk management. This is evident in Chapter 3 (Section 3.6.2.4) when SA adopted the EHRs, they wanted to understand what factors could affect patient files by performing an enterprise risk assessment of the healthcare sector. However, when they performed the assessment, they didn't consider the audit control aspect within the value chain. Thus, to date, SA is facing everlasting challenges towards achieving the health millennium development goals. This HCMF proposes the healthcare organisation perform risk control together with audit control. The following section explains the functionality and support of each pillar in the framework.

i) Audit control

Cybersecurity threat-related incidents span throughout government ministries, municipalities, and provincial government and require our government to develop a framework that embraces governance issues like auditing and risk management control (Sutherland, 2017). In the US

Strategy, amongst several key challenges that were mentioned was the shortage of audit management skills (Report & Ventures, 2020).

Chowdhury and Gkioulos (2021) refer to audit control as assessment, evaluation, and monitoring of the effectiveness of internal controls within the organisation. Similar to risk control, audit control involves three simple processes including a selection of control strategies, justification of strategies to upper management, and compliance within an organisation. According to Section 3.6.2.5 of Chapter 3, control and auditing theory recommends that businesses should institute information security control systems (De Kleijn & Van Leeuwen, 2018). Chapter 3, (Section 7.4) raised concerns about the shortage of audit management skills.

At this tier, organisations are encouraged to keep a comprehensive record of activities performed during this framework. For exceptional results, they are encouraged to perform audit control at least twice a year as a strategy to alert the organisation of any cybersecurity threats that may attack its EHRs.

ii) Risk control

Whitman and Mattord (2018) refer to risk control as when the management of an organisation empowered ICT and information security to control identified risk. Organisations can mitigate risk to their assets through countering the threats they face by performing a risk assessment to their environment (Gkioulos & Chowdhury, 2021). Another defence mechanism according to Sutherland (2017) is to implement security controls and safeguards that prevent the system from attacks and therefore minimising the probability that attacks can occur. Whitman and Mattord (2018) suggest an organisation perform a mitigation risk control strategy, which attempts to reduce the impact of an attack.

When an organisation gets to this tier, they will be required to identify their current cybersecurity and risk management state. Once they understand their state, they will be required to perform a risk assessment. The process of risk assessment will assist the organisation to develop its state profile based on control maturity. The following section discusses the fourth and final implementation tier of the proposed framework.

5.3.1.4 Tier 4 - Contingency management

In the healthcare sector, there is lacking reasonable dynamic processes when it comes to purchasing information security systems (Lamminen et al., 2016). To meet the ever-changing environment, the management of an organisation is required to provide strategic decision

support (Whitman, 2016). The contingency theory recommends the best way of leading an organisation is contingent upon the internal and external challenges (Alqurshi, 2020). The following section will discuss the contingency management of EHRs.

i) Respond pillar

According to Burton, Obel, and Håkonsson (2020) contingency plans exist to respond to adverse events, including incident response plans, business continuity plans, and disaster recovery plans. Using the contingency approach, plans are prepared by the organisation to form a single integrated plan that can be used to anticipate, react to, and recover from adverse events (Whitman, 2016). A contingency planning management team is assembled to respond to the internal and external factors.

The *respond pillar* supports the ability to contain the bearing of a likelihood of cybersecurity event to occur making use of functional pillars from Tier 1 like incident planning and business continuity plan. Healthcare facilities are required to develop and implement appropriate activities in order to take action from the detected cybersecurity events. Tier 2 of the HCMF framework also plays a vital role in support of the contingency management pillar “*Respond*” by evaluating, directing, and appraising. The following section discusses the recovery pillar of the contingency management tier.



ii) Recover pillar

The *recovery pillar* of the HCMF provides context on how a healthcare organisation will recover from an adverse event. In the context of this study, EHRs are referred to as internal factors and cybersecurity threats are considered external factors. An adverse event can originate from either the internal or external environment. The contingency approach examines the organisation’s internal and external factors for the effectiveness of decision making (Lamminen et al., 2016). Based on a theoretical understanding of the contingency approach, the key role of all managers from ICT and information security is contingency planning to sustain effective and efficient decision making during the recovery process.

Developing and implementation of appropriate activities are required to maintain plans for resilience and to restore any capabilities or services that were impaired due to cybersecurity adverse events. The recovery pillar supports timely recovery to normal operations to reduce the impact of a cybersecurity adverse event.

iii) Protect pillar

Developing a cyber-resilience environment has been found to be a shared responsibility in the field of the health sector. Chapter 3 (Section 3.5.2) referred to EHRs as technology means to patients' safety. Chapter 1 (Section 1.3) defined cybersecurity as the “*practice of making the networks that constitute cyberspace secure against intrusions, maintaining confidentiality, availability, and integrity of information, detecting intrusions and incidents that do occur, and responding to and recovering from them*”. However, according to Chapter 1 (Section 1.5.2.2), cybersecurity threats are related to adverse events such as ransomware attacks, denial of service (DoS) attacks, phishing and spear-phishing attacks, password, and many other attacks resulting in dysfunctional EHRs.

Developing and implementing appropriate safeguards to ensure the delivery of critical information between facilities is vital. According to Chapter 4 (Section 4.2), in 2016 Australia followed the United States' example according to Burke, Oseni, Jolfaei, and Gondal (2019), and developed “*Australia's landmark 2016 Cyber Security Strategy*” to protect, defend and investigate cybercrime including the dark web. Section 3.3 of Chapter 3 indicated that Coventry and Branley (2018) mentioned security infrastructure that can be used to protect medical devices, such as Intrusion Detection and Prevention systems (IDPs). The protect pillar of the CMF supports the ability to limit or contain the impact of a potential cybersecurity event making use of the available infrastructure. These include maintenance and protect medical devices, access control, awareness and training, data security, and information protection. The following section discusses the evaluation of the HCMF through the expert review process.

5.3.2 Expert review

Taking the research paradigm of this study, “*interpretivism*” review is deemed as a very important part of the research process. Furthermore, as was mentioned in the methodology chapter that this research study made use of a literature review as means of a collecting secondary data in order to develop the conceptual framework, while for primary data collection, experts from the field of information systems, who had conducted and published EHR implementation in SA, worked in the public sector in South Africa as CISO and experts in security were identified in order to evaluate this HCMF. Liebowitz (2019) defines an expert as an individual with comprehensive knowledge or experience in a particular area. Table 5 provides a summary of expert reviewers who participated in the evaluation of the proposed conceptual framework.

Table 5: Summary of expert reviewers

No.	Subject Matter Expert	Field Experience	Description	Participated in the review
Expert Nr. 1	Expert in EHR	<i>Master's Degree in the field of EHRs</i>	<i>conducted and published EHR implementation in SA</i>	<i>YES</i>
Expert Nr. 2	Expert in EHR	<i>Master's Degree in the field of EHRs</i>	<i>conducted and published EHR implementation in SA</i>	<i>NO</i>
Expert Nr. 3	Expert in EHR	<i>Master's Degree in the field of EHRs</i>	<i>conducted and published EHR implementation in SA</i>	<i>YES</i>
Expert Nr. 4	Expert in Security	<i>Master's Degree in the field of EHRs, vast experience in Security management in the public sector</i>	<i>worked in the public or private sector in SA as CISO</i>	<i>YES</i>
Expert Nr. 5	Expert in Cybersecurity	<i>Master's Degree in the field of Information Systems, vast experience in Cybersecurity in the public sector.</i>	<i>worked in the public or private sector in SA as CIO or CISO</i>	<i>YES</i>
Expert Nr. 6	Expert in Cybersecurity	<i>Master's Degree in the field of Information Systems, vast experience in Cybersecurity in the private sector.</i>	<i>worked in the public or private sector in SA as CIO or CISO</i>	<i>No</i>



In this research study, as presented in the table above, six experts were initially approached to participate in the study to evaluate the HCMF, following two main themes as was indicated in the methodology in Chapter 2. However, only four experts were still willing to participate when approached to complete the review of the framework. Thus, four experts participated in the final study to assist by evaluating the constructs of the four tiers in the framework and how the proposed architecture will assist in governing cybersecurity in EHRs in the public sector. Liebowitz (2019) contends that the definition of the term “expert” should be defined based on the opinions of the relevant respondents.

Based on the experts' experience and knowledge in the fields of electronic health records (EHRs) and cybersecurity, this study selected experts based on their specialties, roles, and knowledge in these fields. Amongst the six experts that were selected to validate the framework, only four expert reviewers were available to participate. The following section presents an account of the four expert reviews.

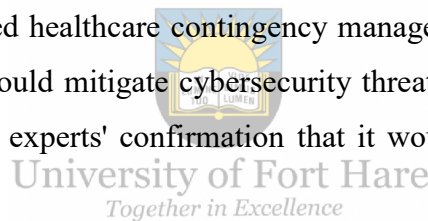
5.3.2.1 The framework validation

Expert reviewers were employed in the study to describe the nature of reality concerning the proposed conceptual framework. A week before conducting the expert interviews, an expert

brief review was sent to the reviewers by email. This was a seven page document including an introduction to the project, an explanation of the framework, and the questionnaires. The objective of this exercise was to elicit the reviewers' in-depth understanding of their area of expertise in order to validate the proposed conceptual framework. The brief can be seen in Appendix D.

Before interviewing the experts, the proposed Healthcare Contingency Management Framework was presented using the *Expert Reviewer Brief* document. The purpose of this presentation was to provide an overview of the research behind the proposed conceptual framework. Moreover, the details of each tier and pillar of the proposed framework were provided so the expert reviewers would have a full understanding of the context. Subsequently, the expert review interview, used the attachment enclosed as part of the "Expert Reviewer Brief". The questions that the experts were asked were fairly reasonable and as a result, the researcher had the opportunity to probe information provided by the experts.

The questions asked were intended to verify all four tiers, each of the pillars, and the applicability of the proposed healthcare contingency management framework. To make sure the proposed framework would mitigate cybersecurity threats to electronic health records, it was essential to obtain the experts' confirmation that it would contribute to the security of public health records.



The interviews were conducted using Microsoft Teams video conferencing, meeting and calling tools. Experts evaluated the framework and provided both positive and negative comments that were used to refine the framework. Overall the experts were very positive that the framework can address the research question and provide a contribution to the field of electronic health records. The comments from the reviewers are unpacked below. Concerning the four implementation tiers of the framework, all four expert reviewers approved these tiers, and one of the expert reviewers expanded by saying:

“If each step in the tier process is linked to indicate the sequence of events and chain of the processes, users of the framework would understand what is the next step”.

The HCMF framework was reviewed with this opinion with arrows interlinking each tier from Tier 1 to Tier 4.

A summary of other remarks made by the expert reviewers is provided in table 6 below, along with how the researcher responded. Appendix D provides further details on the feedback provided by the experts.

Table 6: Concerns and responses

Questions put to reviewers	Responses from reviewers	Impact on Framework
<p>Does the proposed HCMF address the cybersecurity concerns of South African patients that use EHRs and make a meaningful contribution to the field of information security?</p>	<p><i>Most of the experts were in agreement that the advancement of technology has exposed the security of patients' healthcare data.</i></p> <p><i>One of the experts states, "People will always try and exploit any system, central to them will always be hackers and phishing. The newer the system, the higher the chances of it being targeted".</i></p> <p><i>The other expert responded to this issue and said: "Within the era of moving to cloud technology, the introduction of POPIA, Security Risk has increased significantly".</i></p> <p><i>Another expert from the public sector closed this issue and said: "As soon as a medical record is online in any form it is subject to potential loss (system failure, ransomware) or unauthorised access (poor user control or hacking) whereas an offline paper record only exists in one form".</i></p> <p><i>The last expert elaborated on the question as follows: "This is a comprehensive framework that appears to address all cybersecurity concerns of South African Patients. The only area that may be worth adding is the impact of key legislation: New CyberSecurity Act, POPIA PAIA It may also be worth emphasising under "Recover" that there is also a patient reputational recovery required."</i></p>	<p><i>Tier 1 – connected medical device pillar allows the medical institution to securely connect via an organisation network to provide service to patients.</i></p> <p><i>Tier 1 – Awareness and technology pillar has a strong capability to reduce cybersecurity attacks and increase the level of security within a facility.</i></p> <p><i>Tier 1 – Information sharing allows the institution to securely share information amongst other healthcare institutions. This pillar is governed by numerous cybersecurity legislation including NCPF, POPIA, and ECTA.</i></p> <p><i>The foundation of the HCMF is built on the key components of the National Cybersecurity Policy Framework and considers several cybersecurity laws of SA including POPIA, ECTA, and NCPF, and as such, no amendments were made.</i></p> <p><i>Tier 3 – Governance management pillar focused on the audit and risk management processes. Additional pillar cybersecurity legislation that addresses issues of cyber governance is considered. This new cybersecurity pillar will be built with a foundation of National Cybersecurity Policy Framework, POPIA act, and ECTA.</i></p>
<p>Do the proposed HCMF implementation tiers follow a sequential</p>	<p><i>This concern was discussed extensively with all the experts who participated. The first expert responded with "Yes" and elaborated as follow "There is a sequential</i></p>	<p><i>Organisations will engage in a selection process to consider their current risk management practices when using this proposed framework.</i></p>

<p>process to address the cybersecurity concerns of South African patients that use EHRs?</p>	<p><i>process, and the only query is whether or not the individual Tiers have an importance rating of what needs to be addressed first within each Tier and does it then get escalated to the next Tier”. The remaining reviewers responded with “Yes” and did not elaborate.</i></p>	<p><i>Tiers of the HCMF are designed in such a way that they accommodate the escalation process.</i></p>
<p>In the “Support Tier” of the framework, the following question was asked. In your opinion, does Tier 1 of the HCMF include all the necessary constructs for the “Support Function”?</p>	<p><i>Most of the experts were in agreement with what is entailed in the support layer and responded with “Yes”. However, one of the experts from the public sector responded as follows: “The implementation of the Contingency Tier 4 of the framework will region a strong focus on change matrix, that could potentially be an outer layer of the fourth tier of the framework”</i></p>	<p><i>Tier 4 responds to contingency management of EHRs. This tier works in conjunction with support of Tier 1 of the HCMF. The foundation of this pillar is built to ensure a cyber-resilience environment to respond, recover and reduce the impact of a cybersecurity adverse event</i></p>
<p>In your opinion, does Tier 2 of the HCMF include all the necessary constructs for the “Process Management”?</p>	<p><i>The first opinion from the expert was as follow: “Yes, it contains the understanding of process management, with the integration of Tier 1 define, gather, process, analysis, distribution, and feedback.”</i></p> <p><i>The second response was from the public sector security specialist as was as follow: “The process to actively detect and prevent cyberattacks through physical/logical and other key controls and the process to rapidly respond to detected attacks and mitigate and minimise losses are not included.”</i></p> <p><i>The third opinion was as follows: “I would also consider adding step1 as identify, then track, direct and appraise.</i></p> <p><i>The last opinion was solicited from the expert in the Electronic Health Record was positive “Yes” and did not contain any elaboration.</i></p>	<p><i>The first comments provided for Tier 2 of the HCMF framework had no impact on the framework. As a result, no additional information was included.</i></p> <p><i>The second response provided for Tier 2 of the HCMF framework was rather an expected output of the pillars combined as was acknowledged.</i></p> <p><i>The third opinion was considered a contribution to the second tier of the HCMF framework and was added respectively to also address the issue of the sequential process of the HCMF framework</i></p>
<p>In your opinion, how can the proposed HCMF be made more understandable and easy to read?</p>	<p><i>The first opinion from the expert was as follows: “Create a ranking system within the Tiers, maybe, depending on the desired outcome.”</i></p> <p><i>The second opinion from the expert was as follow: “Within each tier, it can assist if each step in the tier process is linked to indicate the sequence of events and the flow of the process”</i></p>	<p><i>The first opinion was considered a valuable contribution to the HCMF; however, this concept was deemed not necessary to be presented as it will confuse the implementers of the framework.</i></p> <p><i>The second opinion was considered a valuable contribution to the HCMF and was implemented. Each tier of the framework was linked to show the coordination of tiers of the HCMF framework.</i></p>

The third opinion from the expert was as follow: “Perhaps a supporting diagram that explains each of the terms - or a key/glossary that explains all the terms to a layman it can have an increased focus legislature compliance and processes to actively detect respond to and mitigate/minimise attacks”

This opinion was also considered and debated extensively. The framework will be issued to the healthcare facility as part of the study and all its elements are explained in the research study.

In addition to the above-mentioned concerns, the expert reviewers were positive about the contribution to the proposed contingency management framework developed to mitigate cybersecurity threats to electronic health records in the public health sector in South Africa.

5.3.2.2 Final HCMF framework

Besides the above concerns expressed by experts, the structure of the HCMF was realigned to better fit the healthcare sector in SA, as well as better describe the impact of cybersecurity in the healthcare environment.

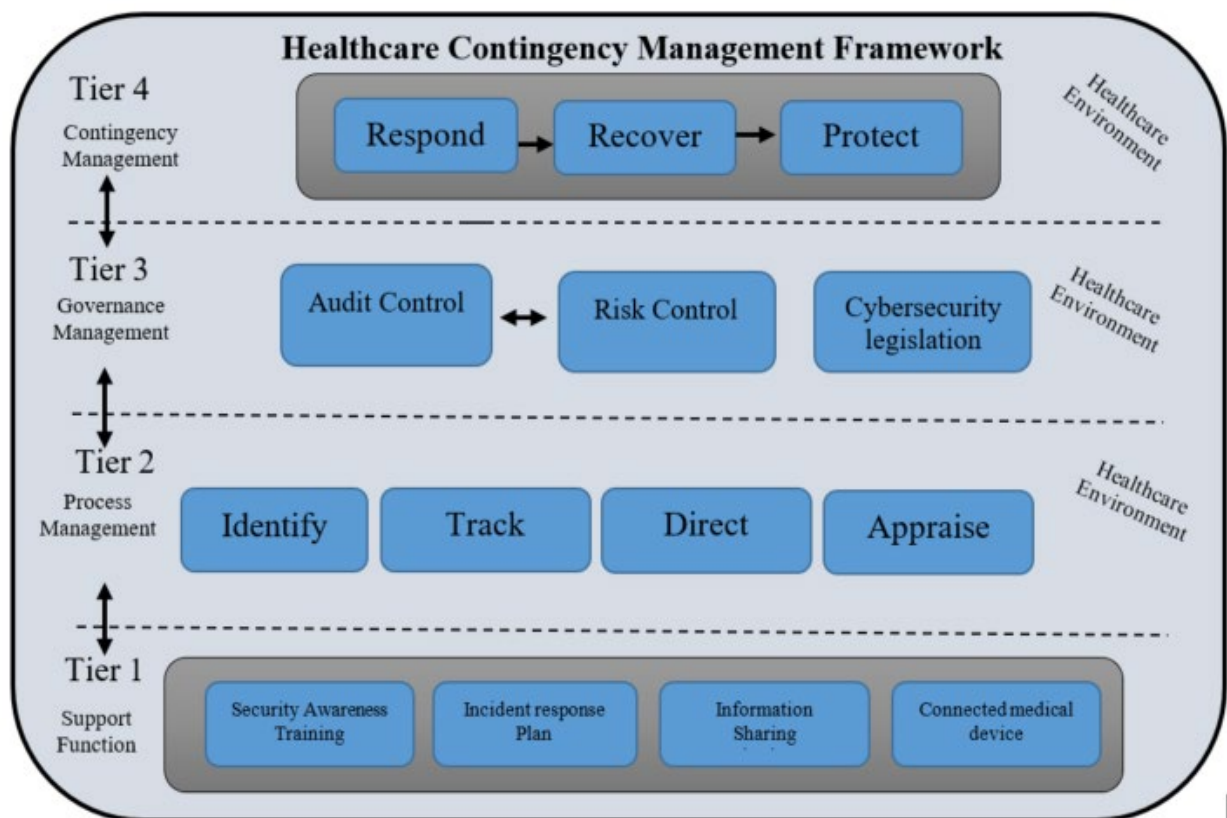


Figure 16: Final Healthcare Contingency Management Framework (HCMF)

Figure 16 above presents the finalised Health Contingency Management Framework which incorporates all the recently discussed opinions from the experts for each tier. The following reiterates the contribution made to each of the tiers of the framework by expert reviews:

- **The HCMF review** – Expert reviewers from the public sector made a considerable contribution. The expert reviewers proposed each tier of the HCMF be linked to indicate the sequence of events and the flow of the process. New arrows were added to the framework interlinking each tier to the next to clearly indicate the sequence of events and flow of the process.

Furthermore, they recommended that the label *healthcare environment* appearing only on the top right of the HCMF be duplicated in each of the tiers to show that each of the tiers is implemented in the healthcare environment. This contribution was considered and implemented respectively.

The HCMF Tier 2 review – Expert reviewers felt the Tier 2 pillars were not complete and required an additional pillar that first identifies the cybersecurity threat in an environment. This opinion was considered as a contribution to the HCFM framework and was added as *identify*, the first pillar of the second tier. The *identify* pillar is defined as the process to actively detect and prevent cyberattacks through physical/logical and other key controls requires first identifying the cyber threat.

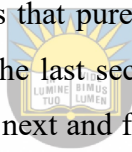
- **The HCMF Tier 3 review** – Governance Management pillar focused on the audit and risk management processes, but the expert review feedback identified a lack of explicit mention of legislation. Therefore, a *cybersecurity legislation* pillar that addresses issues of cyber governance was included as the final pillar in the Tier. The cybersecurity legislation pillar includes, but is not limited to the fundamental precepts of the National Cybersecurity Policy Framework, the Protection of Personal Information Act (POPIA), and the Electronic Communications and Transactions Act. This pillar will support the organisation when responding, recovering or protecting its environment from cybersecurity threats.

With all the contributions added to the HCMF, it can be argued that the HCMF can effectively and efficiently mitigate cybersecurity threats to electronic health records and is sound. The following section concludes the discussion of the chapter.

5.4 CONCLUSION

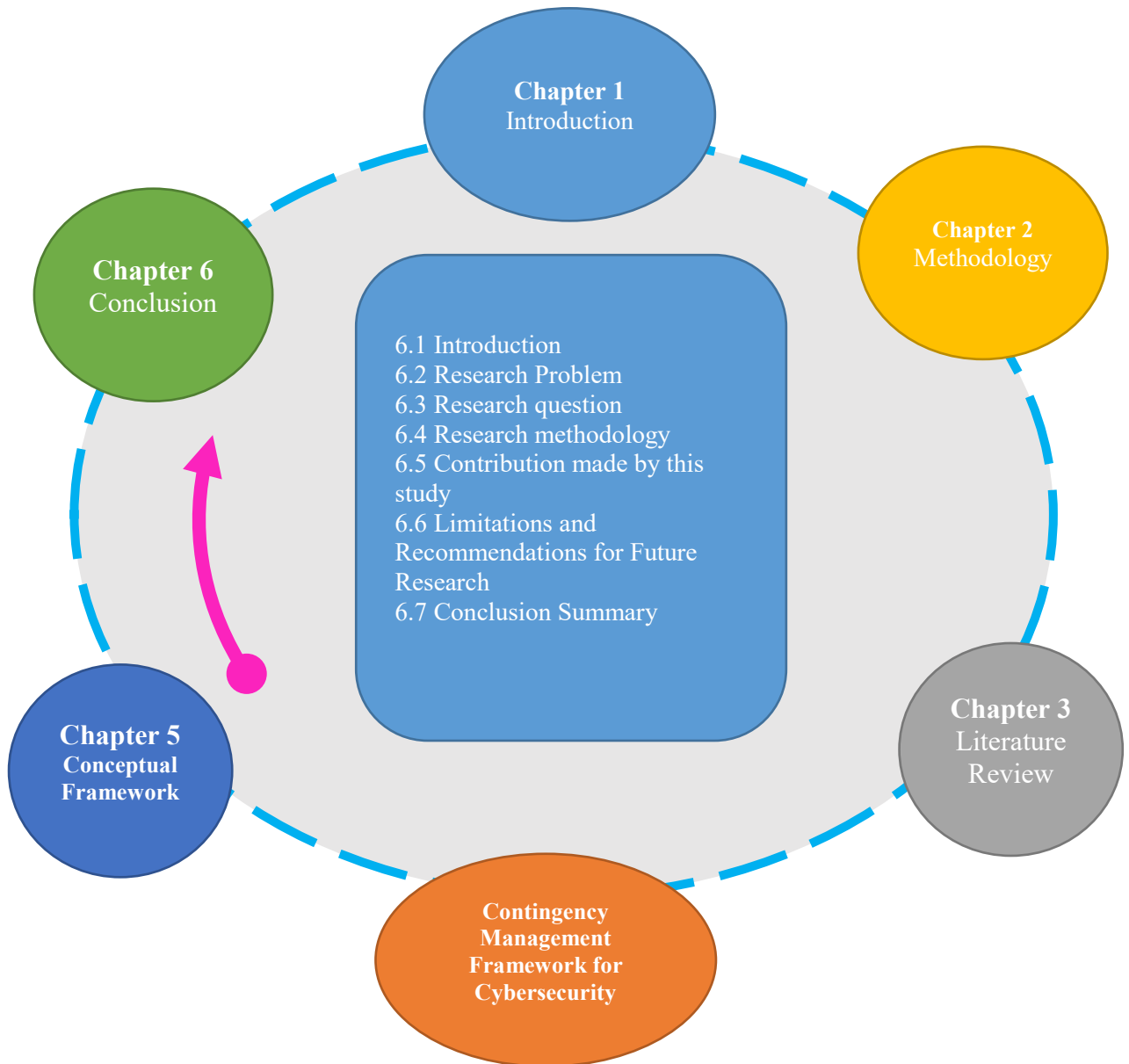
This chapter presented a proposed contingency management framework that focuses on information security management implementation in an organisation. The proposed framework type is verified to be a conceptual framework that assumed the structure of the IST established in previous chapters. Four different implementations tiers that formed the HCMF were derived and presented respectively.

The first implementation tier of the HCMF deals with the support function of the organisation focusing on security awareness training, incident response planning management, information sharing management, and connected medical devices. The next implementation tier is considered to be the four processes of management of the HCMF and consists of identify, direct, appraise, and track. The governance management of the HCMF is dealt with at the third implementation tier. This tier deals precisely with how the organisation will deal with audit control, risk control and the legislation of cybersecurity in the healthcare sector. This is followed by the last implementation tier, the contingency management tier. The final tier of the HCMF is presented as three pillars that purely responds to the contingency approach of EHRs within the healthcare facility. The last section describes the evaluation of the HCMF through an expert review process. The next and final chapter is a concluding summary of the research.



University of Fort Hare
Together in Excellence

CHAPTER 6: CONCLUSION



6.1 INTRODUCTION

“A writer needs to keep in mind that the conclusion is often what a reader remembers best” (Willingham, 2021).

This research study zeroed in on South African endeavors toward safeguarding sensitive patient information against cybersecurity threats. It was confirmed that despite the fact that the South African government was found to have joined the new developments and initiated a project in May 2002 to implement EHR country-wide, there is widespread concern that cybersecurity threats are placing the health and well-being of patients at risk. Thus, the intended goal of the research study was to develop a contingency management framework to use as a means to mitigate cybersecurity threats to electronic health records (EHRs) in the public health sector in SA. This framework was reviewed by subject matter experts and was presented in Chapter 5.

Having completed that task, this final discussion will conclude this dissertation. The first section revisits the research problem introduced in Chapter 1. The researchable problem of the study is followed by research questions that were also discussed in Chapter 1 of the study. The next section outlines the research methodology used by the study followed by the contribution of the study. The following section presents the evaluation of the research study, the limitations, as well as the directions for future research. Thereafter, the chapter concludes.

6.2 RESEARCH PROBLEM

For the past decade, South African healthcare facilities equipped with interconnected medical devices using EHRs to exchange or store patient information have experienced cybersecurity threats and vulnerabilities. The explosion of internet connectivity to existing computer networks has resulted in medical devices being exposed to new cyberspace. The State Security Agency has since declared that South Africa is under cyberattack. Hacker's most important information is related to patients' records. There is an increase in the number of cyberattacks and medical identity theft with millions of medical records stolen globally.

The number of malware attacks compromising healthcare data in South Africa in the first quarter of 2019 increased by 22% compared with the first quarter of 2018. The Verizon Data Breach Investigations Report (DBIR) states that more than 52% of breaches occurred due to hacking, 28% involved malware and 33% included phishing or social engineering respectively. The Cost of Data Report states that more than a 30% chance exists that organisations across the board will be experiencing an increase of major data breaches annually due to cybersecurity

breaches. The IBM Frequency Data Breaches 2019 report predicted that public healthcare organisations will be amongst the top targeted by cyberattacks due to lack of cyber protection. Financial estimates of about ZAR 3.7 billion of indirect losses and ZAR 6.5 billion of direct cost in financial losses from cyberattacks occurred in the healthcare sector. It has been reported that South Africa's financial losses are estimated to be approximately ZAR50 billion due to illegal cyber incidents involving online personal records.

In light of the above research problem, the objective of the research study was to develop a conceptual framework that will be used to mitigate cybersecurity threats to EHRs in the public healthcare sector in SA.

6.3 RESEARCH QUESTION

Chapter 1 introduced the research study. The existing literature on cybersecurity threats compromising EHRs in the public health sector in South Africa was investigated. The researcher found that the digital transformation in healthcare services resulted in the exposure and vulnerabilities of healthcare technologies that included healthcare devices connecting hospitals and clinics to traverse patient data. Based on the literature review, the following research question for the study was formulated: *How can contingency management of electronic health records mitigate cybersecurity threats in the public health sector of South Africa?* The primary objective of the research study was to develop a contingency management framework to mitigate cybersecurity threats to EHRs in the public health sector in South Africa.

Three sub-research questions were also formulated to assist the researcher to answer the main research question. These sub-research questions were listed in Chapter 1 (Section 1.3.2) as follows:

i) How can cybersecurity threats compromise electronic health records in the public health sector in South Africa?

This sub-research question was addressed in Chapter 1 and Chapter 3 during the literature review which provided a detailed overview of how cybersecurity threats can compromise EHRs in the public health sector in South Africa. This led to the understanding of electronic health records, and more importantly the increase in percentages of data breaches in third world countries versus SA. The primary focal point of this sub-research question was to examine instances of patients' information being compromised during cybersecurity threats as a result

of the vulnerability of primary healthcare facilities. The literature review also cited the risk of patients' medical information being in the hands of cybercriminals, resulting in lives at risk.

ii) How can contingency management safeguard information in electronic health records against cybersecurity threats?

The second sub-research question of the study concentrated on safeguarding information in the EHR. Chapter 3 discussed safeguarding measures put in place in SA to protect its citizens from acts of theft and potential sabotage, including policies and procedures such as the Protection of Personal Information Act, Minimum Information Security Standard. As part of measuring safeguards for patient information in the healthcare sector, contingency management activities emanating from security management and proceeding sequentially from security policy, risk management, internal control, and information auditing were discussed.

iii) How can a framework assist with the contingency management to secure electronic health records against cybersecurity threats in the public health sector in South Africa?

Chapters 3, 4, and 5 addressed the third and final sub-research question. A comparative analysis of how various countries promoted cybersecurity in the healthcare sector using policies, models, strategies, and frameworks to safeguard EHRs was presented in Chapter 4 (section 4.2). This section provided an international perspective of how third-world countries responded to cybersecurity attacks. Chapter 3 (Section 3.4) presented initiatives of South Africa's response to cyberattacks where its introduction of the National Cybersecurity Policy Framework (NCPF), Protection of Personal Information Act (POPIA), and the Electronic Communication and Transaction Act (ECT) was made as attempts to address the security and privacy concern in EHRs. However, according to IBM and the Ponemon Institute, despite these initiatives, issues of cybercrime in the healthcare sector continued to increase in periods between 2009 – 2015 and 2017 – 2019 by more than 52% of data breaches targeting medical or health information and that included medical reports, patient discharge, drug information. Mimecast further presented a staggering 30% likelihood that organisations across the healthcare sector are experiencing major data breaches.

As the reliance on information security becomes more prevalent, data security risks continue to grow with no literature found on contingency management frameworks in the healthcare sector to safeguard information in electronic health records. In considering the answer to the above sub-research question led to the development of a proposed healthcare contingency

management framework (HCMF) to mitigate cybersecurity threats to electronic health records in the public health sector in South Africa. The framework served as the contribution of this study and is discussed further in the contribution section.

6.4 RESEARCH METHODOLOGY

Chapter 2 provided an in-depth portrayal of the way in which this research study was conducted. The literature review was used as a paradigm in this research study as it was best suited to answer the question presented in this research study. The literature review was further used to produce qualitative research synthesis and this is more critical of the contents of the literature review. In order to draw and evaluate information from existing knowledge to identify future research needs, a literature review was used as secondary data. Furthermore, to yield better and thorough results, following a predetermined protocol, a three-phased approach was used including:

- i) planning,**
- ii) conducting, and**
- iii) reporting the results of the literature review.**



During the identification process of research, literature relevant to the defined research question was retrieved. This was made possible by grouping search strings of key terms. Each group contains terms that are either synonyms, different forms or search words, or terms that have similar or related meaning within a domain as presented in the search terms table below.

Table 7: Search key terms

	Group 1	Group 2	Group 3	Group 4	Group 5
Term 1	Electronic health record	electronic-health	cybersecurity	Contingency Management	Public healthcare sector
Term 2	Patient health record	EHealth	Cyber security information systems	Incident Management	Public healthcare sector
Term 3		Electronic Health	Cybersecurity information systems	Emergency management	Public hospitals
Term 4			Cybercrime	Uncertainty management	Government clinics
Term 5					Public health facilities

The results filtered from the ACM Digital library between 2016 and 2021 yielded only seven publications that were related to information security and not e-health or electronic health record. The results filtered from Science Direct Digital library gave better results to those of ACM library in that 102 results were found that were related to the first research question of the study *“how can cybersecurity threats compromise electronic health records in the public health sector in South Africa”*. However, most of these results were either *“information Management”* or *“Information Systems”*. The identification process of research proceeded to the second sub-research question *“How can contingency management safeguard information in electronic health records against cybersecurity threats”*, and the narrowing of the search resulted in 58 publications that could be used. The last and final sub-research question *“How can a framework assist with the contingency management to secure electronic health records against cybersecurity threats in the public health sector in South Africa?”* yielded only nine publications. A total of 234 publications from the University of Fort Hare were retrieved from digital libraries

Primary data was collected through expert reviews, and the experts that were used were approached for reviews as they are subject matter experts in cybersecurity and have conducted threat analysis in the field of electronic health records. The literature drawn from secondary data specific to both the domain of cybersecurity and that of EHR in the public health sector in South Africa was reviewed and evaluated by all six experts nominated. The HCMF was also

developed in Chapter 5 and was validated by four experts nominated. The results from these reviews were submitted and amended and were also considered as a contribution to the study as discussed in the following section.

6.5 CONTRIBUTION MADE BY THIS STUDY

Golden-Biddle and Locke, (2007) posit that “*an idea becomes a contribution when it is construed as important by the members of the scholarly community, relative to the accepted knowledge constituted by the field’s written work*”. Within the growing context of the digital transformation in healthcare service, there is ample literature on what electronic health records in the healthcare sector are and the critical information they hold. Furthermore, cyberspace has modified the manner in which information systems operate and the intention was to enhance people's lifestyles. Considering this, institutions and notions at large have embraced and become progressively subject to cyberspace to perform their operations. Consequently, the need for cybersecurity has never been greater.

While trying to resolve the identified problem, the essential goal of this study, as set out in Chapter 1 (Section 1.4), was a proposal that a contingency management framework to mitigate cybersecurity threats to electronic health records in the public health sector in South Africa be developed.



University of Fort Hare
Together in Excellence

To address this objective, the accompanying secondary objectives were illustrated in Chapter 1 (Section 1.4) as presented herewith below:

- i) Investigate cases of patients’ information compromised during cybersecurity threats due to vulnerability of primary care facility;
- ii) Explore strategies that could be applied by contingency management to safeguard information in electronic health records;
- iii) Develop a contingency management framework to assist to secure EHRs against cybersecurity threats in the public health sector in South Africa.

It is clear that each of the secondary objectives of this research study has been achieved. It can therefore be proclaimed that the essential objective of this research study, which was to develop a contingency management framework to mitigate cybersecurity threats to electronic health records in the public health sector in South Africa, has been met satisfactorily.

6.6 LIMITATIONS AND RECOMMENDATIONS FOR FUTURE RESEARCH

The focus of this research study was directed toward providing a contingency management framework to address the cybersecurity threats from patient files in the public health sector in South Africa. One of the major constraints to the research study was the closing of the country due to the COVID19 pandemic, resulting in difficulty to access University resources. Furthermore, with South Africa being a developing country, the study of EHRs which is partially implemented was also a hindrance and as a result the researcher relied on information from developed countries.

6.7 CONCLUSION SUMMARY

Cybersecurity had humble beginnings. In the years since its inception, it has grown exponentially, offering organizations endless challenges. The cybersecurity threats that compromised electronic health records worldwide have also resulted in risks to patient lives. To a large extent, cyberspace has been used to generate financial gains that are better than selling in the black market.



As a result of this conclusion chapter, the research study has been summarized and the implications of findings explained. The research problem was defined and followed by the research questions in order to describe the theoretical background for the study. A summary of how the main research and sub-research questions were presented, followed by the contribution made by this research study. The methodology used in this research study was briefly discussed. Finally, the limitation and recommendations for the future research study were presented.

REFERENCE LIST

- Adom, D., Hussein, E., & Adu-Agyem, J. (2018). Theoretical and Conceptual Framework: Mandatory Ingredients of a Quality Research. *International Journal of Scientific Research*, 7(January), 438–441.
- Akinsanya, O. O., Papadaki, M., & Sun, L. (2020). Towards a maturity model for health-care cloud security (M2HCS). *Information and Computer Security*, 28(3), 321–345. <https://doi.org/10.1108/ICS-05-2019-0060>
- Al-Dhahri, S., Al-Sarti, M., & Abdul, A. (2017). Information Security Management System. *International Journal of Computer Applications*, 158(7), 29–33. <https://doi.org/10.5120/ijca2017912851>
- Al-Matari, O. M. M., Helal, I. M. A., Mazen, S. A., & Elhennawy, S. (2021). Adopting security maturity model to the organizations' capability model. *Egyptian Informatics Journal*, 22(2), 193–199. <https://doi.org/10.1016/j.eij.2020.08.001>
- Alali, H. (2018). Health Information Privacy and Security Framework : Supporting Electronic Medical Records in Healthcare Systems, (June 2017).
- Alba, M. (1980). *National development plan. The Philippine journal of nursing* (Vol. 50). <https://doi.org/ISBN:978-0-621-41180-5>
- Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. *Applied Sciences (Switzerland)*, 10(10). <https://doi.org/10.3390/app10103660>
- Almuhammadi, S., & Alsaleh, M. (2017a). Information Security Maturity Model for Nist Cyber Security Framework, (February), 51–62. <https://doi.org/10.5121/csit.2017.70305>
- Almuhammadi, S., & Alsaleh, M. (2017b). Information Security Maturity Model for Nist Cyber Security Framework, 51–62. <https://doi.org/10.5121/csit.2017.70305>
- Alqurshi, A. (2020). Investigating the impact of COVID-19 lockdown on pharmaceutical education in Saudi Arabia – A call for a remote teaching contingency strategy. *Saudi Pharmaceutical Journal*, 28(9), 1075–1083. <https://doi.org/10.1016/j.jsps.2020.07.008>
- Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers and Security*, 98. <https://doi.org/10.1016/j.cose.2020.102003>
- Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J., Choudrie, J., ... Maynard Sean, B. (2020). A Cyber Security Awareness and Education Framework for South Africa.

Journal of Physics: Conference Series, 51(14), 103284. Retrieved from <https://doi.org/10.1016/j.im.2020.103284>
<https://doi.org/10.1016/j.tele.2020.101415>
<https://doi.org/10.1016/j.ijinfomgt.2020.102123>
<https://doi.org/10.1016/j.chb.2020.106531>

Amin, M. E. K., Nørgaard, L. S., Cavaco, A. M., Witry, M. J., Hillman, L., Cernasev, A., & Desselle, S. P. (2020). Establishing trustworthiness and authenticity in qualitative pharmacy research. *Research in Social and Administrative Pharmacy*, 16(10), 1472–1482. <https://doi.org/10.1016/j.sapharm.2020.02.005>

And, T. N. I. of S. (2014). Framework for Improving Critical Infrastructure Cybersecurity Note to Reviewers on the Update and Next Steps. *Proceedings of the Annual ISA Analysis Division Symposium*, 535, 1–67. Retrieved from https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_with-markup.pdf

Anderson, C., Baskerville, R. L., & Kaul, M. (2017). Information Security Control Theory: Achieving a Sustainable Reconciliation Between Sharing and Protecting the Privacy of Information. *Journal of Management Information Systems*, 34(4), 1082–1112. <https://doi.org/10.1080/07421222.2017.1394063>

Anderson, S., & Williams, T. (2018). Cybersecurity and medical devices: Are the ISO/IEC 80001-2-2 technical controls up to the challenge? *Computer Standards and Interfaces*, 56(June 2017), 134–143. <https://doi.org/10.1016/j.csi.2017.10.001>

Angst, C. M., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quarterly: Management Information Systems*, 33(2), 339–370. <https://doi.org/10.2307/20650295>

Armitage, A., & Keeble-Allen, D. (2008). Undertaking a structured literature review or structuring a literature review: Tales from the field. *Electronic Journal of Business Research Methods*, 6(2), 103–114.

Armitage, A., & Keeble-Allen, D. (2017). Structured Literature Reviews. *A Review of the Field Working Paper*, 1–24.

Australian Digital Health Agency. (2020). Information Security Guide Protect Your Healthcare Business. Retrieved from <https://www.digitalhealth.gov.au/about-the-agency/digital-health-cyber-security-centre/information-security-guide-for-small-healthcare-businesses/HD127> Information Security Guide for small healthcare businesses (co-branded with Stay Smart Online) Online V

- Barrett, M. (2018a). Framework for improving critical infrastructure cybersecurity. *Proceedings of the Annual ISA Analysis Division Symposium*, 535, 9–25.
- Barrett, M. (2018b). Framework for improving critical infrastructure cybersecurity. *Proceedings of the Annual ISA Analysis Division Symposium*, 535, 9–25.
- Bay, M. (2016). What is cybersecurity? In search of an encompassing definition for the post-Snowden era. <https://Frenchjournalformediaresearch.Com:443/Lodel-1.0/Main>.
- Bellekens, X., Seam, A., Nieradzinska, K., Tachtatzis, C., Cleary, A., Atkinson, R., & Andonovic, I. (2015). Cyber-Physical-Security Model for Safety-Critical IoT Infrastructures. *Wireless World Research Forum Meeting 35, At Copenhagen, Denmark*, (October).
- Bilau, A. A., Witt, E., & Lill, I. (2018). Research methodology for the development of a framework for managing post-disaster housing reconstruction. *Procedia Engineering*, 212, 598–605.
- Bissict, J. (2016). *Augmenting Security Event Information with Contextual Data to Improve the Detection Capabilities of a SIEM*. University of Cape Town.
- Blair, G., Pagano, R., & Burns, B. (2019). Contingency Framework for Addressing Failure in Information Systems. *Journal of Innovative Research in IT & Computer Science*, 3(02), 1–4.
- Blumberg, B., Cooper, D., Schindler, P., et al. (2014). *Business Research Methods* (4rd ed.). Oxford: Oxford University Press.
- Bob, U., Padayachee, A., Gordon, M., & Moutlana. (2017). Enhancing innovation and technological capabilities in the management of E-waste: case study of South African government sector. Science, Technology and Society. *Case Study of South African Government Sector. Science, Technology and Society*, 22(2), 332–349.
- Bottomley, E.-J. (2020, June 20). SA hit as hackers target hospitals during Covid-19 crisis - here's what Life may be facing. *Business Insider*. Retrieved from <https://www.businessinsider.co.za/life-hospitals-hit-by-cyberattack-2020-6>
- Brannen, J. (2017). Mixing methods: Qualitative and quantitative research. *Abingdon: Routledge*.
- Bucea-Radu-Tonis (Bucea Manea), R. M.-T. (2014). Management of Innovative Projects through Agile Technology. *Journal of Economic Development, Environment and People*, 3(3), 59. <https://doi.org/10.26458/jedep.v3i3.76>
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS*

- Quarterly: Management Information Systems*, 34(SPEC. ISSUE 3), 523–548.
<https://doi.org/10.2307/25750690>
- Burke, W., Oseni, T., Jolfaei, A., & Gondal, I. (2019). Cybersecurity Indexes for eHealth. *ACM International Conference Proceeding Series*. <https://doi.org/10.1145/3290688.3290721>
- Burns, B., & West, P. (2000). Applying organisational learning: Lessons from the automotive industry. *International Journal of Operations and Production Management*, 10(20), 1236–1251.
- Business Tech. (2019). *Big increase in identity fraud cases in South Africa*. *Business Tech News*. Retrieved from <https://businesstech.co.za/news/technology/342057/big-increase-in-identity-fraud-cases-in-south-africa/>
- Canada, G. of. (2013). Action Plan 2010-2015 for Canada's Cyber Security Strategy, 15. Retrieved from <https://www.securitepublique.gc.ca/cnt/rsrscs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf%0Ahttp://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf>
- Cassell, C., & Symon, G. (2014). *Essential Guide to Qualitative Methods in Organizational Research*. *Essential Guide to Qualitative Methods in Organizational Research*. London: Sage Publications. <https://doi.org/10.4135/9781446280119>
- Chang, L. Y. C., & Coppel, N. (2020). Building cyber security awareness in a developing country: Lessons from Myanmar. *Computers and Security*, 97, 101959. <https://doi.org/10.1016/j.cose.2020.101959>
- Chao, W. C., Hu, H., Ung, C. O. L., & Cai, Y. (2013). Benefits and challenges of electronic health record system on stakeholders: A qualitative study of outpatient physicians. *Journal of Medical Systems*, 37(4). <https://doi.org/10.1007/s10916-013-9960-5>
- Christopher, J. D., Gonzalez, D., White, D. W., Stevens, J., Grundman, J., Mehravari, N., ... Dolan, T. (2014). Cybersecurity Capability Maturity Model (C2M2). *Department of Homeland Security*, (February), 1–76. Retrieved from <https://energy.gov/oe/cybersecurity-critical-energy-infrastructure/cybersecurity-capability-maturity-model-c2m2-program>
- Cilliers, L., & Wright, G. (2017). Electronic Health records in the cloud: Improving primary health care delivery in South Africa. *Studies in Health Technology and Informatics*, 245(October), 35–39. <https://doi.org/10.3233/978-1-61499-830-3-35>
- CISA. (2020). Ransomware Activity Targeting the Healthcare and Public Health Sector Alert (AA20-302A). *Cisa*, 13. Retrieved from <https://us-cert.cisa.gov/ncas/alerts/aa20-302a>
- Clark, P. (1975). Organizational Design: A Review of Key Problems. *Administration &*

- Society*, 7(2), 213–256. <https://doi.org/10.1177/009539977500700205>
- Clubb, A. C., & Hinkle, J. C. (2015). Protection motivation theory as a theoretical framework for understanding the use of protective measures. *Criminal Justice Studies*, 28(3), 336–355. <https://doi.org/10.1080/1478601X.2015.1050590>
- Collis, J., & Hussey, R. (1942). *Business Research. Textile Research Journal* (Vol. 12). Hampshire: Macmillan International Higher Education. <https://doi.org/10.1177/004051754201200610>
- Collis, J., & Hussey, R. (2009). *Quantitative Methods for Business and Management* (3rd Edition). New York: Palgrave Macmillan.
- Commonwealth of Australia. (2016). *Australia's Cyber Security Strategy - Enabling innovation, growth and prosperity*. Department of the Prime Minister and Cabinet. Retrieved from <https://cybersecuritystrategy.dpmc.gov.au/>
- Connelly, L. M. (2016). Trustworthiness in qualitative research. *MEDSURG Nursing*, 25(6), 435–436. <https://doi.org/10.4324/9780203386071-22>
- Coucke, P. A. (2020). Cybersecurity in the health care sector. *Revue Medicale de Liege*, 75(2), 125–129.
- Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, 113(March), 48–52. <https://doi.org/10.1016/j.maturitas.2018.04.008>
- Creswell, J. W. (2003). *Research Design Qualitative, Quantitative, and Mixed Methods. Expert One-on-One Visual Basic. NET Business Objects* (3rd ed). London: Sage Publications.
- Crozier, G., Denzin, N., & Lincoln, Y. (1994). *Handbook of Qualitative Research. British Journal of Educational Studies* (Vol. 42). Thousand Oaks: Sage Publications 1994. <https://doi.org/10.2307/3121684>
- Cukier, M. (2007). Study: Hackers Attack Every 39 Seconds | A. James Clark School of Engineering, University of Maryland. Retrieved December 12, 2019, from <https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds>
- Cyber Security National Strategy. (2019). Turkey - National Cyber Security Strategy 2016-2019. Retrieved from <http://www.udhb.gov.tr/doc/siberg/UlusalSibereng.pdf>
- Daskin, E. (2019). The Turkish Cyber Security Strategy. *Structure, Legislation, and Challenges*, 2(1), 1–39.
- Dave, K., Boorman, R. J., & Walker, R. M. (2020). Management of a critical downtime event involving integrated electronic health records. *Collegian*, 27(5), 542–552. <https://doi.org/10.1016/j.colegn.2020.02.002>

- De Kleijn, R., & Van Leeuwen, A. (2018). Reflections and review on the audit procedure: Guidelines for more transparency. *International Journal of Qualitative Methods*, 17(1), 160940691876321. <https://doi.org/10.1177/1609406918763214>
- Denzin, N. K. (2010). Moments, mixed methods, and paradigm dialogs. *Qualitative Inquiry*, 16(6), 419–427. <https://doi.org/10.1177/1077800410364608>
- Department of Home Affairs. (2020). Australia's Cyber Security Strategy 2020, 1–52. Retrieved from <https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf>
- Department of Telecommunications and Postal Services. (2017). A Baseline Study on Cybersecurity Readiness. *The South African Department of Telecommunications and Postal Services*, 64. Retrieved from www.dtps.gov.za
- Design, O. M. (2013). Enhancing Nursing Students '. In *The effect of learning materials delivered by short message service*. (pp. 12–16). computer & education.
- Dewey, J. (2011). *The influence of darwinism on philosophy*. (J. Boydston & L. (Eds. . Hahn, Eds.), *The Pragmatism Reader: From Peirce through the Present* (The middle). Carbondale: Southern Illinois University Press (Original work published 1910b). <https://doi.org/10.7312/dewe19894-036>
- Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *in Excellence Computers and Security*, 92. <https://doi.org/10.1016/j.cose.2020.101747>
- DoD. (2020). Cybersecurity maturity model certification. *Department of Defense, DM(19–0824)*. Retrieved from <https://www.acq.osd.mil/cmmc/draft.html>
- Du, M., Vidal, J. M., & Markovsky, B. (2019). SOREC: A semantic content-based recommendation system for parsimonious sociology theory construction. *Proceedings - 5th IEEE International Conference on Big Data Service and Applications, BigDataService 2019, Workshop on Big Data in Water Resources, Environment, and Hydraulic Engineering and Workshop on Medical, Healthcare, Using Big Data Technologies*, 138–144. <https://doi.org/10.1109/BigDataService.2019.00025>
- Dumay, J., Bernardi, C., Guthrie, J., & Demartini, P. (2016). Integrated reporting: A structured literature review. *Accounting Forum*, 40(3), 166–185. <https://doi.org/10.1016/j.accfor.2016.06.001>
- eHealth NSW Government. (2016). eHealth Strategy for NSW Health. *NSW Government*. Retrieved from <https://www.health.nsw.gov.au/ehealth/documents/ehealth-strategy-for-nsw-health-2016-2026.pdf>

- Els, F., & Cilliers, L. (2018). *A privacy management framework for personal electronic health records*. *African Journal of Science, Technology, Innovation and Development*. University of Fort Hare. <https://doi.org/10.1080/20421338.2018.1509489>
- Englander, M. (2012). The Interview : Data Collection in Descriptive Phenomenological Human Scientific Research *. *Journal of Phenomenological Psychology, 43*, 13–35. <https://doi.org/10.1163/156916212X632943>
- Englander, M. (2016). The interview: Data collection in descriptive phenomenological human scientific research. *Journal of Phenomenological Psychology, 47*(1), 13–35. <https://doi.org/10.1163/156916212X632943>
- Eubank, B. H., Mohtadi, N. G., Lafave, M. R., Wiley, J. P., Bois, A. J., Boorman, R. S., & Sheps, D. M. (2016). Using the modified Delphi method to establish clinical consensus for the diagnosis and treatment of patients with rotator cuff pathology. *BMC Medical Research Methodology, 16*(1), 1–15. <https://doi.org/10.1186/s12874-016-0165-8>
- Experian. (2017). Fourth annual 2017 data breach industry forecast.
- Family health international. (2011). *Qualitative Research Methods Overview : A Data Collector's Field Guide*. *Qualitative Research Methods A Data Collectors Field Guide* (Vol. 2005). North Carolina: Family Health International. Retrieved from <http://www.fhi360.org/NR/rdonlyres/etl7vogszehu5s4stpzb3tyqlpp7rojv4waq37elpbyei3tgmc4ty6dunbccfzxtaj2rvbaubz4f/overview1.pdf>
- Feakin, T., Woodall, J., & Nevill, L. (2015). Cyber Maturity in the Asia-Pacific 2015. *Journal of the Japanese Society of Economics and Mathematics, Vol37, No.1/2*, 1–27. Retrieved from <https://www.aspi.org.au/publications/cyber-maturity-in-the-asia-pacific-region-2015/Cyber-Maturity-2015.pdf>
- Feix, M., & Procházka, D. (2017). Securing the Required Cyber Defence Capabilities. *Vojenské Rozhledy, 26*(4), 35–54. <https://doi.org/10.3849/2336-2995.26.2017.04.035-054>
- Flahault, S. T. A., Troncoso-Pastoriza, J. R., Lacey, D. F., Marie-Valentine Calcavecchia, F. A., Burlison, D., Vogel, D., ... Antoine, B. (2018). BMC Medical Informatics and Decision Making Cybersecurity of Hospitals. *Discussing the Challenges and Working towards Mitigating the Risks, 20*(1), 146.
- Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers and Security, 61*(61), 169–183. <https://doi.org/10.1016/j.cose.2016.06.002>
- Gage, N. (1989). *The Paradigm Wars and Their Aftermath: A*. (M. Hammersley, Ed.), *Teachers College Record* (Educational, Vol. 91). London: Sage Publications.

- Gasiba, T. E., Lechner, U., & Pinto-Albuquerque, M. (2021). CyberSecurity Challenges: Serious Games for Awareness Training in Industrial Environments. Retrieved from <http://arxiv.org/abs/2102.10432>
- Gill, A. Q., & Chew, E. (2019). Configuration information system architecture: Insights from applied action design research. *Information and Management*, 56(4), 507–525. <https://doi.org/10.1016/j.im.2018.09.011>
- Gkioulos, V., & Chowdhury, N. (2021). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review*, 40, 100361. <https://doi.org/10.1016/j.cosrev.2021.100361>
- Golden-Biddle, K., & Locke, K. L. (2007). *Qualitative Composing Second Edition*.
- Gourisetti, S. N. G., Mylrea, M., & Patangia, H. (2020a). Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis. *Future Generation Computer Systems*, 105, 410–431. <https://doi.org/10.1016/j.future.2019.12.018>
- Gourisetti, S. N. G., Mylrea, M., & Patangia, H. (2020b). Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis. *Future Generation Computer Systems*, 105, 410–431. <https://doi.org/10.1016/j.future.2019.12.018>
- Graneheim, U. H., & Lundman, B. (2004). Qualitative content analysis in nursing research: Concepts, procedures and measures to achieve trustworthiness. *Nurse Education Today*, 24(2), 105–112. <https://doi.org/10.1016/j.nedt.2003.10.001>
- Granja, C., Janssen, W., & Johansen, M. A. (2018). Factors determining the success and failure of eHealth interventions: Systematic review of the literature. *Journal of Medical Internet Research*, 20(5), e10235. <https://doi.org/10.2196/10235>
- Grey, J. A., Bernstein, K. T., Sullivan, P. S., Purcell, D. W., Chesson, H. W., Gift, T. L., & Rosenberg, E. S. (2016). Estimating the population sizes of men who have sex with men in US States and counties using data from the American community survey. *JMIR Public Health and Surveillance*, 2(1), e14. <https://doi.org/10.2196/publichealth.5365>
- Groves, R. M., Fowler Jr, F. J., Couper, M. P., Lepkowski, J. M., Singer, E., & Tourangeau, R. (2011). *Survey methodology*. J. Wiley.
- Hamidi, H. (2019). An approach to develop the smart health using Internet of Things and authentication based on biometric technology. *Future Generation Computer Systems*, 91, 434–449. <https://doi.org/10.1016/j.future.2018.09.024>
- Hegde, V. (2018). Cybersecurity for Medical Devices. *Proceedings - Annual Reliability and*

- Maintainability Symposium, 2018-Janua*. <https://doi.org/10.1109/RAM.2018.8463049>
- Henriques, D., Pereira, R. F., Almeida, R., & Mira da Silva, M. (2020). IT governance enablers in relation to IoT implementation: a systematic literature review. *Digital Policy, Regulation and Governance*, 22(1), 32–49. <https://doi.org/10.1108/DPRG-02-2019-0013>
- Hilma Inoukapo, S. T. (2014). Non-Elective Caesarean Sections In The Khomas Region, Namibia. *Implications for Midwifery Practice.*, 105.
- Hong, K. S., Chi, Y. P., Chao, L. R., & Tang, J. H. (2003). An integrated system theory of information security management. *Information Management and Computer Security*, 11(5), 243–248. <https://doi.org/10.1108/09685220310500153>
- Höpken, W., Eberle, T., Fuchs, M., & Lexhagen, M. (2019). Google Trends data for analysing tourists' online search behaviour and improving demand forecasting: the case of Åre, Sweden. *Information Technology and Tourism*, 21(1), 45–62. <https://doi.org/10.1007/s40558-018-0129-4>
- Hothersall, S. J. (2019). Epistemology and social work: Enhancing the integration of theory, practice and research through philosophical pragmatism. *European Journal of Social Work*, 5(22), 860–870.
- IBM. (2016). *2016 Cost of Data Breach Study: Global Analysis*. Retrieved from <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN%0Ahttps://securityintelligence.com/media/2016-cost-data-breach-study/>
- IBM. (2019). Cost of a data breach report. *IBM Security*, 76. Retrieved from <https://www.ibm.com/downloads/cas/ZBZLY7KL>
- Igwenagu, C. (2016). Fundamentals of Research Methodology and Data Collection. *LAP Lambert Academic Publishing*, (June), 4. Retrieved from https://www.researchgate.net/publication/303381524_Fundamentals_of_research_methodology_and_data_collection
- Insights, M., & Popular, M. (2015). Insights & Publications Strategic choices for banks in the digital age. *McKinsey Quarterly*, 2018(1), 2–5. Retrieved from http://www.mckinsey.com/insights/financial_services/Strategic_choices_for_banks_in_the_digital_age?cid=DigitalEdge-eml-alt-mck-oth-1501
- Izaara, A. A., Ssembatya, R., & Kagawa, F. (2019). An access control framework for protecting personal electronic health records. *2018 International Conference on Intelligent and Innovative Computing Applications, ICONIC 2018*, 1–6. <https://doi.org/10.1109/ICONIC.2018.8601287>

- Jalali, M. S., & Kaiser, J. P. (2018). *Cybersecurity in hospitals: A systematic, organizational perspective*. *Journal of Medical Internet Research* (Vol. 20). <https://doi.org/10.2196/10059>
- Jaquire, V., & Von Solms, B. (2015). A best practice strategy framework for developing countries to secure cyberspace. *Proceedings of the 10th International Conference on Cyber Warfare and Security, ICCWS 2015*, 472–480.
- Jennings, G. R. (2012). *Qualitative research methods. Handbook of Research Methods in Tourism: Quantitative and Qualitative Approaches*. California: Sage Publications. <https://doi.org/10.4337/9781781001295>
- Johnson, L. (2020). Cybersecurity framework. *Security Controls Evaluation, Testing, and Assessment Handbook*, (February 2014), 537–548. <https://doi.org/10.1016/b978-0-12-818427-1.00012-4>
- Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed Methods Research: A Research Paradigm Whose Time Has Come. *Educational Researcher*, 33(7), 14–26. <https://doi.org/10.3102/0013189X033007014>
- Karabacak, B., Yildirim, S. O., & Baykal, N. (2016). A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness. *International Journal of Critical Infrastructure Protection*, 15, 47–59. <https://doi.org/10.1016/j.ijcip.2016.10.001>
- Katurura, M. (2018). *A framework to evaluate the e-readiness of Public Healthcare in the Eastern Cape to implement an Electronic Health record system*.
- Katurura, M., & Cilliers, L. (2016). The extent to which the POPI act makes provision for patient privacy in mobile personal health record systems. In *2016 IST-Africa Conference, IST-Africa 2016*. <https://doi.org/10.1109/ISTAFRICA.2016.7530595>
- Katurura, M., & Cilliers, L. (2017). A review of the implementation of electronic health record systems on the African continent. *African Conference on Information Systems & Technology (ACIST)*, (10th-11th July), 1–11. Retrieved from <https://www.researchgate.net/publication/322701219%0AAr>
- Katurura, M., & Cilliers, L. (2018). Electronic health record system in the public health care sector of South Africa: A systematic literature review. *African Journal of Primary Health Care & Family Medicine*, 10(1), 1–8. <https://doi.org/10.4102/phcfm.v10i1.1746>
- Katuu, S. (2016). Transforming South Africa's health sector: The eHealth Strategy, the implementation of electronic document and records management systems (EDRMS) and the utility of maturity models. *Journal of Science and Technology Policy Management*,

7(3), 330–345. <https://doi.org/10.1108/JSTPM-02-2016-0001>

- Katuu, S. (2018). Health information systems, ehealth strategy, and the management of health records: The quest to transform South Africa's public health sector. *Healthcare Policy and Reform: Concepts, Methodologies, Tools, and Applications, 1*, 493–517. <https://doi.org/10.4018/978-1-5225-6915-2.ch024>
- Katuu, S. (2019). Health Information Systems, eHealth Strategy, and the Management of Health Records: The Quest to Transform South Africa's Public Health Sector. *Healthcare Policy and Reform: Concepts, Methodologies, Tools, and Applications. IGI Global*, 493–517.
- Kaušpadienė, L., Ramanauskaitė, S., & Čenys, A. (2019). Information security management framework suitability estimation for small and medium enterprise. *Technological and Economic Development of Economy, 25*(5), 979–997. <https://doi.org/10.3846/tede.2019.10298>
- Kempen, A. (2017). Cybersecurity in South Africa-are there lessons to be learned from the major data breach?. *Servamus Community-Based Safety and Security Magazine, 110*(12), 16–19.
- Kessler, R., & Hitt, J. R. (2016). Re: Electronic Health Record Challenges, Workarounds, and Solutions Observed in Practices Integrating Behavioral Health and Primary Care. *Journal of the American Board of Family Medicine, 29*(2), 289–290. <https://doi.org/10.3122/jabfm.2016.02.150355>
- Kgabo, H. B. (2017). the Improvement of Organisational Performance and Healthcare Service Delivery Through Knowledge Management Practices in the Gauteng Department of Health.
- Kitts, J. (2017). For more information : Critical Infrastructure and Canada's Health Sector.
- Klein, H. K., & Myers, M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly: Management Information Systems, 23*(1), 67–94. <https://doi.org/10.2307/249410>
- Kleynhans, A. (2011). Is South Africa ready for a national Electronic Health Record (EHR)?, (70992657), 1–100.
- Kofod-petersen, A. (2014). How to do a structured literature review in computer science. *Researchgate*, (May 2015), 1–7.
- Kortjan, N. (2013). *A Cyber Security Awareness and Education Framework for South Africa*.
- Kothari, C. . (2004). *Research Methodology: Methods and Techniques* (2nd revise). Jaipur: New Age International (P) Limited.

- Kremer, J. F., & Müller, B. (2014). *Cyberspace and international relations: Theory, prospects and challenges*. *Cyberspace and International Relations: Theory, Prospects and Challenges* (Vol. 9783642374). <https://doi.org/10.1007/978-3-642-37481-4>
- Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, 25(1), 1–10. <https://doi.org/10.3233/THC-161263>
- Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences (Switzerland)*, 8(6). <https://doi.org/10.3390/app8060898>
- Kurth, A. (2019). Angola Passes Personal Data Protection Law | Privacy & Information Security Law Blog. Retrieved July 22, 2020, from <https://www.huntonprivacyblog.com/2011/09/19/angola-passes-personal-data-protection-law/>
- La Fleur, C., Hoffman, B., Gibson, C. B., & Buchler, N. (2021). Team performance in a series of regional and national US cybersecurity defense competitions: Generalizable effects of training and functional role specialization. *Computers and Security*, 104, 102229. <https://doi.org/10.1016/j.cose.2021.102229>
- Lamminen, J., Tech, L. S., Forsvik, H., Eng, M. S., Ph, D., Voipio, V., & Tech, D. S. (2016). Decision making process for clinical it investments in a public health care organization - contingency approach to support the investment decision process. *Finnish Journal of EHealth and EWelfare*, 7(2–3), 122–134.
- Land, M. (2016). Information security. *The Comprehensive Handbook of School Safety*, (June), 75–86. <https://doi.org/10.31803/tg-20180717222848>
- Latham, D. (2021). Cyberattackers increasingly target healthcare and South Africa is not immune. Retrieved March 30, 2021, from <https://health-e.org.za/2021/01/09/cyberattackers-increasingly-target-healthcare-and-south-africa-is-not-immune/>
- Le Bris, A., & El Asri, W. (2021). STATE OF CYBERSECURITY & CYBER THREATS IN HEALTHCARE ORGANIZATIONS Applied Cybersecurity Strategy for Managers. *ESSEC Business School*, 13. Retrieved from <http://blogs.harvard.edu/cybersecurity/files/2017/01/risks-and-threats-healthcare-strategic-report.pdf>
- Le, N. T., & Hoang, D. B. (2017a). Can maturity models support cyber security? *2016 IEEE 35th International Performance Computing and Communications Conference, IPCCC*

2016. <https://doi.org/10.1109/PCCC.2016.7820663>
- Le, N. T., & Hoang, D. B. (2017b). Capability maturity model and metrics framework for cyber cloud security. *Scalable Computing*, 18(4), 277–290. <https://doi.org/10.12694/scpe.v18i4.1329>
- Leech, N. L., Barrett, K. C., & Morgan, G. A. (2005). SPSS for Intermediate Statistics: Use and Interpretation. Retrieved July 29, 2019, from <https://psycnet.apa.org/record/2004-18541-000>
- Lejaka, T. K., Da Veiga, A., & Loock, M. (2019). Cyber security awareness for small, medium and micro enterprises (SMMEs) in South Africa. *2019 Conference on Information Communications Technology and Society, ICTAS 2019*, 1–6. <https://doi.org/10.1109/ICTAS.2019.8703609>
- Leppan, C. (2017). Analysis of a South African cyber-security awareness campaign for schools using interdisciplinary communications, (April), 180. <https://doi.org/http://hdl.handle.net/10948/18167>, vital:28582
- Lewis, C. (2018). *Qualitative Research in Nursing and Healthcare (Fourth edition)*. *Nursing Standard* (Vol. 32). John Wiley @ Sons. <https://doi.org/10.7748/ns.32.22.34.s27>
- Liebowitz, J. (Ed. . (2019). *The Handbook of Applied Expert Systems. The Handbook of Applied Expert Systems*. <https://doi.org/10.1201/9780138736654>
- Liu, C., & Zhang, X. (2015). Critically Analyse the Contribution Made by Qualitative Research to ELT (English Language Teaching) in China. *International Journal of English Language Teaching*, 2(2), 45–55. <https://doi.org/10.5430/ijelt.v2n2p45>
- LLC HITRUST Alliance. (2016). Healthcare Sector Cybersecurity Framework Implementation Guide, (May), 1–112.
- LUO, H. (2012). Introducing Research Methodology: A Beginner’s Guide to Doing a Research Project by FLICK, UWE. *The Modern Language Journal*, 96(3), 481–483. <https://doi.org/10.1111/j.1540-4781.2012.01382.x>
- Ma, F. (2015). A Review of Research Methods in EFL Education. *Theory and Practice in Language Studies*, 5(3), 566. <https://doi.org/10.17507/tppls.0503.16>
- Malakoane, B., Heunis, J. C., Chikobvu, P., Kigozi, N. G., & Kruger, W. H. (2020). Public health system challenges in the Free State, South Africa: A situation appraisal to inform health system strengthening. *BMC Health Services Research*, 20(1), 1–14. <https://doi.org/10.1186/s12913-019-4862-y>
- Mambo, M., & Saeednia, S. (2003). Signature schemes based on the DSA and the related atomic proxy functions. *IEEE International Symposium on Information Theory -*

- Proceedings*, 535, 138. <https://doi.org/10.1109/isit.2003.1228152>
- Marchildon, G. P., Allin, S., & Merkur, S. (2020). Canada: Health system review. *Health Systems in Transition*, 22(3), 194. Retrieved from <https://apps.who.int/iris/handle/10665/336311>
- Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: How safe are we? *BMJ (Online)*, 358(May 2021), 0–4. <https://doi.org/10.1136/bmj.j3179>
- Massaro, M., Dumay, J., & Guthrie, J. (2016). On the shoulders of giants: undertaking a structured literature review in accounting. *Accounting, Auditing and Accountability Journal*, 29(5), 767–801. <https://doi.org/10.1108/AAAJ-01-2015-1939>
- Masum, M. R. (2018). Information Security & Risk Management Training, (September). <https://doi.org/10.13140/RG.2.2.23797.01764>
- McCusker, K., & Gunaydin, S. (2015). Research using qualitative, quantitative or mixed methods and choice based on the research. *Perfusion (United Kingdom)*, 30(7), 537–542. <https://doi.org/10.1177/0267659114559116>
- McNeill, P., & Chapman, S. (2010). Secondary data. *Research Methods*, 131–171. https://doi.org/10.4324/9780203463000_chapter_5
- Miller, R., & Brewer, J. (2015). *Naturalistic Inquiry. The A-Z of Social Research*. Beverly Hills: SAGE Publications UK: London, England. <https://doi.org/10.4135/9781412986281.n232>
- Mkhomazi, S. S., & Iyamu, T. (2013). A guide to selecting theory to underpin information systems studies. In *IFIP Advances in Information and Communication Technology* (Vol. 402, pp. 525–537). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-38862-0_33
- Moeti, M., & Kalema, B. M. (2014). Analytical hierarchy process approach for the metrics of information security management framework. *Proceedings - 6th International Conference on Computational Intelligence, Communication Systems and Networks, CICSyN 2014*, (May), 89–94. <https://doi.org/10.1109/CICSyN.2014.31>
- Mohammed, I., & Musa Bade, A. (2019). Cybersecurity Capability Maturity Model for Network System. *International Journal of Development Research*, 9(7), 28637–28641. <https://doi.org/28 July 2019>
- Moody, G. D., Siponen, M., & Pahlila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, 1(42).
- Morgan, D. L. (2014). Pragmatism as a Paradigm for Social Research. *Qualitative Inquiry*,

- 20(8), 1045–1053. <https://doi.org/10.1177/1077800413513733>
- Mouhammed, A. (2015). *Quantitative methods for business and economics. Quantitative Methods for Business and Economics* (3rd ed.). New York NY: Palgrave Macmillan. <https://doi.org/10.4324/9781315701332>
- Mouton, J. (1996). *Understanding social research*. Pretoria: Van Schaik.
- Mouton, J. (2001). *How to succeed in your master's and doctoral studies*. Pretoria: Van Schaik Publishers.
- Mungadze, S. (2020, August 31). Life Healthcare reveals damage caused by data breach. Retrieved from <https://www.itweb.co.za/content/rW1xLv59YPGvRk6m>
- Murire, O. T. (2016). *Critical success factors for the adoption and continued use of social media in teaching and learning among lecturers at a historically Black university in South Africa*. University of Fort Hare.
- Murshed, F., & Zhang, Y. (2016). Thinking orientation and preference for research methodology. *Journal of Consumer Marketing*, 33(6), 437–446. <https://doi.org/10.1108/JCM-01-2016-1694>
- Mustard, S. (2014). The NIST cybersecurity framework. <https://doi.org/10.4018/978-1-7998-4471-6.ch008>
- Nalin, M., Baroni, I., Faiella, G., Romano, M., Matriciano, F., Gelenbe, E., ... Clemente, F. (2019). The European cross-border health data exchange roadmap: Case study in the Italian setting. *Journal of Biomedical Informatics*, 94(April), 103183. <https://doi.org/10.1016/j.jbi.2019.103183>
- Nathan, A. J., & Scobell, A. (2012). How China sees America. *Foreign Affairs*, 91(5), 1689–1699. <https://doi.org/10.1017/CBO9781107415324.004>
- Nehouse, W., Keith, S., Scribner, B., & Witte, G. (2017). NIST 2017 National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. *National Institute of Standards and Technology (NIST)*, (November), 144. Retrieved from <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf>
- Netherlands. (1967). 濟無No Title No Title No Title. *Angewandte Chemie International Edition*, 6(11), 951–952., p. 2.
- News24. (2019a). City of Joburg slowly resumes services after cyber attack | News24. Retrieved December 11, 2019, from <https://www.news24.com/SouthAfrica/News/city-of-joburg-slowly-resumes-services-after-cyber-attack-20191026>
- News24. (2019b). Cyber criminals hacking remote-controlled medical devices could kill

- patients, conference hears | Fin24. Retrieved January 18, 2020, from <https://www.fin24.com/Companies/Health/cyber-criminals-hacking-remote-controlled-medical-devices-could-kill-patients-conference-hears-20190829-2>
- News24. (2019c). SA, Zim must work together to fight cyber attacks - Mugabe | News24. Retrieved December 11, 2019, from <https://www.news24.com/Africa/Zimbabwe/sa-zim-must-work-together-to-fight-cyber-attacks-mugabe-20171004>
- Ngoqo, B., & Flowerday, S. V. (2015). Information Security Behaviour Profiling Framework (ISBPF) for student mobile phone users. *Computers and Security*, 53(53), 132–142. <https://doi.org/10.1016/j.cose.2015.05.011>
- Ngxabane, M., & Cilliers, L. (2020). A framework for addressing young adults' trust issues concerning mobile access to electronic health records. *2020 Conference on Information Communications Technology and Society, ICTAS 2020 - Proceedings*, 01(1), 15. <https://doi.org/10.1109/ICTAS47918.2020.233998>
- Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic Analysis: Striving to Meet the Trustworthiness Criteria. *International Journal of Qualitative Methods*, 16(1), 1–13. <https://doi.org/10.1177/1609406917733847>
- Nunu, K. (2019). A Big Data Framework to improve government service delivery in South Africa. *Thesis (Unpublished Research Material Cited in Terms of the Written Approval of Prof. Tiko Iyamu) Faculty of Informatics and Design, Cape Peninsula University of Technology, South Africa*, (October).
- O’Cathain, A. (2019). Mixed methods research. In *Qualitative Research in Health Care* (pp. 169–180). Burlington, MA: Jones and Bartlett Learning. <https://doi.org/10.1002/9781119410867.ch12>
- Oates, B. J. (2006). *Researching Information Systems and Computing. Inorganic Chemistry* (Vol. 37). Retrieved from <http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=2836698&tool=pmcentrez&rendertype=abstract>
- Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information Communication and Society*, 23(1), 128–147. <https://doi.org/10.1080/1369118X.2018.1486870>
- Offner, K. L., Sitnikova, E., Joiner, K., & MacIntyre, C. R. (2020). Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation. *Intelligence and National Security*, 35(4), 556–585.

<https://doi.org/10.1080/02684527.2020.1752459>

Olden, P. C. (2016). Contingency Management of Health Care Organizations: It Depends. *Health Care Manager*, 35(1), 28–36. <https://doi.org/10.1097/HCM.0000000000000093>

Oliver, J. (2019). *State of Email Security Report 2019*. *Journal of Chemical Information and Modeling* (Vol. 53).

Onuiri, E. E., Idowu, S. A., & Komolafe, O. (2015). Electronic Health Record Systems and Cyber- Security Challenges. *International Conference on African Development Issues*, (July), 98–105.

Park, et. al. (2018). Consolidating structured and unstructured security and threat intelligence with knowledge graphs, *I*. Retrieved from <https://patents.google.com/patent/US20180159876A1/en>

Ponemon Institute. (2015). 2015 Cost of Data Breach Study: Impact of Business Continuity Management, (June), 1–19.

Ponemon Institute. (2019). *2019 Cost of a data Breach report: Global Analysis*. Retrieved from <https://www.ibm.com/downloads/cas/ZBZLY7KL>

Public Safety Canada. (2018). *National Cyber Security Strategy : Canada's Vision for Security and Prosperity in the Digital Age*. Public Safety Canada. Retrieved from <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx?wbdisable=true>



University of Fort Hare
Together in Excellence

PWC. (2018). Building a united front on financial crimes in the financial services sector. Retrieved July 25, 2020, from <https://www.pwc.co.za/en/press-room/cyber-security.html>

Quay-De La Vallee, H., Selby, P., & Krishnamurthi, S. (2016). On a (Per)Mission: Building privacy into the app marketplace. *SPSM 2016 - Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices, Co-Located with CCS 2016*, 63–72. <https://doi.org/10.1145/2994459.2994466>

Rascado Sedes, P., Ballesteros Sanz, M. A., Bodí Saera, M. A., Carrasco Rodríguez-Rey, L. F., Castellanos Ortega, A., Catalán González, M., ... Trenado Álvarez, J. (2020). Contingency plan for the intensive care services for the COVID-19 pandemic. *Medicina Intensiva (English Edition)*, 44(6), 363–370. <https://doi.org/10.1016/j.medine.2020.03.003>

Report, S., & Ventures, C. (2020). The 2020 Healthcare Cybersecurity Report 2020 Healthcare Cybersecurity Report Cybersecurity Ventures, 1–5. Retrieved from www.herjavecgroup.com

Republic of South Africa. (2002). Electronic Communication and Transaction Act.

- Government Gazette*, 446(1046). Retrieved from <http://www.gov.za/sites/www.gov.za/files/a25-02.pdf>
- Republic of South Africa. (2013). Protection of Personal Information, Act 4 of 2013. *Government Gazette*, (912), 1–75. Retrieved from http://www.gov.za/sites/www.gov.za/files/37067_26-11_Act4of2013ProtectionOfPersonalInfor_correct.pdf
- Reychav, I., Beerli, R., Balapour, A., Raban, D. R., Sabherwal, R., & Azuri, J. (2019). How reliable are self-assessments using mobile technology in healthcare? The effects of technology identity and self-efficacy. *Computers in Human Behavior*, 91(June 2018), 52–61. <https://doi.org/10.1016/j.chb.2018.09.024>
- Rojas, R., Muedas, A., & Mauricio, D. (2019). Security maturity model of web applications for cyber attacks. *ACM International Conference Proceeding Series*, 130–137. <https://doi.org/10.1145/3309074.3309096>
- Ross, J. (2017). Cybersecurity: A Real Threat to Patient Safety. *Journal of Perianesthesia Nursing*, 32(4), 370–372. <https://doi.org/10.1016/j.jopan.2017.05.005>
- Rowlands, B. (2003). Employing Interpretive Research to Build Theory of Information Systems Practice. *Australasian Journal of Information Systems*, 10(2), 3–22. <https://doi.org/10.3127/ajis.v10i2.149>
- Salkind, N. (2012). *Encyclopedia of Research Design*. Encyclopedia of Research Design. Sage Publications. <https://doi.org/10.4135/9781412961288>
- Sandison, B. (2018). Australian Institute of Health and Welfare. *Impact*, 2018(2), 80–81. <https://doi.org/10.21820/23987073.2018.2.80>
- Sarstedt, M., Bengart, P., Shaltoni, A. M., & Lehmann, S. (2018). The use of sampling methods in advertising research: a gap between theory and practice. *International Journal of Advertising*, 37(4), 650–663. <https://doi.org/10.1080/02650487.2017.1348329>
- Saunders, M., Lewis, P., & Thornhill, A. (2018). *Understanding research philosophies. Creative Research*. Harlow: Pearson Education. <https://doi.org/10.5040/9781474247115.0016>
- Saunders, M. N. K., & Bezzina, F. (2015). Reflections on conceptions of research methodology among management academics. *European Management Journal*, 33(5), 297–304. <https://doi.org/10.1016/j.emj.2015.06.002>
- Saunders, M. N. K., & Thornhill, A. (2003). Organisational justice, trust and the management of change: An exploration. *Personnel Review*, 32(3), 360-375+394. <https://doi.org/10.1108/00483480310467660>

- Şentürk, H., Çil, C. Z., & Sağıroğlu, Ş. (2016). Cyber Security Analysis of Turkey. *International Journal of Information Security Science*, 1(4), 112–125.
- Shah, S. M., & Khan, R. A. (2020). Secondary use of electronic health record: Opportunities and challenges. *IEEE Access*, 8(July), 136947–136965. <https://doi.org/10.1109/ACCESS.2020.3011099>
- Simon, M. K. (2011). Dissertation and scholarly research: Recipes for success (2011 Ed.). *Dissertation Success, LLC*, 344. Retrieved from <http://www.dissertationrecipes.com/>
- Sinkovics, R. R., Penz, E., & Ghauri, P. N. (2008). Enhancing the trustworthiness of qualitative research in international business. *Management International Review*, 48(6), 689–714. <https://doi.org/10.1007/s11575-008-0103-z>
- Smith, C. (2019). *Major spike in SA cyber attacks, over 10 000 attempts a day. News24*. Retrieved from <https://www.fin24.com/Companies/ICT/major-spike-in-sa-cyber-attacks-over-10-000-attempts-a-day-security-company-20190429>
- Smith, M., Busi, M., Ball, P., & Van Der Meer, R. (2019). Factors influencing an organisation's ability to manage innovation: a structured literature review and conceptual model. *Managing Innovation: What Do We Know About Innovation Success Factors?* 69–90.
- Sobers, R. (2019). 110 Must-Know Cybersecurity Statistics for 2020 | Varonis. Retrieved December 3, 2019, from <https://www.varonis.com/blog/cybersecurity-statistics/>
- Somepalli, S. H., Tangella, S. K. R., & Yalamanchili, S. (2020). Information Security Management. *HOLISTICA – Journal of Business and Public Administration*, 11(2), 1–16. <https://doi.org/10.2478/hjbpa-2020-0015>
- South African Government. (2015a). the National Cybersecurity Policy Framework. *Government Gazette*, (39475), 66–95.
- South African Government. (2015b). *the National Cybersecurity Policy Framework. Government Gazette*. Retrieved from www.gpwonline.co.za
- South African National Department of Health. (2017). Government Notices - National Health Insurance Policy. *Government Gazette*, 7(40955), 1–70. Retrieved from https://www.gov.za/sites/default/files/gcis_document/201707/40955gon627.pdf
- Strekalova, Y. A. (2019). Electronic health record use among cancer patients: Insights from the Health Information National Trends Survey. *Health Informatics Journal*, 25(1), 83–90. <https://doi.org/10.1177/1460458217704246>
- Sutherland, E. (2017). Governance of Cybersecurity – The Case of South Africa. *The African Journal of Information and Communication*, 20(20), 83–112. <https://doi.org/10.23962/10539/23574>

- Swart, I. (2015). Pro-active visualization of cyber security on a National Level: A South African Case Study, (April 2015). Retrieved from https://www.researchgate.net/publication/305443420_Pro-active_visualization_of_cyber_security_on_a_National_Level_A_South_African_Case_Study
- Tatar, Mehtap, Mollahaliloğlu, Salih, Şahin, & Bayram. (2017). Turkey: health system review, *13*(6), 186. Retrieved from <https://apps.who.int/iris/handle/10665/330325>
- TechTarget. (2019). Cybersecurity maturity model lays out four readiness levels. Retrieved August 8, 2020, from <https://searchsecurity.techtarget.com/tip/Cybersecurity-maturity-model-lays-out-four-readiness-levels>
- The Guardian. (2020). *US hospitals systems facing “imminent” threat of cyber-attacks, FBI warns*. Retrieved from <https://www.theguardian.com/society/2020/oct/28/us-healthcare-system-cyber-attacks-fbi>
- Thomas, S. (2016). *An analysis of the adoption of electronic health records in primary healthcare*. Retrieved from <https://repository.up.ac.za/handle/2263/52333>
- Tikkanen, R., & Abrams, M. (2020). U.S. Health Care from a Global Perspective, 2019 | Commonwealth Fund. *The Commonwealth Fund*. Retrieved from <https://www.commonwealthfund.org/publications/issue-briefs/2020/jan/us-health-care-global-perspective-2019>
- Tobergte, D. R., & Curtis, S. (2015). THE CONTRIBUTION MADE BY QUALITATIVE RESEARCH TO TESOL (Teaching English to Speakers of Other Languages). *International Journal of English Language Teaching Vol.3, 3*(2), 1–14.
- Tungpantong, C., Nilsook, P., & Wannapiroon, P. (2021). A Conceptual Framework of Factors for Information Systems Success to Digital Transformation in Higher Education Institutions. *2021 9th International Conference on Information and Education Technology, ICIET 2021*, 57–62. <https://doi.org/10.1109/ICIET51873.2021.9419596>
- UNISA. (2001). CHAPTER 3 Research design, research method and population. *Convenience Sampling*, 84–99. Retrieved from <http://uir.unisa.ac.za/bitstream/handle/10500/1313/04chapter3.pdf?sequence=4>
- Uppal, R. (2020). NIST Cybersecurity Framework Improving Critical Infrastructure Cybersecurity by managing it’s cyber risks | International Defense Security & Technology Inc. Retrieved April 20, 2021, from <https://idstch.com/cyber/nist-cybersecurity-framework-improving-critical-infrastructure-cybersecurity-by-managing-its-cyber-risks/>
- Ursillo, S. J., & Arnold, C. (2019). Cybersecurity Is Critical for all Organizations - Large and

- small. *Ifac*. Retrieved from <https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/cybersecurity-critical-all-organizations-large-and-small>
- Valizadeh, M., & Vaezi, S. . (2016). Education Teachings of Molla Hadi Sabzevari. *International Journal of Humanities and Cultural Studies, 1*, 729–744.
- Van Heerden, R., Von Soms, S., & Mooi, R. (2016). Classification of cyber attacks in South Africa. *2016 IST-Africa Conference, IST-Africa 2016*, (May 2016). <https://doi.org/10.1109/ISTAFRICA.2016.7530663>
- Van Niekerk, B. (2017). An Analysis of Cyber-Incidents in South Africa. *The African Journal of Information and Communication*, (20), 113–132. <https://doi.org/10.23962/10539/23573>
- Verizon. (2019). Verizon: 2019 Data Breach Investigations Report. *Computer Fraud & Security, 2019*(6), 4. [https://doi.org/10.1016/s1361-3723\(19\)30060-0](https://doi.org/10.1016/s1361-3723(19)30060-0)
- WBI Evaluation Group. (2007). Guided Expert Reviews. *Needs Assessment Knowledge Base*, 1–4.
- Weeks, R. (2014). The implementation of an electronic patient healthcare record system : a South African case study. *Journal of Contemporary Management, 11*, 101–119.
- White, G. B. (2007). The community cyber security maturity model. *Proceedings of the Annual Hawaii International Conference on System Sciences, 1*(January 2015), 8. <https://doi.org/10.1109/HICSS.2007.522>
- Whitman, M. E. (2016). *Principles of information security. Cengage Learning* (Sixth Edit). Boston, MA 02210. Retrieved from www.cengagebrain.com
- Wiid, J., & Diggines, C. (2013). Marketing research (2nd ed). *Cape Town, South Africa: Juta*.
- Williams, P., Ashill, N., & Naumann, E. (2017). Toward a contingency theory of CRM adoption. *Journal of Strategic Marketing, 25*(5–6), 454–474. <https://doi.org/10.1080/0965254X.2016.1149211>
- Willingham, D. T. (2021). Why don't students like school? *A Cognitive Scientist Answers Questions about How the Mind Works and What It Means for the Classroom John Wiley & Sons*.
- Woo, S. H., Pettit, S. J., Kwak, D. W., & Beresford, A. K. C. (2011). Seaport research: A structured literature review on methodological issues since the 1980s. *Transportation Research Part A: Policy and Practice, 45*(7), 667–685. <https://doi.org/10.1016/j.tra.2011.04.014>
- World Economic Forum. (2019). *WEF_4IR_Beacons_of_Technology_and_Innovation_in_Manufacturing_report_2019*.

World Economic Forum. Retrieved from www.weforum.org

- Wright, G., Mahony, D. O., & Cilliers, L. (2017). Electronic health information systems for public health care in South Africa : a review of current operational systems 10th Health Informatics in Africa Conference (HELINA 2017) Electronic health information systems for public health care in South Afri. *Health Informatics in Africa*, 4(January), 1–164. <https://doi.org/10.12856/JHIA-2017-v4-i1-164>
- Yassine, A., Singh, S., Hossain, M. S., & Muhammad, G. (2019). IoT big data analytics for smart homes with fog and cloud computing. *Future Generation Computer Systems*, 91, 563–573. <https://doi.org/10.1016/j.future.2018.08.040>
- Zastepa, E., Sun, J. C., Clune, J., & Mathew, N. (2020). Adaptation of contingency management for stimulant use disorder during the COVID-19 pandemic. *Journal of Substance Abuse Treatment*, 118(August), 108102. <https://doi.org/10.1016/j.jsat.2020.108102>
- Zayyad, M. A., & Toycan, M. (2018). Factors affecting sustainable adoption of e-health technology in developing countries: An exploratory survey of Nigerian hospitals from the perspective of healthcare professionals. *PeerJ*, 2018(3). <https://doi.org/10.7717/peerj.4436>
- Zelmer, J. (2018). Cybersafe Healthcare, 45.



University of Fort Hare
Together in Excellence

APPENDICES

Appendix A – Ethical Certificate

ETHICS CLEARANCE REC-270710-028-RA Level 01

Project Number:	CIL021SNGX01
Project title:	A contingency management framework to mitigate cybersecurity threats to electronic health records in the public health sector in South Africa.
Qualification:	Masters in Information Systems
Principal Researcher:	Mbulelo Ngxabane
Supervisor:	Prof L Cilliers
Co-supervisor:	Mr D Boucher

On behalf of the University of Fort Hare's Research Ethics Committee (UREC) I hereby grant ethics approval for CIL021SNGX01. This approval is valid for 12 months from the date of approval. Renewal of approval must be applied for BEFORE termination of this approval period. Renewal is subject to receipt of a satisfactory progress report. The approval covers the undertakings contained in the above-mentioned project and research instrument(s). The research may commence as from the 30/07/20, using the reference number indicated above.

Note that should any other instruments be required or amendments become necessary, these require separate authorisation.
Please note that the UREC must be informed immediately of

-
- Any material breaches of ethical undertakings or events that impact upon the ethical conduct of the research.

The Principal Researcher must report to the UREC in the prescribed format, where applicable, annually, and at the end of the project, in respect of ethical compliance.

The UREC retains the right to

- Withdraw or amend this approval if
 - Any unethical principal or practices are revealed or suspected;
 - Relevant information has been withheld or misrepresented;
 - Regulatory changes of whatsoever nature so require;
 - The conditions contained in the Certificate have not been adhered to.
- Request access to any information or data at any time during the course or after completion of the project.

Your compliance with DoH 2015 guidelines and other regulatory instruments and with UREC ethics requirements as contained in the UREC terms of reference and standard operating procedures, is implied.

The UREC wishes you well in your research.

Yours sincerely



Professor Renuka Vithal
UREC-Chairperson
31 August 2020

Appendix B – Proof Reader Certificate



Editing certificate

TO WHOM IT MAY CONCERN

I, Jeanne Enslin, acknowledge that I did the language editing of **Mbulelo Ngxabane's** dissertation submitted in fulfilment of the requirements for the degree Master of Commerce – Information Systems – at the University of Fort Hare.

The title of the dissertation is:

A contingency management framework to mitigate cybersecurity threats to electronic health records in the public health sector in South Africa

All language corrections and changes are evident in the version of the dissertation in track changes and with several comments for the student's attention.

The quality of the final document, in terms of language, formatting and references remains the student's responsibility.

Jeanne Enslin
Language editor
jeanneenslin@gmail.com

28 October 2021.

BA English and History (University of Stellenbosch)
Senior Teaching Diploma (University of Stellenbosch)
Honours in Translation Studies, cum laude (Unisa)
Post-graduate diploma in Editing, cum laude (University of Stellenbosch)

Appendix C – Turnitin Report

Thesis final version			
ORIGINALITY REPORT			
16%	13%	7%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS
PRIMARY SOURCES			
1	Submitted to University of Fort Hare Student Paper		1%
2	hdl.handle.net Internet Source		1%
3	www.sis.pitt.edu Internet Source		1%
4	etd.cput.ac.za Internet Source		1%
5	libdspace.ufh.ac.za Internet Source		1%
6	uir.unisa.ac.za Internet Source		<1%
7	bmcmedinformdecismak.biomedcentral.com Internet Source		<1%
8	www.homeaffairs.gov.au Internet Source		<1%
9	www.nist.gov Internet Source		<1%

Appendix D – Expert Review Brief and Questionnaire



University of Fort Hare
Together in Excellence

Department of Information Systems, University of Fort Hare

Questionnaire: A contingency management framework to mitigate cybersecurity threats to electronic health records in the public health sector in South Africa

Expert Review Brief

Dear Expert Reviewer,

Thank you for your willingness to participate in this study. Your feedback is important. Please complete the consent form and read the relevant summary regarding the proposed Healthcare Contingency Management Framework before completing the Questionnaire.

Purpose of the Framework

I am a student in the Department of Information System at the University of Fort Hare (East London Campus), The focus of the research project is to investigate cybersecurity threats to electronic health records in the public health sector in South Africa. The purpose of this healthcare Contingency Management Framework (HCMF) is to propose how to mitigate cybersecurity threats to electronic health records (EHR) in the public health sector in South Africa. Contingency management includes activities that originate from security management and proceeds sequentially from security policy, risk management, internal control to information auditing. By answering the 15 questions in this questionnaire you will have participated in the evaluation of the Contingency Management Framework (HCMF). As a subject matter expert, you are nominated to participate in this study. You may choose to participate in this research study voluntarily.

Below graphic presentation is the Contingency Management Framework (HCMF) with its four (4) tiers briefly explained.

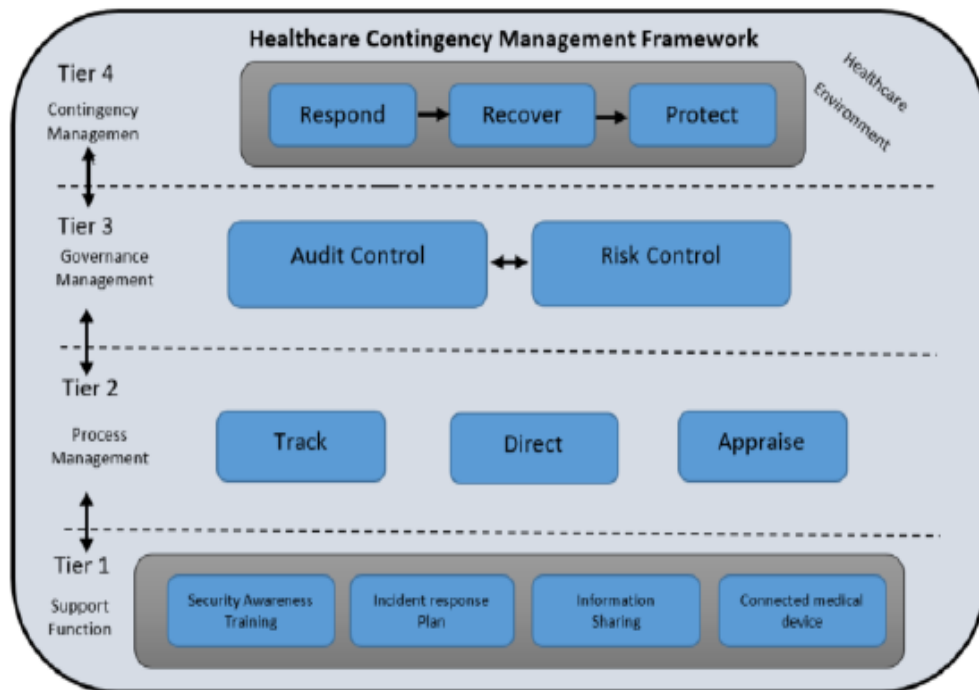


Figure 1: Proposed Contingency Management Framework

The proposed conceptual framework is divided into four (4) implementation tiers that provide how the healthcare organisation views its cybersecurity risk starting from the bottom first-tier going upward to fourth-tier as follows: -

- **Tier 1 – Support Function**

In considering repeated cyber intrusions through EHRs into the healthcare sector environment, the Tier 1 Support Function is focusing on providing security awareness training, incident response planning management, information sharing management, and monitoring of connected medical devices within the healthcare facility. This function is the ground level function that focuses on the everyday operations of the institution.

- **Tier 2 - Process Management**

The goals and priorities of a healthcare organization are to ensure consistent methods are in place to respond effectively and efficiently to cybersecurity threats against the EHR. The Process Management tier of the HCMF is designed to provide a consistent approach by determine elements of cybersecurity threats and ensuring no anomalies or a breach in the information system. Govern information obtained from an organisation and ensure health providers follow relevant guidelines. Finally, it tracks the effectiveness and performance of cybersecurity to ensure a continuously improved safe environment.

- **Tier 3 - Governance Management**

The highest level of security measures is required to manage cybersecurity and a risk-based approach through enterprise risk management is necessary. The Governance Management tier of the framework provides governance management functional support to the organisation, ensuring the establishment of relevant structures like Audit management committees and Risk Management committee. This tier will perform the audit management and risk management to the healthcare facility.

- **Tier 4 - Contingency management**

The healthcare sector is lacking a clear decision-making framework in information security of an EHR system investment. The best way of leading an organisation is contingent upon the internal and external challenges. Contingency plans exist to respond to adverse events, including incident response plans, business continuity plans, and disaster recovery plans. This tier enforces organisation to develop plans that support the response to threats against the EHRs.

Please read the relevant questions about the proposed Healthcare Contingency Management Framework and completing the Questionnaire below.

The Proposed Conceptual Framework for Healthcare Contingency

Management Questions

NB: Make use of space underneath every question to provide your opinion or additional pages as needed

1. Does the proposed HCMF address the cybersecurity concerns of South African patients that use EHRs and make meaningful contribution to the field of the information security?

Yes No

Elaborate

-
2. Does the proposed HCMF implementation tiers follow a sequential process to address the cybersecurity concerns of South African patients that use EHRs?

If you have selected 'No', then what can be improved?

Yes No

Elaborate

3. Do you think the proposed HCMF can assist in ensuring the cybersecurity awareness is addressed?

Yes No

Elaborate why you made the choice?

4. In your opinion, does tier 1 of the HCMF include all the necessary constructs for the “*Support Function*”?

Yes No

If you have selected 'No', then what can be improved?

Elaborate

5. In your opinion, does Tier 2 of the HCMF include all the necessary constructs for the “*Process Management*”?

Yes No

If you have selected 'No', then what can be improved?

Elaborate

6. In your opinion, does Tier 3 of the HCMF include all the necessary constructs for the “*Governance Management*”?

Yes No

If you have selected 'No', then what can be improved?

Elaborate

7. In your opinion, does Tier 4 of the HCMF include all the necessary constructs for the “*Contingency Management*”?

Yes No

If you have selected 'No', then what can be improved?

Elaborate

8. In your opinion, does all tiers of the HCMF interact between each other well?

Yes No

If you have selected 'No', then what can be improved?

Advantages

9. In your opinion, how can the proposed HCMF be made more understandable and easy to read?

Elaborate

10. Do you think the advancements in healthcare technology has exposed the security of patients' healthcare data in South Africa?

Yes No

Elaborate why you made the choice?

11. In your opinion, does the proposed CMF include the necessary elements to make a meaningful contribution towards mitigating cybersecurity threats to EHRs?

Elaborate why you made the choice?

12. Do you think the proposed Healthcare Contingency Management Framework (HCMF) can help to mitigate threats to patients' healthcare in South Africa?

Yes No

Elaborate

13. What is your overall opinion of the Healthcare Contingency Management Framework (HCMF) and how best you think it can be improved?

Yes No

Elaborate