



University of the Western Cape

South African National Bioinformatics Institute

Private Bag X17 Bellville 7535 South Africa
Telephone: +27 21 959 3645 / Fax +27 21 959 1237
E-mail: 3614275@myuwc.ac.za



**EXPLORING THE INFLUENCE OF ORGANISATIONAL,
ENVIRONMENTAL, AND TECHNOLOGICAL FACTORS ON
INFORMATION SECURITY POLICIES AND COMPLIANCE
AT SOUTH AFRICAN HIGHER EDUCATION INSTITUTIONS:
IMPLICATIONS FOR BIOMEDICAL RESEARCH.**

MSc Bioinformatics

Supervisor: Prof Alan Christoffels

Co-supervisor: Dr. Dominique Anderson

Student Researcher: Oluwafemi Peter, ABIODUN

Student no: 3614275

July 2020

DECLARATION

I, Oluwafemi Peter Abiodun, declare that this written submission represents my work and where other's ideas or words have been included, I have adequately cited and referenced the sources. I also declare that I have adhered to all ethics of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have not been properly cited or from whom proper permission has not been taken when needed. This thesis has not been submitted for any other degree at any other higher education institution.



Signed

July 07, 2020

Date

ABSTRACT

Headline reports on data breaches worldwide have resulted in heightened concerns about information security vulnerability. In Africa, South Africa is ranked among the top 'at-risk' countries with information security vulnerabilities and is the most the most cybercrime-targeted country. Globally, such cyber vulnerability incidents greatly affect the education sector, due, in part, to the fact that it holds more Personal Identifiable Information (PII) than other sectors. PII refers to (but is not limited to) ID numbers, financial account numbers, and biomedical research data.

In response to rising threats, South Africa has implemented a regulation called the Protection of Personal Information Act (POPIA), similar to the European Union General Data Protection Regulation (GDPR), which seeks to mitigate cybercrime and information security vulnerabilities. The extent to which African institutions, especially in South Africa, have embraced and responded to these two information security regulations remains vague, making it a crucial matter for biomedical researchers.

This study aimed to assess whether the participating universities have proper and reliable information security practices, measures and management in place and whether they fall in line with both national (POPIA) and international (GDPR) regulations. In order to achieve this aim, the study undertook a qualitative exploratory analysis of information security management across three universities in South Africa. A Technology, Organizational, and Environmental (TOE) model was employed to investigate factors that may influence effective information security measures. A Purposeful sampling method was employed to interview participants from each university.

From the technological standpoint, Bring Your Own Device (BYOD) policy, whereby on average, a student owns and connects between three to four internet-enabled devices to the network, has created difficulties for IT teams, particularly in the areas of authentication, explosive growth in bandwidth, and access control to security university servers. In order to develop robust solutions to mitigate these concerns, and which are not perceived by users as overly prohibitive, executive management should acknowledge that security and privacy issues are a universal problem and not solely an IT problem and equip the IT teams with the necessary tools and mechanisms to allow them to overcome commonplace challenges.

At an organisational level, information security awareness training of all users within the university setting was identified as a key factor in protecting the integrity, confidentiality, and availability of information in highly networked environments. Furthermore, the University's information security mission must not simply be a link on a website, it should be constantly re-

enforced by informing users during, and after, the awareness training. In terms of environmental factors, specifically the GDPR and POPIA legislations, one of the most practical and cost-effective ways universities can achieve data compliance requirements is to help staff (both teaching and non-teaching), students, and other employees understand the business value of all information. Users which are more aware of sensitivity of data, risks to the data, and their responsibilities when handling, storing, processing, and distributing data during their day to day activities will behave in a manner that would makes compliance easier at the institutional level.

Results obtained in this study helped to elucidate the current status, issues, and challenges which universities are facing in the area of information security management and compliance, particularly in the South African context. Findings from this study point to organizational factors being the most critical when compared to the technological and environmental contexts examined. Furthermore, several proposed information security policies were developed with a view to assist biomedical practitioners within the institutional setting in protecting sensitive biomedical data.

Keywords: Biomedical data, GDPR, Information security and management, POPIA, South African universities, TOE framework.

ACKNOWLEDGEMENTS

I would like to express my utmost gratitude to the Lord for making this research successful. He has been my strength, bestows wisdom, and everything throughout the course of this study.

My heartfelt appreciation goes to my amiable, wonderful and ever dynamic supervisor, **Professor Alan Christoffels** for giving me a superlative courage, uncommon support with a wonderful and excellent guidance throughout the duration of this study. He opened my eyes to a wider realm of knowledge, polished my research abilities, and gave me invaluable inputs at different stages of this study. To my co-supervisor, **Dr. Dominique Anderson**, I am grateful for being my incredible mentor over the years. Dominique has patiently guided me through this whole journey, providing me with unwavering support whenever I needed it. She has always had trust and confidence in me. Her expertise and pedagogical strategy has indeed shaped my life. I am sincerely indebted to her for all she has done during my learning period and her love, care, guidance and advice with humility has seen through and will have a lasting impact on my life. I was so fortunate to have had a competent, hardworking and skillful supervisors.

My sincere thanks also goes to my funders- SA Medical Research Council and the South African Research Chairs Initiative of the Department of Science and Innovation and National Research Foundation of South Africa, for their generous support throughout this study.

I also would like to express my appreciation to the entire Bioinformatics Department (SANBI) of UWC. I wish to thank Mrs. Ferial Mullins and Mrs. Fungie Mpithi for their administrative assistance at all times, and also the academic staff; Peter Van Heusden, Dr. Ruben Cloete, etc., for their assistance, support, and kind gestures. Many thanks also to Christoffel's lab and Cubicle 7 research group, for their very helpful advice, valuable feedback, and ongoing support. Likewise, I gratefully acknowledge the encouragement, motivation, and assistance from my colleagues most especially Rumbidzai Chitongo, Mrs. Abiola Babajide, Alicia Fernol Rudolph Serage, etc.

My sincere gratitude also goes to my family members mainly Prof. Babatunde J. Abiodun, Dr. Gbenga J. Abiodun, Mrs. Olabisi Abiodun, Mrs. Ayomidele Abigael, Mrs. Ruth Olagbegi, Mrs. Owolabi Toyin, Mr. Sesan Abiodun, Sanmi Abiodun, Deji Abiodun and Seun Abiodun for their love, prayers, and support as always.

Finally, I would like to appreciate my mother, Mrs. Alice Abiodun, for her uncommon affection, love, prayers, and support throughout my study.

GLOSSARY

BAYD – Bring All Your Devices

BYOD – Bring Your Own Device

CIA – Confidentiality, Integrity and Availability

CISO – Chief Information Security Officer

COBIT - Control Objectives for Information and Related Technologies

DES – Data Encryption Standard

DNA – Deoxyribonucleic Acid

EU – European Union

FAIR – Factor Analysis of Information Risk

FICA – Financial Intelligence Centre Act

GDPR – General Data Protection Regulation

HIPPA – Healthcare Information Portability and Accountability

ICS – Information and Communication

ID – Identification

IOT – Internet of things

ISMS – Information Security Management System

ISMT- Information Security Management Team

IT – Information Technology

ITU – International Telecommunication Union

NIST – National Institute of Science and Technology

PAIA – Promotion of Access to Information Act

PHI – Protected Health Information

PII - Personal Identifiable Information

POPIA – Protection of Personal Information Act

TOE - Technology, Organizational, and Environmental

PAPA – Privacy, Accuracy, Property, and Accessibility

RNA - Ribonucleic Acid

TABLE OF CONTENTS

DECLARATION.....	i
ABSTRACT.....	ii
ACKNOWLEDGEMENTS.....	iii
GLOSSARY.....	v
TABLE OF CONTENTS.....	vi
Chapter One: Overview	1
1 Introduction.....	1
1.1 Background.....	3
1.2 Overview of Research Problem Statement	4
1.3 The aim of the study	7
1.4 Research objectives.....	7
1.5 Justification	8
1.6 Ethical Measures	9
1.7 Limitations of the study	10
1.8 Dissertation Structure	10
Chapter Two: Overview	12
2 Introduction.....	12
2.1 Information.....	12
2.1.1 Information security.....	13
2.1.2 A Historical View to Information Security.....	17
2.1.3 Information Security Management System.....	20
2.1.4 Information Security Management System (ISMS) Frameworks	21
2.1.5 Conclusion on Information Security Management System	29
2.2 Security Policy	30
2.2.1 Policy as a Foundation to Security Management	30
2.2.2 Conclusion on Security Policy.....	33
2.3 Awareness of Information Security.....	33
2.3.1 Conclusions on Security Awareness	34
2.3.2 Compliance with Security.....	35
2.4 Data and information legislation	37
2.4.1 Some of the international and national information security laws and regulations required by South African Universities.	37
2.4.2 Information Security in Universities and some of the challenges	42
2.4.3 Summary and conclusion of the Literature Review.....	44

Chapter Three: Research Methodology and Motivation.....	46
3 Introduction.....	46
3.1 The standard for scientific empirical research methodology.....	46
3.2 Stage A- Research Design.....	47
3.2.1 Phase 1.....	47
3.2.2 Phase 2.....	48
3.2.3 Phase 3.....	49
3.3 Stage B - Data collection.....	52
3.3.1 Phase 4.....	53
3.3.2 Phase 5.....	53
3.4 Stage C- Data Analyse.....	55
3.5 Coding Software.....	56
3.6 Summary of the Chapter.....	56
Chapter Four: Findings and Discussion.....	58
4 Introduction.....	58
4.1 Demographic features of the participating institutions.....	58
4.1.1 Coding Results.....	59
4.1.2 Key findings.....	61
4.2 Discussion.....	64
4.2.1 University X.....	65
4.2.2 University Y.....	69
4.2.3 University Z.....	73
4.3 Overview of identified technology issues.....	76
4.4 Overview of identified Organizational Issues.....	77
4.5 Overview of Environmental Factors.....	79
Chapter Five: Observations and Recommendations Related to Addressing the Communication Gaps.....	82
5 Introduction.....	82
5.1 How can a university protect and secure their information?.....	83
5.2 The executive members and some of the common mistakes committed in information security decisions.....	84
5.2.1 Primarily depend on firewall instead of the 'human-wall'......	84
5.2.2 IT security approval duration and delays.....	85
5.2.3 Lack of understanding in relating information security to the organizational issue	85

5.2.4	Ignoring information security issues in the hopes they will resolve themselves	85
5.2.5	Failing to realize how much money the information and organizational reputations are worth.	86
5.2.6	Assigning CISO without given them necessary authority over people and organization processes	86
5.3	Some suggested responsibilities for the executives in order to have efficient and effective information security practices within their university settings.	87
5.4	The Security teams (CISOs) and some of the common mistakes committed on information security decisions.....	88
5.4.1	Lack of a holistic approach.....	88
5.4.2	Failure to organize consistent security awareness training programs.....	90
5.4.3	Ignoring the fundamental services and focusing on the extravagant	91
5.5	Suggested responsibilities for the CISOs and the security teams to minimize or avoid the above-mentioned mistakes to have effective information security practices within the university settings.	91
5.6	Users and some of the common mistakes committed on information security	93
5.6.1	Inappropriate use of technology devices as a result of BYODs policies.	94
5.6.2	Improper use of university accounts e.g. staff or student email account.....	94
5.6.3	Installing applications from unknown sources or unsafe sites.	95
5.6.4	Failing to install or update security patches.....	95
5.7	Some suggested responsibilities for the users for an effective information security practices within the university settings.	96
Chapter Six: Conclusion		97
6	Conclusion and Future Directives	97
References		99
Appendices		119

LIST OF FIGURES

Figure 1: The top ten sectors facing data breached (Symantec's Internet Security Threat Report Between January to December 2014).	6
Figure 2: Diagram demonstrating the polymorphous nature of information security and terms which are used interchangeably to define it (Crawley, 2017).....	16
Figure 3: Summary of methodology processes employed in this study	57
Figure 4: Generated codes in cloud words form.....	61
Figure 5: Technology, Organizational and Environmental (TOE) issues identified in univeristy X	65
Figure 6: Technology, Organizational and Environmental (TOE) issues identified in university Y	69
Figure 7: Technology, Organizational and Environmental (TOE) issues identified in university.....	73
Figure 8: An overview of themes on technology issues identified.....	77
Figure 9: An overview of identified themes on organisitional issues	78
Figure 10 : An overview of identified themes on environmental factors.	80
Figure 11: Combined trait issues identified from the extracted themes amongst the three universities.....	81

LIST OF TABLES

Table 1: Privacy concerns raised in the information age (Mason 2016).....	13
Table 2: Parkerian’s definition of information security.....	14
Table 3: Definitions of Information security from literature.....	15
Table 4: Comparison of ISMS frameworks (adapted from Susanto <i>et al.</i> , 2011).....	29
Table 5: Showing a methodology standard of an empirical research study	46
Table 6: Types of case study	50
Table 7: Participant recruitment and interview processes.....	54
Table 8: Summary of demographic features of the participated institutions.	58
Table 9: Super codes summary with respective density.	59

APPENDICES

Appendix 1: Proposed Information Security Policy.....	119
Appendix 2: Supplementary Data.....	144

Chapter One

Overview

1 Introduction

Globally, concerns over information security vulnerabilities are growing exponentially and are fuelled by several headline reports of data breach incidents, which appear to be increasing in size with each incident (AnnaMaria Andriotis, 2018; Lord, 2016; Regina Pazvakavambwa, 2018). South Africa was ranked amongst the most 'at-risk' countries on the continent for information security vulnerabilities, after losing approximately R50-billion to cybercrime in 2014 and is still considered the most cybercrime targeted country in Africa (Selene Brophy, 2017; Dean Workman, 2017; Van Niekerk, 2017; SAPS, 2011; Dlamini & Modise, 2012; Ahmore Burger-Smidt, 2018). Worldwide, when such incidents occur due to cyber vulnerabilities, the education sector is greatly affected due to the fact it holds more Personal Identifiable Information (PII) than most other sectors (Symantec's Internet Security Threat Report 2014; EDUCAUSE, 2018). The PII ranges from (but is not limited to) ID numbers and financial account numbers to biomedical research data. In response to growing threats, the General Data Protection Regulation (GDPR) was approved by European Union (EU) in April 2016, and became enforceable in May 2018, following the two years of a post-adoption grace period (Staunton, Slokenberga and Mascalzoni, 2019). This regulation applies to organizations (both within and outside the EU), that process and holds personal data of 'natural persons' residing in the EU, or who want to share data or collaborate with EU organization/institutions (Vollmer, 2018). This implies that any organization, whether a private or public, and which collects, stores, or shares identifying data of people in the EU, or transfers this personal data to third-party countries or international organizations will need to comply with the GDPR regardless of their location. Non-compliance may result in substantial fines up to 20 Million Euros or 4% of the worldwide annual turnover of the prior fiscal year (Stibosystems, 2018; EUGDPR, 2017).

In South Africa, a similar strategy is being implemented to mitigate the exponential increase in cybercrime and information security vulnerabilities. A regulation known as The Protection of Personal Information Act (POPIA), was designed to protect any personal information which is processed by both private and public organizations (including universities). The purpose of the POPI Act is to ensure that all South African organizational institutions responsibly conduct themselves when collecting, processing, storing, and sharing Personally Identifiable

Information (PII) (Staunton and De Stadler, 2019). The Act was signed into law in November 2013, and in April 2014 certain sections of the Act came into force (SAICA, 2016). It may take more time before the regulator starts to impose fines, and complete adherence of organizations is enforced, due to some compliance requirement processes which will only commence on a date to be announced by the authority. Earlier this year, the Office of the information regulator approached the president of South Africa requesting that all remaining sectors of POPIA come into force on the 1st of April 2020. As such, organizations will only have a one-year grace period to comply, following the proclamation date.

The manner in which African institutions, specifically South African universities, have embraced and respond to these two information security regulations (GDPR and POPIA) is not yet clear and is very important for biomedical researchers. The core activities of biomedical research are the collection and processing of PII data and information, to perform health-related research, which can be geared towards the diagnosis, prevention and treatment of diseases, the study of disease epidemiology and research into the genetics of disease. To achieve the protection and confidentiality of any associated data and personal information that is captured during a study, effective information security management and practices must be developed and implemented within the university setting.

This research study conducted a qualitative exploratory analysis of information security management across the three universities in South Africa. This pilot study is proposed to make a significant contribution to growing research on the adoption, implementation and management of information security among the above-mentioned universities, by investigating the factors which may influence the effectiveness of information security measures. Moreover, the study will assess whether the participating universities have proper and reliable information security practices and management in place and whether they are in line with international and national standards such as GDPR and POPIA. This study employed the TOE (Technology, Organizational, and Environmental) model as a theoretical model, to investigate the main research questions in this study.

Findings obtained in this study have been used to elucidate the current status, issues, and challenges which face information security practitioners at universities, particularly in the South African context. Furthermore, results assisted with the development of an information security policy for biomedical practitioners, with a view of protecting biomedical data in a more secure way within the university systems.

1.1 Background

It has been postulated by Malin, Emam, & O’Keefe, (2013) that data protection and information security may date back to ancient Greece. The notion of data protection and security was first presented in 1890 and included ideas, views, and perceptions contextualized by individuals (Warren & Brands, 1979; Zhao & Dong, 2017). However, the principles applied in 1890, would no longer apply to current day information security, as privacy content changes with time due to evolution and innovation in technology. To this end, constant adaptation, and new developments and features, need to be implemented in information security policies and procedures. The field of data protection is concerned with protecting assets in general, and information security examines the protection of information in all forms, whether written, spoken, electronic, graphical, or other methods of communication (Caballero, 2013). The universal truth of security, regardless of the application, is that the job of the protector (information security manager and other information security officers) is always complicated by the attacker (Cyber-hackers). A potential hacker needs only to find one weakness, while the protector must try to cover all possible vulnerabilities. The hacker is not restricted by rules and they can follow unusual paths, abuse the trust of the system, or resort to destructive practices to achieve their goal. The protector must try all possible ways to keep their assets (information, data,) intact, and minimize damage while keeping costs to a minimum. A practical illustration of this is homeowners who want to protect their properties, they must attempt to anticipate every attack that is likely to happen, whereas attackers can simply use, bend, break, or mutilate the house’s defenses. Therefore, the homeowners will experience greater difficulty in trying to protect their assets against all types of attacks.

The simple illustration above describes security as a paradigm, a philosophy, and a way of thinking. Defensive failure occurs when blind spots exist and a defender who overlooks a vulnerability risks exploitation of that vulnerability. As such, the best approach to security is to consider every asset in the context of its associated risk, and its value, as well as to consider the relationships among all assets and risks. In the organizational context, each expected loophole must be blocked or protected before achieving the protection of data to acceptable levels. This can be achieved by using a layered, comprehensive approach to mitigate hacking risk, even when one control fails. The field of security is interrelated, and therefore, before security approaches can be effective, a comprehensive protective method must be practiced.

Organizations such as universities are experiencing a wide range of information and data breaches due to one-sided focus by institutions when it comes to the protection of their data,

specifically sensitive data. This failure to realize that in information security, there is no magic bullet, results in an inability to sufficiently secure their assets. For instance, adopting one of the well-known information frameworks will not solve the problem of security policies if those tasked to carry out the implementation do not follow or comply with the framework. Similarly, purchasing a database does not solve the problem of how to manage sensitive data. Therefore, all security controls should complement each other. In essence, every single contributing factor that might influence the effectiveness of information security measures must be considered essential equally.

Limitations of many studies on information security are demonstrated by the fact that most studies focused on technical factors alone, while some focused their attention on organizational factors such as managerial or human factors (Eminağaoğlu, Uçar, & Eren, 2009; Sêmola, 2014; Albuquerque Junior & Santos, 2015a). Some studies have been performed in the technology area of information security measures. It has also been demonstrated that external pressures, such as environmental pressures, may influence the effectiveness of information security practices in organizations especially in academic organizations (Kam *et al.*, 2013; Albuquerque Junior and Santos, 2015b). However, to date, a limited number of studies have been carried out on the above-mentioned factors, with even fewer academic studies that investigate integrated technological, organizational and environmental contexts. A review of literature has shown that studies in this area have not been performed in the South African university sphere. There is an urgent need for improvements in the way data and information are collected, stored and disseminated within university systems and with reference, particularly to sensitive information and data. Prior to determination of the effectiveness of such improvements, security measures and policies must be in place to guarantee the integrity, confidentiality, and availability of the information. To achieve this, technological, organizational and environmental factors must all be investigated without undervaluing any factors.

1.2 Overview of Research Problem Statement

In today's environment, information has become increasingly valuable and can be the lifeline of multiple organizations across the globe. Organizations collect, transmit, and use the information to perform a variety of business-related functions (Glaspie and Karwowski, 2018a). These functions affect all sectors in all aspects, from top management right down to the operational level, in communications, finance, commerce, higher education and government (Singh, 2002). For this reason, no business or organization can afford any loss or

damage to its information resources. Lost or damaged information can result in a loss of time, money and trust in the business sphere and it is therefore imperative to protect and secure information in the business area. This protection of information is called information security (Barnard and Von Solms, 2000).

One of the greatest challenges facing scholarly organizations such as universities, today is how to effectively manage the security of information in their information systems that support teaching, learning and research activities. These organizations (universities) are completely reliant on information technology to carry out day -to -day activities. The wealth of information which is stored at these institutions makes them prime targets for attacks from cybercriminals and it is for this reason that substantial investment has been made in secure information storage, networks and information security systems. However, despite these investments, cyber-crime is still prevalent, with massive breaches being reported almost daily (Glaspie, 2018; Glaspie and Karwowski, 2018b)

Over the past few years, a number of information security incidents have occurred globally, both in public and private universities with many more incidents being unreported. Whenever such incidents occur, it usually involves a loss of confidentiality, integrity, and availability of information, which subsequently has high monetary implications. According to a report by Zecurion (2017), roughly 360,000 individuals had their personal and sensitive data publicly exposed at Auburn University in April 2015. Also, in September 2015, approximately 80,000 students who were enrolled for an online course at California State University had their sensitive information undermined as a result of a cyber hack (Rivera, 2015). The University of Florida was also subjected to a data breach in February 2016, where the personal data of more than 60,000 students were exposed to hackers (Heitsmith, 2016). A similar case occurred in May 2015 at Penn State University, where approximately 18,000 personal and sensitive data records were accessed by unauthorized people (Walter, 2015). The alarming issue in the latter case is that unauthorized access had started as far back as 2012 and had proceeded unnoticed until 2015 (Coleman and Purcell, 2015). Similarly, a breach that occurred at the University of Connecticut in July 2015, showed that the school servers were hacked in 2013, two years prior to being detected (Vectra, 2017; Davis, 2019; Kelsner, 2019). Because of these information breach incidents, universities were ranked among the top three targeted sectors for hackers and data vulnerabilities (Figure 1).



Figure 1: The top ten sectors facing data breached (Symantec's Internet Security Threat Report Between January to December 2014).

Despite the alarming rate of information breaches at universities, many still undervalue the importance of information security. While many claims to recognize information security as a vital function, the actual priority allocated to security is rarely commensurate with its importance. Besides, on multiple occasions, security tools have been put together arbitrarily, without the formulation of effective information security policies and procedures (Jourdan *et al.*, 2010; Rao and Nayak, 2014a). Moreover, there is often in conflict with regards to how the implementation of security practices should occur, and the impact that implementation has on standard work practices (Kessler, 2001; Alotaibi, Furnell and Clarke, 2017).

To date, there has been limited published academic literature, specifically in the areas focused on information security management at South African universities. Concurrently, the profile of security is increasing due to the recognition of its important role in protecting data, especially sensitive and confidential information such as biomedical data. The biomedical data is considered sensitive in nature due to the fact that it may contain information related to human health, such as medical history and genetics information. Furthermore, this data may also contain personal identifiable information which could result in discrimination, stigmatisation and other ethical considerations if not adequately protected (Humer and Finkle 2014).

Many South African universities are coming to terms with establishing effective governance over information security due to the external forces on the institutional environment from data regulatory agencies. Taken together, these issues demonstrate some problems which can be experienced in a university setting and as such, a key focus of this study is to determine the processes which should be followed and improved upon, in the university information security management setting. This will be achieved by investigating factors that may influence the effectiveness of information security measures, specifically as it relates to the securing of, and protecting biomedical data and information.

1.3 The aim of the study

This study aims to conduct a qualitative based exploratory research study across three universities in South Africa by using a Technology, Organizational and Environmental (TOE) framework to investigate the factors which may influence the effectiveness of information security measures among universities. The study also aims to assess whether these universities have proper and reliable information security measures, practices, policies, and management in place and whether they are in line with both national (POPIA) and international regulations (GDPR).

1.4 Research objectives

In order to achieve the primary aim and objective of this study, the study is proposed to answer three research questions, which are;

1. What is the current status of information security management practices at the three universities?
2. What are the major factors which influence the effectiveness of information security management practices? (Identified issues will be classified under, Technology, Organizational and Environmental issues or factors)
3. How could developments or improvements in information security management be attained at these universities?

To investigate how information security is currently being managed in the participating universities, interviews were conducted with the Chief Information Security Officers at each participating university. The interview process aimed to investigate the current status of information security management at the Universities and understand the associated information security management issues and deficiencies faced by IT practitioners at the

institutions. The insight gained from the above was used to identify strategies for improving the future status of information security management, with results expected to assist with the development of a security practitioner's Management Model, with a view of developing a framework for biomedical data.

1.5 Justification

The current study utilized the TOE model which integrates Technological, Organizational and Environmental factors which can influence the effectiveness of information security management and measures in university systems. The importance of this study is demonstrated by gaps in previous studies that have failed to integrate these three themes (Technological, Organizational and Environmental). Additionally, a limited number of studies that have attempted this, made use of theoretical approaches in the organizational context and not the university context.

The area of organizational context such as human factors (Mitnick & Simon, 2003, Hsu, Lee, & Straub, 2012), and administrative measures (Sêmola, 2014) has been investigated in a few studies. However, the mechanism of decision making for implementation and management of information security countermeasure by IT personnel, managers, or those responsible for information security (Chief Information Security Officer) have not been studied, and as such, factual recommendations have not been given in this area (Kreicberga, 2010). Therefore, this study aims to address themes that were not examined in previous studies, using open-ended interview questions, face- to- face conversations and observations. Recommendation policies will be formulated and designed in light of the findings with the aim to improve the present state of information security in the universities, and ultimately, the development of security policies for biomedical data. This research aims to assist in facilitating security management in the South African university sector, by linking theories and findings from the study to an improved process for information security management, specifically in the processing of sensitive data and information such as biomedical data.

However, the current study is the first phase of a larger project. The current study focuses on exploring the factors which can influence the effectiveness of information security management and measures in university systems, by focusing on data held by universities generally. It is assumed that sensitive and confidential data such as biomedical data should be treated with the same core principles. However, biomedical data would require a higher level of protection and security when compared to other kinds of general data in the university's databases. Sensitive biomedical data should additionally be securely stored to

reduce the risk of disclosure or unauthorized access. Ideally, this would also involve a master copy and a single backup, at a separate location. Unfortunately, most universities prioritized data coming from the financial department network over that of the biomedical departments' network because, the financial data usually contains banking details such as credit card digits and pins. However, on the black market, personal health information may be 50 times more valuable than financial information (Humer and Finkle, 2014). Stolen biomedical data or records can fetch upwards of \$60 per record, a value 10-20 times more than that of credit card information.

In the first phase of the project, it may be assumed that if universities are having difficulties in effectively securing both the general and financial information, which they consider to be most sensitive data, then protecting and securing biomedical data may be exponentially more problematic.

1.6 Ethical Measures

This study was approved by the Biomedical Science Research Ethics Committee of the University of the Western Cape with the ethics reference number (BM18/7/11). Respondents recruited for the study were informed and only those who signed consent were permitted to participate. Privacy protection was extended to all respondents and universities involved in this study. The ultimate care was taken to ensure that the personal information of the participants, as well as data provided by participants remained confidential during and after the study. Information was protected from unauthorized disclosure, tampering, or damage, by restricting participant identity and data provided by the participants to the research team, ensuring that identifying details were stored separately and using codes were used to protect participant identities, particularly during transcription of the audio recordings. Furthermore, information collected is only being used for the purpose for which it was collected under the consent of the research participants and in accordance with ethical guidelines.

Furthermore, all interview data collected in this study was classified as sensitive information due to the sensitivity around feeling exposure as a result of failure to implement secure processes at universities as well as the possibility of identifying a participant by their voice. This may result in discrimination towards the participant and as such, the voice biometric data is considered sensitive. In addition, this study employed qualitative techniques which involves unstructured data that may make extraction confidential information prior to transcription and analysis, difficult. Therefore, data coding analyses was employed in order to remove names

and contact details of the respondents and their corresponding universities to ensure that no person can be identified.

1.7 Limitations of the study

This study included participants from three universities in South Africa, and as such only includes academic organizations, which differ from any other common public organizations. It will, therefore, be beyond the scope of this study to generalize the findings to the entire academic landscape in South Africa. Furthermore, the diverse historical development, organizational culture and resourcing of tertiary education institutes in the country prevents a one-size-fits-all approach to implementation of the findings in the study. In addition, the research centered on educational institutions or organizations and as such, it is considered beyond the scope of this study to apply findings to other organizations of a different type and structure.

Moreover, it was impractical to interview all the staff working in the Department of Information and Communication Service (ICS) of each participating university; therefore, selective and representative employees were chosen.

South Africa, despite significant improvements in the area of information security adoption, is a developing country. Therefore, findings from this study may be more applicable to other developing countries, mostly within the African continent. Another limitation is the fact that the study was limited to the effectiveness of information security measures, practices, and management, and as such, the overall information security work process was not subject to investigation in this study.

1.8 Dissertation Structure

This research is divided into six chapters and has two appendices. Chapter 1 introduces the research problem and describes the research objectives, question and delimitations. Chapter 2 contains a review of various literature sources on information security, information security management systems, information security policies, awareness and training, and information legislation. The chapter also highlights and compares some of the well-recognised information security frameworks as one of the countermeasures used to reduce information security threats in an organization such as university. Lastly, the chapter also presents a reviewed debate on universities and some of their challenges concerning information security. Chapter 3 explains in detailed the complete description of the methodology used in this study. This includes the research design and method, the sampling plan, data collection techniques and

the method of data analysis. Chapter 4 highlights and discusses the key findings or results of the study and how they answered the research questions of this particular study. Chapter 5 addresses the communication gaps issues revealed from the results of this study to be existing between the decision-makers (such as the board members of the universities), the CISOs (such as IT security teams, cybersecurity teams) and the users (such as students, teaching and non-teaching staffs, academicians). And finally, Chapter 6 concludes the research by summarizing the key findings, discusses the limitation of the study and future directives. Following a detailed bibliography of references used in this study, the proposed policy, as well as the peer-reviewed publication can be found in the appendix and supplementary data sections respectively.

Chapter Two

Literature Review

2 Introduction

The literature review chapter is recognized as one of the indispensable sections in any academic study. It connects previous studies by various scholars on a particular area, to the present (Graham, 2011; Taylor, 2012). Webster (2002) emphasized that a useful literature review should also identify significant biases and knowledge gaps in the literature of a particular field, to allow for identification of corresponding future research directions (Rowe, 2014). This chapter of the study aims to provide the background knowledge and a broad understanding of the previous works in the world of information security, specifically, in the aspect of information security management, policies, and compliance. In addition, this chapter aims to incorporate the study into an extensive outline of imperative hypothesis and justify the need for the research.

2.1 Information

The term 'information' has had multiple definitions by authors in different fields, both within and outside the information concept or domain. For instance, according to Mikkelinen (2015), the author defined information as something of fact, that does not have to be the truth, nor does it have to be relevant to anything. The author elaborated on this by providing a scenario of an individual claiming that they are in pain. Of course, this is a piece of information, however, we cannot deduce if the person is lying or telling the truth (Israel and Perry, 1991; Mikkelinen, 2015). Hamid (2011), defined information as something that characterizes human beings and describes the era in which they live and the societies they inhabit. Given the ubiquity of the vast collection of information technology (IT) at our disposal to create, communicate, interpret and exploit information, humans currently, and undoubtedly, exist in a digital age (Robert 2014; Pyati, 2007; Richardson, 2007; Hamid, 2011; Lyon, 2013). This era has ushered in a new range of emerging technologies and computer-mediated activities that have revolutionized the way humans think, live, communicate and interact with each other (Fairhurst and Stephanidis, 1988; Spinuzzi, 1997; Mesthene, 2014).

As a result of this, information has become an essential element in our daily lives. Organizations collect data on what individuals search, buy, and react to surroundings or specific settings, and harness this data to invent products (He, Zha and Li, 2013). Data is used

as a roadmap to improve services and products offered to consumers – and as such, information has become critical for business operations, with organizations progressively increasing storage, use and distribution of data. This makes information a high value commodity and an essential strategic asset (IFIP, 2004). In addition, information has expanded from scarce resource to superabundant one (Bieker *et al.*, 2017). The excess of information does however pose several threats to humans and society as a whole. The threats include, but not limited to, the exponential growth of information technology, with its enhanced capacity for surveillance, communication, computation, storage and retrieval (Warwick, 2018). Mason (2016), summarised these threats as PAPA, meaning P (Privacy), A (Accuracy), P (Property), and A (Accessibility). In the table below, four major issues of concern in the information age are highlighted and to address these issues, information must be protected at an appropriate level (ISO/IEC, 2016); this protection is called information security.

The author expanded on each of these, and concerning questions which have been raised, is shown in the table below;

Table 1: Privacy concerns raised in the information age (Mason 2016)

Threat	Concern questions raised
P- (Privacy)	What information should one be required to share about one's self to others? Under what condition? What information can people keep to themselves and not be forced to reveal to others?
A- (Accuracy)	Who is responsible for the authenticity, fidelity, and accuracy of information? Who is to be held accountable for errors in information, and how is the injured party to be made whole?
P- (Property)	Who owns the information? What are the just and fair prices for its exchange? Who owns the channels through which information is transmitted?
A- (Accessibility)	What information does a person or an organization have a right or a privilege to obtain, under what conditions, and with what safeguards?

2.1.1 Information security

According to ISO/IEC 17799 information security is defined as “the preservation of Confidentiality, Integrity, and Availability” of information (CIA) (ISO/IEC 17799, 2000, cited in Braman 2002). Confidentiality is the preservation of the secrecy of information by ensuring

that it is accessible only to authorized individuals (Nggondi, 2009; Whitman and Mattord, 2012). Integrity ensures information is accurate, consistent, and has not been manipulated during the application of processing methods (Gelbstein, 2011; Caballero, 2013). Availability ensures that authorized users have access to information and associated assets when needed (Solms, Solms and Caelli, 1993; Braman, 2002; ISO, 2005). This definition, which is also referred to as “the CIA definition,” is the most cited definition because of its simplicity in (Braman, 2002) describing information security as a way to preventing unauthorised access (confidentiality) or alteration (integrity) of information while preserving access (availability).

However, CIA has received some criticism from scholars, writers and theorists, stating that the definition is too general and shallow. It defines insecure states as secure and secure states as insecure (Lundgren and Möller, 2017). Braman (2002) claimed that the CIA definition was a near verbatim copy of the definition of ‘computer security’, proposed when the computer was first introduced (Mainframe computers). In that time period, governments and businesses were responsible for the protection of data and information by ensuring the physical security of the mainframe from hazards such as theft and fire. However, in today’s environment, the internet and portable mobile computing technologies such as laptops and smartphones is commonplace, and has brought about ease of access to data, information manipulation and distribution from within, and outside of, the organization premises. As such the application of earlier principles will likely no longer apply to current information security practices. Confidentiality, integrity and availability of content changes with time due to the evolution and innovation in various technologies (Lundgren and Möller, 2017). Braman (2002), added that the CIA definition does not acknowledge the employee related aspects of information security. In response, Dhillon and Backhouse (2002), proposed a version of the definition which added responsibility, the integrity of organizational members, trust, and ethical norms and behaviour as principles of information security (Dhillon and Backhouse, 2000). Donn Parker added three more properties to the CIA, to develop the Parkerian hexad for information security, presented in table 2 below (Andress and Winterfeld, 2014a; Pender-Bey, 2016).

Table 2: Parkerian’s definition of information security

Parkerian description, also known as “The Parkerian hexad.”					
Confidentiality	Availability	Integrity	Control	Authenticity	Utility

Several other definitions also exist, apart from the CIA version and Parkerian version. A list of various definitions found in textbooks, articles and white papers is presented in table 3. Many attempts had been made by experts in the IT field, and related disciplines to appropriately define information security (Zafar and Clark, 2009). However, no universally accepted definition, or standardized critical success factor taxonomy currently exists (Firesmith, 2003; Torres *et al.*, 2006; Cherdantseva and Hilton, 2015; Lundgren and Möller, 2017). Zafar and Clark (2009), further state information security consists of such broad scope that it cannot be defined in one sentence and as a result, terms such as data protection, IT security, computer security and cybersecurity are used interchangeably to refer to information security (Figure 2), indirectly resulting in a lack of appreciation for the value of information security (Dimitriadis, 2011). Information security is, therefore, a polymorphous, multi-dimensional field aimed at the legitimate control of access to, and use of, any stored data.

Table 3: Definitions of Information security from literature

Author(s)	Definition
(Braman, 2002)	Defined information security as the practice of protecting organizational information of value from both intentional and unintentional acts that adversely affect its safety and providing reasonable assurance of this protection via adequate controls and accountability
(James & Inovant, 2002).	A 'well-informed sense of assurance that the information risks and controls are in balance.'
(NSTISSC, 2000)	"Protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats."
(Whitman & Mattord, 2003)	"... is the protection of information and the systems and hardware that use, store, and transmit that information."
US Government, Legal Information Institute	Defined information security as "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction,"

ISO/IEC 27001 (2005, 2013)	“... as the protection of information from a wide range of threats to ensure business continuity, minimize business risk, and maximize return on investment (ROI) and business opportunities.”
(Cherdantseva and Hilton, 2013)	“... as a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security countermeasures of all available types (technical, Organizational, human-oriented and legal) to keep information in all its locations (within and outside the organization's perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destructed, free from threats.”

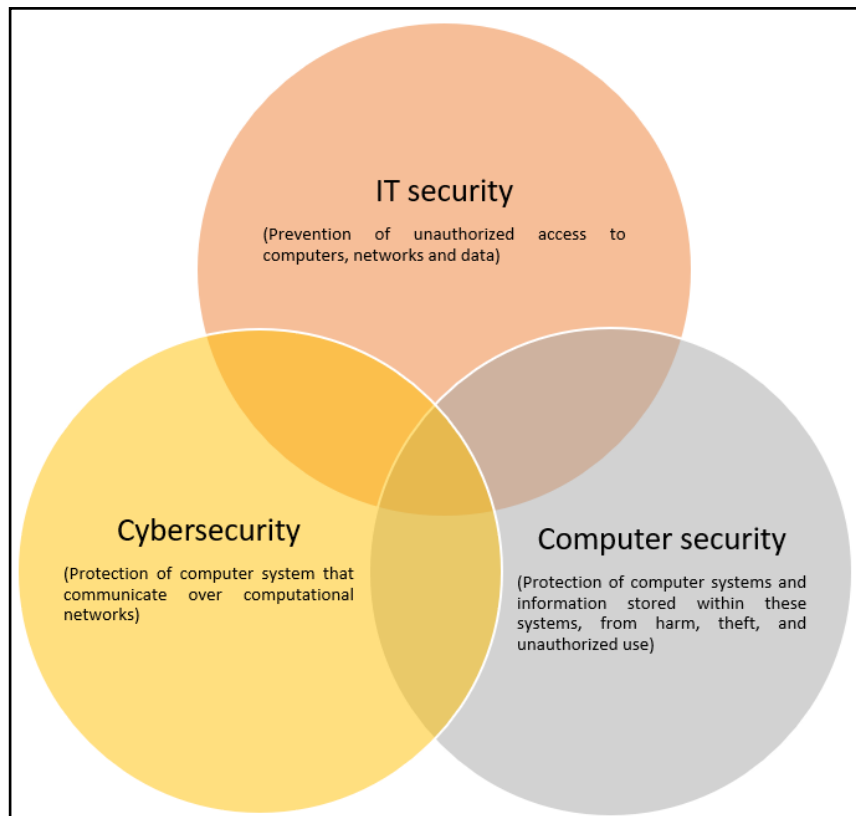


Figure 2: Diagram demonstrating the polymorphous nature of information security and terms which are used interchangeably to define it (Crawley, 2017)

Although the view of information security varies dependant on it application in a study (Dimitriadis, 2011), the ultimate goal of information security is to protect information assets

(including computer and non-computer equipment and facilities) and data, from all threats and risks, and in so doing, increase institutional business continuity, reduce organization losses, and increase the return on investment (Kruger, Drevin and Steyn, 2010). For this study, information security, as defined by the Parkerian hexad (Figure 2), conceptualized by Donn Parker has been adopted. In summary, it defines information security as;

1. The preservation of information attributes or properties which are; confidentiality, integrity, availability, authenticity, utility, and possession.
2. It is the protection of these attributes mentioned above from destruction and interference with the use, modification and replacement, misrepresentation and repudiation, misuse and failure to use, disclosure, and observation, copying and stealing, and endangerment.
3. It is ensuring that the functions to accomplish (2) are; avoidance, deterrence, prevention, detection, mitigation, transference, sanction, recovery, and correction.
4. It is also ensuring that the efforts to achieve condition (3) are to be guided by meeting the standard of due care and identification of real vulnerabilities and threats.
5. Lastly, it is by proper application protection, which is often accomplished by installing and effectively using renowned security controls and practices, and by using a set of control principles as guides.

2.1.2 A Historical View to Information Security

In the information security world, Botha and Gaadingwe, (2006), claimed that the future of information security could be realized if past and current situations are well understood. The sections below highlight the evolution of information security over the past few decades.

2.1.2.1 How information security came into existence

Dlamini, Eloff, and Eloff (2009), argued that information security came into existence even before the invention of the computer, while, Lebtinen, (2006a), ascertained that the notion of information security is as old as information itself. Due to the industrial revolution, there was an enormous use of paper but during World War 1, massive amounts of documents were destroyed, resulting in the need for a new medium to store and protect information. 1930 has been recognized as the first point in altering the mode of storing information from physical to digital methods. To make data more secure, the first-ever Information security System called “Enigma” was developed by a German engineer Arthur Scherbius, which used the techniques

of encryption and decryption as a measure of security for protecting the secret messages (Bar Ilan, 2008). In 1932, the first computer was invented by Konrad Zuse. It was an electro mechanical computer, bulky in size, and used difficult programming languages, and was mainly used for scientific calculations, census, accounting, payroll and inventory problems (Albert, 2015). Following this, there was massive development in the field of computing and in 1942 the first electronic digital computer was invented with computing functionality and parallel processing (Whitman and Mattord, 2012).

In 1946 ENIAC I was developed, mainly for American military research. The most critical security issue during this era was ensuring that only a privileged computer operator would have access to the system, and that the physical computer was not stolen or damaged by outsiders (Suganthy and Maiti, 2014). Prior to 1948, machines used vacuum tubes, but after 1948, transistors were introduced, and by the end of 1960 (Clements, 2006), integrated circuits were invented and at this point, security of information became a more pertinent concern. Physical safekeeping was the fundamental principle underlying all security of computer systems during this era and transferring programs or data between computers was via human messengers or physical mail. The only threat related to this method of transmission was that stored media could be lost or stolen and although it would take days to get information to its destination, data was generally considered to be safe. Nevertheless, this raised a challenging question: “How can one send information from one place to another, faster?” and in 1960, the concept of computer networking was borne (Bar Ilan, 2008; Dlamini, Eloff and Eloff, 2009b; Suganthy and Maiti, 2014). The same year (1960), during the Cold War, Larry Roberts (the founder of the Internet) examined the feasibility of maintaining the secrecy of the United States military’s data and on 3rd June 1968, he delivered the ARPANET Program Plan. Computer networking, the predecessor to the internet, enabled users (multiple users – one computer) access to remote data. However, a new risk to remotely held data was introduced, whereby both authorized and unauthorised individuals could gain access to data. Physical security alone could not deal with this unique risk and as such user identification and authorization came into play in the early 1970s (Whitman and Mattord, 2012).

The introduction of mini computers marked the beginning of networks, time-sharing and multi-user systems which changed the rules of the game (Paul *et al.*, 2019). The number of people with computer know-how increased with a subsequent decrease in the cost of modems and terminals. Access controls were introduced to prevent users from interfering with another workspace. The work of Harrison, Ruzzo and Ullman (the HRU model) pioneered access controls and was followed by the Bell-LaPadula confidentiality model for Multics (Rue, Pfleeger

and Ortiz, 2007), and digital signatures from around the late 1970s to the early 1980s. Over-and-above confidentiality, concern over data integrity was highlighted and public-key cryptography came into existence. The Data Encryption Standard (DES) was adopted by the National Bureau of Standard (NBS) [now called the National Institute of Standards and Technology] of the USA with DES innovations introducing new dimensions for the protection of information. In addition, the US government passed the Privacy Act of 1974 with the view to safeguard personal data recorded in government systems (Rusell and Gangemi, 1991; Lebtinen 2006).

The late 1970s and early 1980s marked the introduction of personal computers (Rusell and Gangemi, 1991), increased access to the technology subsequently resulted in a higher number of people with computer know-how. With companies beginning to automate operations and storage of critical data on easily accessible devices, new security threats emerged, and the scope of information security widened. In 1979 the first worm created by Robert Morris was discovered, which corrupted files and computers (FindingDulcinea, 2011) and in 1982, the first virus attacking the Apple DOS operating system was found. This was followed by the first PC virus threat to information security in 1986 (Rahul, 2013). In response, the USA government issued the Computer Fraud and Abuse Act of 1984 to prosecute and establish harsh penalties for creators and authors of computer viruses (Russell and Gangemi, 1991; Denning, 1991, 1999). This was followed by the Computer Security Act of 1987, which dealt with training of security personnel involved in the processing of sensitive information.

The late 1980s saw the introduction of anti-virus software (Marshall and Wesley, 2016) and by the end of 1990, there were approximately nineteen antivirus software environments, including Symantec's Norton Anti-Virus, VirusScan by McAfee, and IBM's Anti-Virus (Carey 2008). This prompted attackers to change from using worms and viruses, to more sophisticated methods in an effort to breach data security. The introduction of distributed denial of service and malicious code attached to business emails and web pages shifted the focus to gateways, resulting in the introduction of filtering firewalls (Suganthi and Maiti, 2014).

The 21st century saw IT infrastructure became universal, and in almost all industries (known as the era of ubiquitous computing) everything became electronic, and cyber hacking attacks were no longer a demonstration of skill, but rather a means for financial gain (Mohapatra, 2000; Dabbagh and Bannan-Ritland, 2005; Laudon and Traver, 2016). Evolution in computing devices (Personal Digital Assistants, Smartphones, Laptops, Tablet PCs, etc.) coupled to emergence of mobile computing (Bluetooth and Wi-Fi) introduced new developments in online

payment systems and web-based applications, all of which were vulnerable to cyber-crime risks and opened new doors for the hacking community (Dhillon and Backhouse, 2000; Lee, 2002). As a result, and in addition to the authorization and authentication credentials, verification of users became an access requirement, banks introduced the 'chip-and-pin', and non-repudiation has since become a critical issue.

Two things remain certain – IT infrastructures is vulnerable and motivated attackers are always ready to exploit these vulnerabilities. It is therefore critical that information and infrastructure is secured. This requires innovative ideas and insightful analysis of security issues in order to appropriately respond to the challenges posed by new developments, and existing well-known threats.

2.1.3 Information Security Management System

According to Jones et al. (2010), organizations and their information systems have been exposed to both internal (threats from employees in the organization who have access to sensitive organization's information) and external (threats from hackers who are always finding a loophole to get access to organization's data) threats. As a result, headline reports continue to expose companies impacted by hackers which have exploited information vulnerabilities. To minimize these threats, organizations are advised to implement an Information Security Management System (ISMS) - a systematic and structured approach to managing information so that it remains secure (Dhillon and Backhouse, 2000). Terroza (2015) described ISMS as a combination of interrelated/interacting information security elements within an organization, to ensure that policies, procedures, and objectives are created, implemented, communicated, and evaluated to better guarantee overall information security. In essence, the primary aims of ISMS in any organization is to; a) identify threats to information resources of the organization, b) define the risk associated with identified threats, c) define the information security policy and d) implement controls to mitigate the risks (Sulaiman *et al.*, 2016). To achieve the above aims, several information security management frameworks and standards exist, which organizations may adopt as guidelines or best practices to develop and implement an effective ISMS in their organization. Terroza (2015) advised that the adoption of an ISMS framework should be directly influenced by factors such as the organization's objectives, the security requirements of the organization, size and structure of the organization, and existing processes employed in the organization. However, despite the numerous ISMS frameworks that organizations can adapt and adopt to minimize threats associated with information security vulnerabilities, many organizations and institutions still struggle with the concepts (Ashenden, 2008). This is evident by the increased number of

breaches experienced by organizations, which is growing at an exponential rate. Ashenden (2008) concludes that the issue is not with the frameworks, but that the difficulties are in the implementation phase in the workplace. Curphey (cited in (Jagruti, 2008; Watuthu, Kimwele and Okeyo, 2015) argued that the reason organizations still experience cyber-vulnerabilities is that, components of ISMS frameworks are being practiced in isolation. The following sections will explain well-known ISMS frameworks, their strengths, and weaknesses, and the dangers of not adopting them.

2.1.4 Information Security Management System (ISMS) Frameworks

The ISMS frameworks are basically 'blueprints' for building information security practices to manage risk and reduce vulnerabilities in an organization. Talabis and Martin (2012), described ISMS frameworks as a logical structure to organize information activities within an organization. They are a series of documented processes that can be used to define policies and procedures for implementation and on-going management of information security controls in an enterprise environment.

However, Al-Dhahri, Al-Sarti, and Abdul (2017) argued that the frameworks are failing to address implementation details and rather focus on foundational concepts associated with risk elements, high-level activities, formulas, and decision matrices. It is vital to note that the implementation of these frameworks by an organization or institution does not universally guarantee that such an institution or organization is not going to be hacked. The frameworks are guiding principles that outline necessary precautions to protect information from unauthorized access and provide a structure for making risk decision, achieving compliance, and being conscious of security problems (ISO, 2013).

As such, organisations must be mindful of the dangers of blindly following frameworks without considering how they apply to a given situation. In view of this, authors have advised that there are essential considerations which organizations should put in place before integrating any information security framework (Gray, 2010; Goosen and Rudman, 2013a). These include but not limited to; developed operational environments that foster cooperation and collaboration across all the departments, IT and security areas, active information security systems, installed advanced technologies in operational areas and, compliance with regulatory requirements (Goosen and Rudman, 2013b; Al-Dhahri, Al-Sarti and Abdul, 2017). Winkler (2011), suggested that a comprehensive and practical ISMS framework implementation must be able to connect three essential components: people, technology, and process.

2.1.4.1 COBIT (Control Objectives for Information and Related Technologies)

COBIT is a good-practice framework for information and related technologies developed by the International Professional Association, ISACA (Information Systems Audit and Control Association) for IT (information technology) management and IT governance (Morimoto, 2009; De Haes, Van Grembergen and Debreceeny, 2013). The framework provides an implementable "set of controls over information technology and organizes them around a logical structure of IT-related processes and enablers".

ISACA released the first version of COBIT in 1996, mainly as a set of control objectives to assist the financial audit community in IT-related environments. Shortly after the first version was released, it was observed that this framework could be of value to others outside of the audit community, and version 2 was released in 1998. Version 3 was released in 2000 with additional functions such as management guidelines and Version 4, released in 2007, addressed issues related to business processes and responsibilities in value creation and risk management.

Several drivers contributed to the updating of version 4 to COBIT 5 (released in early 2012), such as the need for a more coherent understanding of how standards, best practices, and other tools relate and supplement each other, the requirement for greater end-to-end organization scope that covers all business and IT functions, and need for improved guidance relating to emerging technologies (De Haes, Van Grembergen and Debreceeny, 2013)

Consequently, COBIT 5 is a comprehensive framework that assists organizations in achieving objectives for the governance and management of IT by maintaining a balance between realizing benefits, optimizing risk levels, and resource use (Juan José, Eugenio and Antonio, 2013). Moreover, implementation of COBIT 5 for information security in an organization guides IT and security professionals to understand, utilize, implement and direct important information security-related activities, and make reasonable decisions while maintaining awareness about emerging technologies and the accompanying threats (Nicho and Fakhry, 2013). Some of the benefits organizations can obtain by leveraging COBIT 5 for information security are highlighted below.

2.1.4.1.1 Strengths of the COBIT framework and its benefits

The advantages of the COBIT framework are its substantial linkage towards business objectives in conjunction with the IT framework of the organization, which includes application, data, infrastructure, and individuals (Juan José, Eugenio and Antonio, 2013). COBIT also has a heavy focus towards an organization's goals and what needs to be accomplished in order

to achieve them and includes daily business operations, and information security (De Haes *et al.*, 2019). Moreover, COBIT creates a persistent information governance environment that assures business-aligned IT solutions and ensures the goals of an organization are at the forefront of all employees (Feltus, Petit and Dubois, 2009). Other strengths and benefits of COBIT include;

1. Reduced complexity and increased cost-effectiveness due to improved, easier integration of information security standards, ethical practices and sector-specific guidelines
2. Ability to partially implement this framework without requiring a full-spectrum analysis and commitment by the organization
3. Increased user satisfaction with information security arrangements and outcomes
4. Improved integration of information security in the enterprise
5. Informed risk decision and awareness
6. Improved prevention, detection, and recovery
7. Supports innovation and competitiveness
8. Improved management of costs related to the information security function
9. Provides a better understanding of information security (Isaca, 2012).

2.1.4.1.2 Weaknesses and disadvantages of the COBIT framework

COBIT framework lacks focus on how to achieve the necessary goals recommended by the context (Rouyet, Ruiz, 2008). As a result, the endeavour of implementing the framework is left to the management team. In addition, Chen, Research (2010) argued that the framework might be difficult to implement due to the necessity for all stakeholders to be involved in the creation and management of the framework and as such, the framework tends to be more ideal for smaller organisations. Other weaknesses of the COBIT framework include;

1. The high cost of this framework due to the knowledge and skill required for implementation to provide support to information technology governance or in assessing the performance of a company's information technology has resulted in many organizations avoiding its use in their activities (intellectsoft, 2017).
2. While the wide scope can be viewed as a strength for COBIT, it can also be a deleterious during implementation. The design is not limited to a specific area, and this can lead to gaps in coverage (Merhout and Joseph, 2015).
3. The framework has all the descriptions in terms of processes, activities, and responsibilities, but it lacks the specification of its connections (Moller, 2010).

4. The framework provides a shallow analysis of the given situation and as such it requires a very experienced analyst to conduct credible maturity assessments (Merhout and Joseph, 2015).
5. There is no evidence or assurance that the experienced analysts would get the required solution regarding the maturity of an organization's information technology (intellectsoft, 2017).

2.1.4.2 NIST Framework

The National Institute of Standards and Technology (NIST) is a standards organization that is sponsored by the US Federal Government (NIST, 2015). It regularly publishes guidelines and standards related to a variety of information security topics, from cryptography to incident response processes. NIST outlines a series of activities related to assessing and managing organizational risk and is adopted not only by federal agencies but also by local governments. Organisations which are under federal regulations, such as FISMA or HIPAA, typically refer to this framework to conduct risk assessments and operate risk management programs (NIST, 2015).

Ruth Horaczko, a practice leader of the risk assessment and IT advisory consulting firm, postulated that the NIST framework is not only invaluable in assessing risks but also in managing those risks (Violino, 2010). The framework was designed to help individual businesses and other organizations to carry out information security management in a cost-effective way. Furthermore, she elaborated on the flexibility within the framework, designed to take into consideration the full range of organizations that would adopt this standard. The framework is known to comprise of a compilation of risk-based guidelines that can assist organizations in identifying, implementing, and improving information security practices. The framework creates a common language for internal and external communication of cyber-security issues (Violino, 2010).

The NIST framework comprises three main components: Profile, Implementation Tiers, and Core.

1. The **profile** component enables organizations to align and improve information security practices based on individual business needs, tolerance for risk, and available resources.
2. **Implementation Tiers** help to create a context that enables organizations to understand how their current information security risk-management capabilities stack up against the characteristics described by the Framework.

3. The **framework core** defines the standardized information security activities, desired outcomes, and applicable references, and is organized by five continuous functions: Identify, Protect, Detect, Respond, and Recover.

2.1.4.2.1 Strength of NIST Framework

1. The framework provides an assessment mechanism that enables organizations to determine their current information security capabilities, sets individual goals for a target state, and establish a plan for improving and maintaining information security programs (Stoneburner, Goguen and Alexis, 2006).
2. The framework is open-ended and provides substantial flexibility to the assessor making it ideal for use in highly diverse environments (Mell and Grance, 2011)
3. The framework has a good discussion regarding the concept of threat and vulnerability pairs. The risk mitigation section is very detailed and may be useful for risk management implementations (Violino, 2010).

2.1.4.2.2 Weaknesses of the NIST framework.

1. The framework is not as objective and data-driven as other frameworks (Beckers and Beckers, 2015).
2. There is a lack of criteria and decision guides. For instance, some of the matrices provided in the standard are highly subjective (Violino, 2010). When results become heavily dependent on the experience and opinions of the individual executing the assessment, it may become open to interpretation and challenge.
3. The framework threat sources are primarily geared for government and military scenarios (M. Talabis and Martin, 2012a)
4. NIST framework terminology uses acronyms throughout and supporting tools are not collated (M. Talabis and Martin, 2012a).

2.1.4.3 FAIR framework

FAIR (Factor Analysis of Information Risk) is a risk analysis framework that codifies factors which contribute to risk and how these factors ultimately affect each other. FAIR establishes accurate probabilities for the frequency and magnitude of risk and can be utilised by organizations to translate the impact of cyber risk and allow for prioritizing risk treatments (Kim, 2019). Fox (2009), further described FAIR as a risk assessment model that can objectively quantify the economic consequence of information risk (Fox, 2009). The model has four main components which are- Threats, Assets, Organization and External

environment and the details of these components are summarised in the article by Nair, 2019.

According to the developers of the FAIR framework, the shortcomings of current risk assessment practices are primarily the result of information security being practiced as an “art” rather than a science (M. Talabis and Martin, 2012a). Violino (2010) commented that while the FAIR framework has many complex terms and formulas, it is straightforward, and the documentation provides the criteria, charts, and explanations to understand the framework.

2.1.4.3.1 Strengths of the FAIR framework.

1. The framework is very objective making it defensible and repeatable (M. Talabis and Martin, 2012a).
2. The framework is useful and suitable for organizations that have strong metrics.

2.1.4.3.2 Weaknesses of the FAIR framework.

1. This framework can initially appear to be overwhelming because of the terminologies and matrices involved (M. Talabis and Martin, 2012a).
2. Some criteria may be difficult to interpret in a real scenario (Beckers and Beckers, 2015).
3. The framework might be challenging for organizations with immature programs (M. Talabis and Martin, 2012a).
4. It might be difficult for inexperienced assessors due to lack of knowledge in specific areas such as threat frequencies (Pandey 2012)
5. The framework may be challenging to articulate in cross-disciplinary groups (Violino, 2010).

2.1.4.4 ISO 27000 Series

The ISO 27000 series was developed by the International Standards Organization (ISO) (Disterer, 2013) and provides a comprehensive information security framework that can be applied to any type and size of organizations. The ISO 27000 series allows the organization to manage the security of assets such as financial information, intellectual property, employee details or information by third parties and is divided into different sub-standards based on the content, making ISO very comprehensive. For instance, ISO 27000 consists of an overview and vocabulary, while ISO 27002, which was evolved from the British standard BS7799, defines the operational steps necessary in an information security program. ISO 27799 defines

information security in healthcare, which could be useful for those companies requiring HIPAA compliance, and ISO 27001 defines the Information Security Management System (ISMS).

ISO 27001 (formally known as *ISO/IEC 27001:2005*) is the most well-known standard in the ISO 27000 series, providing requirements for information security management (ISMS), providing a framework of policies and procedures that includes all legal, physical, and technical controls involved in an organization's information risk management processes (Disterer, 2013).

According to the documentation, the framework was developed to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an information security management system and defines 14 discretionary planning processes, listed below:

1. Information security policies.
2. Organization of information security.
3. Human resources security.
4. Asset management.
5. Access control.
6. Cryptography
7. Physical and environment security
8. Operations security
9. Communication Security
10. System acquisition, development, and maintenance
11. Supplier relationships
12. Information Security Incident Management
13. Information security aspects of business continuity
14. Compliance

2.1.4.4.1 Strengths of ISO 27000 series including ISO 27001 framework

1. ISO frameworks are recognized worldwide in terms of standards, quality, business continuity and planning, and as such the framework is well researched (Kairab, 2004).
2. ISO is more specific and more precise when compared to most other information security frameworks (Talabis and Martin 2012).
3. The framework provides information and examples of a threat catalog, vulnerabilities, and various computation and plotting techniques for rating risk (Kairab, 2004).
4. The framework is very flexible and focuses on objectives, which provides flexibility to organizations in terms of how the standard is implemented (Talabis and Martin 2012).
5. ISO 27001 management system is a continuous improvement cycle (Plan, Do Check, Act), allowing an organization to improve their security practices (Pandey 2012).

2.1.4.4.2 Weaknesses of ISO 27001 framework

1. The framework is very open to interpretation because it is not prescriptive. There is a higher risk that different organizations and different assessors would conduct an activity differently. Moreover, stakeholders and auditors might also have a different interpretation of the standards (Fomin, Vries and Barlette, 2008).
2. Some of the requirements in the framework are unclear (Gikas, 2010).
3. The framework lacks a data classification policy, which has an effect on defining levels of encryption for different data types (Talabis and Martin 2012a).
4. Also, ISO implementation and maintaining accreditation is very expensive. For instance, it usually involves internal and external audits every year plus a 3-year cycle of accreditation (Verry, 2012).

2.1.4.5 Comparison between the Frameworks

ISMS framework is a broad document that covers different areas of the vast information security domain and while a detailed discussion each of these reviewed frameworks is outside of the scope of this thesis, this section attempts to summarize each framework into universal themes, and compares them to identify the gaps between the reviewed frameworks. A comparative study performed by Susanto et al. (2011) benchmarked each section in the ISO 27000 against different information security standards: BS7799, PCI-DSS, ITIL, and COBIT. The result of the study demonstrated that ISO 27000, COBIT and PCI-DSS covered all focus areas while having one or two deficiencies. The authors claimed that ISO 27000s was the most widely accepted information security standard next to standards as COBIT, PCIDSS, BS

7799, and ITIL (Susanto et al., 2011). Table 4 below shows the comparison of the reviewed information security framework in this chapter.

Table 4: Comparison of ISMS frameworks. Tick marks represent commonality while the closed points indicate focus areas not included in a particular framework (adapted from Susanto et al., 2011)

Focus Area	COBIT 5	NIST	FAIR	ISO 27001
Information Security Policy	✓	✓	✓	✓
Communications and Operations Management	✓	✓	✓	✓
Access Control	✓	✓	✓	✓
Information Systems Acquisition, Development and Management	✓	✓	✓	✓
Organization of Information Security	✓	✓	✓	✓
Asset Management	✓	✓	•	✓
Information Security Incident Management	✓	✓	•	✓
Business Continuity Management	✓	•	✓	✓
Human Resource Security	✓	✓	✓	✓
Physical and Environmental Security	✓	✓	✓	✓
Compliance	✓	✓	✓	✓

2.1.5 Conclusion on Information Security Management System

The information provided above on selected ISMS frameworks does not seek to undervalue any framework but rather to assist in understanding these frameworks in order to guide decision-makers. It is essential that an organization first understand their environment prior to adopting and implementing any information security framework, as a particular framework may be more applicable than another, based on the existing level of implementation and the availability of essential resources. Adequate information security is required for major organisational functions such as, supporting the organization’s continuity, supporting the safe operation of applications running on the organization’s IT systems, protecting the data and information which the organization uses in running day-to-day functions and protecting the organization’s technology assets.

It is important to note that there is no single security framework or control that can provide absolute and complete protection of an organization’s information and data. The most

reasonable means for preventing data breaches involves 'common sense' security practices (Silowash *et al.*, 2012), which includes understanding of security basics (Lebtinen, 2006b; Andress and Winterfeld, 2014b), conducting vulnerability and penetration testing on a consistent basis (Shah and Mehtre, 2015; Baloch, 2017), applying proven malware protection, using strong passwords (Dell'Amico, Michiardi and Roudier, 2010; Bindu, 2015), and using necessary software patches on all systems (Meyer and Lambert, 2007) (these measures are also recommended in all the reviewed frameworks).

2.2 Security Policy

Security policy is supported in the literature as being extremely important and fundamental to information security (Mutongi and Marume, 2016). Yet policy is an area that faces several challenges, including a lack of understanding about what security policy is and how it is best used (Hina and Dominic, 2018). An organizational security policy is described by Olson, Abrams and Bailey (2001) as the "set of laws, rules and practices that regulate how an organization manages, protects and distributes resources to achieve specified security policy objectives. To be meaningful these laws, rules and practices must provide individuals (with a) reasonable ability to determine whether their actions violate or comply with the policy".

Security policy, therefore, plays a strategic role in defining high-level organizational direction, as well as being specific to users with regards to the practical operations. One of the main goals of an information security policy, according to Hina and Dominic (2018), is to define the rights and responsibilities of information resource users.

2.2.1 Policy as a Foundation to Security Management

Alnatheer (2015), suggests that an information security policy is a prerequisite to security management. Similarly, Mutongi and Marume (2016), claimed that an information security policy is the foundation to proper administration of information for nations and organizations. There is a high degree of consensus overall that effective information security management is significantly correlated to, and dependent on the existence, and practical application of a security policy (Hassan, Wan and Widyarto, 2016; ECAR, 2003; Lowry *et al.* 2015). The evidence in literature demonstrates a growing acknowledgment and emphasis on information security within organizations (Furnell and Clarke, 2005; Bulgurcu, Cavusoglu and Benbasat, 2010; Lowry *et al.*, 2015) and a subsequent associated increase in the uptake of security implementation measures, including development and deployment of security policies.

Studies on security policy within universities, specifically in the South African context are rare. However, studies of other large organizations have indicated several gaps that may apply to

universities. A survey by Fulford and Doherty (2003) investigated the application of information security policies in large UK-based organizations. The authors sent nearly 3000 questionnaires to senior ranking IT professionals and received 208 responses. The research specifically examined security policy in terms of dissemination, information coverage, and factors affecting the success of the policy. While results indicated a high rate of policy existence (76%), it was noted that most organizations relied only on a single mode of dissemination. The authors suggested that this single mode of dissemination had the potential to result in a lower level of compliance because the information in the policies would not reach all people concerned (Fulford and Doherty, 2003).

The research by Fulford and Doherty (2003) noted that a general lack of academic research had been conducted into the adoption of specific areas of security policy, or the impact thereof. Some of the studies on information security-related matters within higher education sector include a study by Hina and Dominic (2017) which investigated the need for information security compliance within university settings, analysis of contributing factors on information security management in higher education institutions by Sari, Nurshabrina, and Candiwan (2016) and a study by Kumar, Joshi, and Gaud (2016) which measured the security dangers in the university network. All the above-mentioned studies do not however, report on the organizational impact of policy.

2.2.1.1 Development Issues with Information Security Policy

There exists very little research in areas of policy development, policy effectiveness and factors used to determine policy success (Yu, Peng and Leng, 2010). Research on security policy tends to be normative and does not indicate what is happening in organizations (Ruighaver, Maynard and Chia, 2002; Alshaikh *et al.*, 2015; Veiga and Eloff, 2019). One development process proposed by Ismail *et al.* (2017) suggests that policy formulation should focus on examining assets which require security, prototyping documents, and finally, drafting of policy. Guidelines recommended by Thomas, (2016) uses a 'policy', 'procedures,' and 'standards' methodology to develop guidelines for effective information security management. However, neither of these two authors provide information on how policy should be structured.

Work by Dhillon (2001) suggests a model for policies by classification as 'individual' (as described as being specific to individual technologies), 'modular' (fairly broad but grouping technologies) and 'comprehensive' (principles-based and applying to all techniques, processes and people). Furthermore, the author raises a critical issue by stating that governance over systems through security policy is a significant part of security but is often

neglected. Whether policies in organizations are becoming more frequent or not, the literature indicates that success in the development, implementation, and compliance with policies is still greatly lacking.

2.2.1.2 Implementation Issues with Information Security Policy

Security policy not only plays an essential function in communicating the vision and stance of the organization on information security, it also guides end-users within the organisation. The actual implementation of security policies can, however, be complicated (Baskerville and Siponen, 2002; Höne and Eloff, 2002). Reasons for this may include weak dissemination and communication of the policy to users (Straub, Goodman and Baskerville, 2008). The policy may be too long or technical, and the relationship between the security policy and users' responsibilities is often not understood, or, seen as needing a 'workaround' due to the perception that it is obstructive (Bayuk *et al.*, 2012). An underlying assumption in information security is that users will refer to policies during their daily work.

Thus, Information security should be provided as a service to enable the organization's priorities. While the importance of policy cannot be denied, ineffective or incorrect application of policy is likely to dilute the process of information security and may result in information security being seen as unnecessary, unhelpful, and even obstructive (Mutongi and Marume, 2016). Implementation of practical and effective security policy should not only show the required responsibilities of users but should also reflect the objectives of the organization so that end-users understand the relevance to daily functions and tasks (Höne and Eloff, 2002) (Eminağaoğlu, Uçar and Eren, 2009). In a similar note, policy needs to be linked to an associated high-level management commitment, which, when combined with user awareness, gives an appropriate organizational context for the implementation of, and compliance with, information security (Landoll, 2016; Williams, 2016)

The overall responsibility for security policy development often falls to the technical administrators or information security officers, who may have insufficient authority or knowledge of the organization's higher objectives (Karyda, 2008). Moreover, the information security officers are often forced to manage critical priorities that compete for their time and resources. They must simultaneously stay on top of cyber incidence while maintaining open access and additionally meet an array of regulatory and compliance requirements (Vectra, 2017). This is due to information security being perceived as 'IT Security', and thus an IT problem, instead of 'Information Security', which is rather an organizational or business issue (Karyda, 2008; Tang, Li and Zhang, 2016; Cram, Proudfoot and D'Arcy, 2017). Policy

developed under these circumstances tends to lack ownership and stakeholder collaboration and can result in essential objectives not being appropriately considered (Vahti, 2009). Even reviews of policy by senior management can be conducted without a strong sense of ownership by the managers themselves if they are dissatisfied with the content or process, or if they do not see it as part of their responsibility (EDUCAUSE, 2018). This situation can result in a policy being developed by people not necessarily aware of, or understanding, high-level objectives. However, these people are required to engage with individuals within the organization to ultimately implement an effective policy, making a difficult task even more arduous and ineffective (Lee, Lee and Kim, 2016).

The actual writing, implementation and compliance with a policy are major areas requiring careful consideration and further research for effective security management. Therefore, with respect to information policy, this research study focuses on which areas are being covered in university policies, especially in relation to biomedical departments, since they are among departments that collect, process, and share the most sensitive data and information in the university. Moreover, the study also examines the methods utilised for awareness of, and compliance with, the contents of the policy.

2.2.2 Conclusion on Security Policy

The scantiness of research on security policy (aside from content-focused research) has been noted in investigations into the application of information security policies in large organizations (Fulford and Doherty, 2003; Hasbini, Eldabi and Aldallal, 2018). Nonetheless, several common themes have emerged with security policy. Firstly, although the prevalence of instances of security policy appears to be increasing in this information age, a lack of a consistent approaches to policy development and requirements, is apparent.

Additionally, a lack of consistency in uptake and dissemination methods is apparent. The absorption of policy in terms of gaining excellent support from management and attaining compliance at all levels is another major problem. The gaps in academic research which this thesis aims to investigate includes universities' policies with consequences for biomedical departments and researchers. This study further proposes operational information security for the departments, or groups of researchers within the university setting.

2.3 Awareness of Information Security

Information security awareness is a state brought about primarily through initiatives and activities by the organization, and aimed at ensuring that both management and end-users are aware of, and committed to, policies and guidelines as well as security risk mitigation

(AlHogail, 2016; Hanus and Wu, 2016). Bulgurcu, Cavusoglu and Benbasat (2017) argue that information security awareness is considered necessary because information security techniques or procedures concerning information systems can be misused, inadvertently incorrectly applied or not used at all, rendering security guidelines as less useful and practical (Thomson and Von Solms, 1998; Bulgurcu, Cavusoglu and Benbasat, 2017; Hina and Dominic, 2018).

However, solving information security issues through awareness activities has some challenges. One such problem is that awareness of the requirements for behaviour is essential (AlHogail, 2016). Secondly, the set of factors that influence with the user's willingness to comply needs to be understood (Kreicberga, 2010). Another aspect of awareness is that its effectiveness depends on the interest of the person receiving it (Safa *et al.*, 2015) (Bada, Sasse and Nurse, 2019). Awareness activities are not particularly useful when done in the absence of an actual interest in information security and as such, steps taken towards improving security awareness should be influenced by the receiver's predisposition towards information security (Cohen, 1999; Safa, Solms and Fletcher, 2016). In order to address these challenges, a security culture must be developed through an effective security strategy that targets all necessary levels within the organization. At a university for instance, this requires focusing on students or end-users, staff and general management, academics, senior management and executive, as well as the council.

Successful information security in organizations such as a university depends on having everyone in the organization motivated to be compliant with information security. Understanding how to encourage people requires understanding their current knowledge of the area. With respect to information security awareness, the focus of this study is to identify the activities that are being undertaken for awareness development within the participant institutions. And to determine at what levels these are being conducted. Moreover, issues that exist with this process are examined and recommendations for improving awareness within the university community are provided.

2.3.1 Conclusions on Security Awareness

The literature reviewed in this chapter illustrates that information security awareness is considered an essential mechanism for improving information security management. However, focus and prioritization on awareness activities tends to be ignored and underfunded, despite the demonstrated links between increased awareness and increased compliance (Karyda, 2008; Rahim *et al.*, 2015)

In undertaking awareness as an activity, it is worth examining the human element in the design and application of any strategy. Understanding the underlying human motivation is likely to increase the chances that the application of an awareness program may lead to improved compliance. This human motivation can vary significantly in universities due to the variety of situations that exist. It is therefore important to examine effective, and non-effective strategies being employed in the university setting in order to identifying the problems and develop possible solutions. Understanding the influencing factors of successful approaches is highly valuable in developing and implementing an awareness program.

2.3.2 Compliance with Security

A theme relating to awareness involves the concept of imparting a 'culture of compliance' towards information security within an organisation (Furnell et al., 2000). An organization with a 'culture of compliance' has a level of compliance that is not only demonstrated from 'the top,' but includes norms for security guidelines and practices that are invariably practiced and respected by all in the organization (Yazdanmehr and Wang, 2016; Page, 2017). Research by Gartner and AMR (Haldar and Forsyth, 2004) concludes that many enterprises remain inadequately protected from security threats because of the perceived high cost of an effective security strategy that suits the organization's culture. The lack of focus on security strategy has led to an emphasis on products and technologies instead of a security strategy that incorporates awareness, training, and policy and standards to develop a 'culture of compliance' towards information security.

A sufficient commitment to security requires that a process is in place that suits the culture of the organization (Spurling, 1995; Leach 2003). Forsey (2018), defined organization culture as a system of shared assumptions, values, and beliefs, which governs how people behave in organizations. Hero, (2020) further explain the seven major characteristics of organizational culture which are: innovation and risk taking, outcome orientation, stability, aggressiveness, team orientation, people orientation and attention detail. Exploring these characteristics in an organization will allow a better understanding of how of an organization operates, their strength area and weaknesses even in the context of security and compliance.

However, in an organization such as an education sector, understanding the factors that add to compliance within the university environment is multifaceted. As, universities contain a mix of corporate culture and traditional academic freedoms. It is not uncommon for information security to be seen by individuals or groups within the university environment as disabling

rather than enabling. Usually, the negative attitudes of users toward information security should decrease as awareness increases, but this is not always the case.

According to Dickie (1996), security tends to be a transparent process when operating efficiently, and it is often unnoticed when things are running smoothly. Because information security tends to be intangible, a general lack of awareness and understanding can quickly develop. This can result in a lack of ownership and responsibility, and the perception that information security is not essential, leading to the question 'why should any attention be paid to information security?'

Dickie (1996) further asserts that information security is a management responsibility and forms one of the internal control systems which are monitored and reviewed by an audit. It must be noted however, that information security compliance is not simply a matter of applying controls and procedures. The potential conflicts between various stakeholders within universities preclude such a straightforward approach. There exists tension between those who want to provide open access to information, those who want to protect information, and those who require privacy of information yet expect information to be shared. Additionally, when the work practices of the organization are threatened, unless there is an understanding of the clear and present requirement for change, resistance will follow. The balance between transparency and confidentiality of information continues to be a challenge requiring a comprehensive organization-specific approach. An effective security program or strategy that introduces changes in a managed way, while taking into account the conflict between security requirements and working practices, is necessary (Gaunt, 2000).

Other factors that can reduce the potential for developing a culture of compliance include a lack of information security process in human resource recruitment and training, disregard of the importance of information security education and training, ignorance and poor user attitude, conflicting demands of users, inadequacy of systems, and inconsistently applied policies and procedures (Gaunt, 2000).

In the Educause book, 'Computer Network Security in Higher Education', Luker and Petersen (2003) discuss the principals of academic freedom with strategies which can be employed by universities for successful information security awareness and compliance. Luker and Petersen (2003) suggest that achieving an acceptable security strategy can often result in conflict and problems in achieving a balance between information security and the survival of academic freedom or ingrained work practices. Developing a culture of compliance is recognised as a major challenge in the higher education sector and it is therefore necessary

to carefully balance work practices with security control in order to make any progress toward the necessary culture of compliance.

2.4 Data and information legislation

The aim of data and information legislation is to fulfil two main objectives. Firstly, it provides a legal framework through which the integrity and privacy of personal information in systems can be assured and protected, and secondly, to enable the country or region which has such legislation in place, to preserve an appropriate trading status in transactions involving data (Liu *et al.*, 2015). A nation enforcing such legislation would be reluctant to transfer personal data to any other country which does not have data and information laws in place. There is a perception that countries under such circumstances will become 'data deserts', since no self-respecting data processing nation would send information or 'data havens' to a country where illicit processing could be undertaken (Dalacoura, 2010). Central to the data and information protection legislation was the specification of eight guiding principles governing activity involving personal information in computers (IFIP, 2004). The guiding principle states that personal data and information be;

1. Obtained fairly and lawfully
2. Held only for one or more lawful purposes declared by the data user
3. Used or disclosed only following the data user's declaration
4. Adequate, relevant and not excessive for the stated purposes
5. Accurate and where necessary up to date
6. Not kept longer than necessary for the declared purposes
7. Made available to those about whom data related (data subjects) on request
8. Adequately protected, through appropriate security, against loss or disclosure

2.4.1 Some of the international and national information security laws and regulations required by South African Universities.

2.4.1.1 Common law:

This law was developed through decisions of courts rather than through statutes. Prior to the enactment of the Electronic Communications and Transactions Act (2002) in South Africa, common law regulated crimes of defamation, indecency (online child pornography), crimen injuria (also known as cyber-smearing), fraud (cyber fraud), defeating the ends of justice, contempt of court (in the form of publishing any court proceedings without the courts permission online or by other electronic means), and forgery to these cyber offenses (Dalacoura, 2010). As stipulated in common law, a director owes two duties to the company:

A fiduciary duty and a duty of skill and care. A fiduciary is a person who is in a particular position of trust and they must act in good faith, exercise powers for a proper purpose, avoid conflicts of interest, and should not misuse the organization's property (Lionel, 2018).

Further, a duty of skill and care requires that this person should possess reasonable skills and should devote his full attention to the business of the organization. This duty of care includes responsibility for mitigating risks and protection of the organization's information assets. Gregory (2011) states that "it is becoming increasingly evident that a court of law may go behind the 'corporate personality' of the company and find individuals, particularly members of management, who can be held accountable for the breaches in information security policy" (Gregory, 2011). Indeed, following the judgment in the case "Minister of Safety & Security v Van Duivenboden [2002] 3 All SA 741", a university may be held liable for the damages caused to its students or staff if a person in a responsible position would have foreseen the risk and not have acted to prevent that risk.

2.4.1.2 FICA

The Financial Intelligence Centre Act (FICA), came into effect on 1 July 2003. FICA was introduced to fight financial crime, such as money laundering, tax evasion, and terrorist financing activities (De Koker, 2004). This Act brings South Africa in line with similar legislation in other countries designed to reveal the movement of money derived from unlawful activities, thereby curbing money laundering and other criminal activities. The Act stipulates that the accountable institution, may not conclude a business transaction with a client, nor establish an ongoing business relationship with a client, without having complied with information gathering and reporting duties imposed by FICA (FIC, 2019). These obligations include Proof of identity, proof of residential address, and proof of banking account.

However, since Universities are also increasingly involved in e-business and e-commerce (e.g., with suppliers through e-procurement), they need to abide by the requirements of FICA.

2.4.1.3 King III

King III is a comprehensive international corporate governance regulation that addresses the financial, social, ethical and environmental practices of organizations. The regulation identified several characteristics of good Corporate Governance i.e. discipline, transparency, independence, accountability, responsibility, fairness and social responsibility. It addresses the accountability and responsibilities of boards of directors and the processes of auditing and accounting (IDSA, 2019). According to the section 4.16 of the Act, the board is required to

operate with IT governance in mind and IT should be on the board's agenda. IT performance should be measured and reported to the board, the board should set a management framework for IT governance based on common approach such as COBIT and audit committees should oversee IT risks and controls. In addition to this, chapter one of the Act deals with ethical leadership and corporate citizenship (IDSA, 2019). Price Waterhouse Coopers (2009) indicated that the King III code states that companies must be responsible corporate citizens. This implies an ethical relationship of responsibility between a company and the society in which it operates. Price Waterhouse Coopers (2009) further indicated that companies, apart from rights, also have legal and moral obligations. The company should protect, enhance, and invest in the well-being of the economy, society and the natural environment (Institute of Directors, 2009).

2.4.1.4 Promotion of Access to Information (PAIA)

This Act was passed to comply with the obligations contained in section 9 (4) and section 32 (2) of the South African Constitution (Varney, 2017). Section 32(1)(a) of the constitution of 1996 states that "everyone has the right of access to any information held by the state or any of its organs" (Arko-Cobbah, 2008). In terms of Sections 14 and 51 of the PAIA, public and private bodies are required to compile documentation that details the subjects and categories of information held by that public/private body and requires that these bodies have a PAIA manual that details procedures that should be adopted in requesting access to the records.

In the university setting, records held include, but are not limited to, records of individual students; human resources records (individual staff members, staff recruitment, and other staff-related policies); research records (undertaken by staff and students); financial records (budgets, financial statements, assets register, procurement policies). The Higher Education Act (Act 101 of 1997) as amended also states in Chapter 7 (section 56(1)), that any person may inspect the register of Higher Education, and auditors' reports. All these emphasize again the need that universities must ensure that information kept in their networks and databases must be compiled accurately and stored safely, and while some exemptions apply in certain circumstances, it is prudent to work on the assumption that all records are accessible (Varney, 2017).

2.4.1.5 The Healthcare Information Portability and Accountability Act (HIPAA)

This Act signed into US law in 1996, mandates healthcare information flow, maintenance and protection (Atchinson and Fox, 1997; HIPAA Guide, 2018). HIPAA generally requires that an organization or institution have (1) a written policy procedures that describe, among other things,

who has access to protected information, how such information will be used, and when the information may be disclosed; (2) require their business associates to protect the privacy of health information; (3) train employees in the privacy policies and procedures; (4) take steps to protect against unauthorized disclosure of personal health records; and (5) designate an individual to be responsible for ensuring the procedures are followed ('Health Insurance Reform Act of 1995). Educational institutions are obligated to comply with HIPAA (Cheng and Hung, 2006).

2.4.1.6 European Union - General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is regarded as the most significant change to the European data protection laws, in over 20 years (Lexology, 2018). It was approved by European Union (EU) in April 2016 and became enforceable in May 2018, following the two years of a post-adoption grace period (Staunton, Slokenberga and Mascalconi, 2019). The EU-GDPR is the latest step in the ongoing global recognition of the value and importance of personal information. Although the information economy has existed for some time, the real value of personal data has only become evident more recently (Perdana, 2018). Cyber theft of personal data exposes residents in the EU to significant risks. Big data analysis techniques enable organizations to track and predict individual behaviour and can be deployed in automated decision-making. The combination of all these issues, together with the continuing advancement of technology and concerns about the misuse of personal data by governments and corporations, resulted in the GDPR law (Pham, 2019). This legislation was passed by the EU to clarify the data rights of data subjects and to ensure an appropriate level of EU-wide protection for personal data and also addressed the transfer of personal data outside of the European Economic Area, and the European Union. The law applies across all the member states of the EU, but its reach is far more extensive, and any organization (including universities) anywhere in the world that provides services to the EU which involves processing personal data will have to comply (Dinu, 2018; Denley, Foulsham and Hitchen, 2019). This implies that any organization, whether a private or public, and which collects, stores, or shares identifying data originating in the EU, or transfers this personal data to third-party countries or international organizations, will need to comply with the GDPR regardless of their location. Non-compliance may result in substantial fines up to 20 Million Euros or 4% of worldwide annual turnover of the prior fiscal year. The GDPR is perceived as the most significant data security law in the world, which builds on the work of the EU's Data Protection Directive (DPD), the HIPAA regulation of the USA and various other data protection regimes. The GDPR can

be regarded as a refined and comprehensive update of the EU's goals in protecting the rights and freedoms of data subjects.

2.4.1.7 Protection of Personal Information Act (POPIA).

In terms of data protection, the European Union's (EU) data protection laws have been regarded as a current global gold standard (The EU's independent data protection Authority, 2018). South Africa is one of only 28 countries in the world with cyber security policy in place, however, it remains one of the countries that is lagging in terms of information security (PayU, 2014). Due to this, its cybersecurity policy faced heavy criticisms (SAPS, 2011; Dlamini & Modise, 2012; Ahmore Burger-Smidt, 2018). In 2014, it was reported that South Africa lost approximately R50-billion to cybercrime and was ranked as the most 'cybercrime targeted' country on the Africa continent. Song (2017) claimed that the threat would become more widespread going forward, as the number of South African Internet users' increases. In response to this growing threat, a regulation known as POPIA (The protection of Personal Information Act) was designed to decrease the occurrence of vulnerabilities in the country. POPIA's legislation is similar to the EU's Data Protection Act and it has been designed to protect any personal information which is processed by private and public organizations (including universities). POPIA's goal is to guarantee that all South African institutions conduct themselves in an ethical and legal manner when it comes to collecting, managing, storing and dispensing Personally Identifiable Information (PII) (SAICA, 2016). It was marked into law in November 2013, and in April 2014 certain segments of the Act came into force. These include sections dealing with the establishment of the Information Regulator, the procedure for establishing regulations, and the nature of the rules that the Information Regulator may make, amongst other things (Scharnick, Gerber and Futcher, 2016). The primary aim of the Act is to protect the privacy rights determined by section 14 of the Constitution of the Republic of South Africa (Act, No. 108 of 1996). POPIA was introduced to establish minimum requirements for the processing of personal information; to provide for the establishment of an information regulator to exercise specific power and to perform particular duties and function in terms of POPIA and PAIA, to provide for the issuing of codes of conduct, to provide for the right of persons regarding unsolicited electronic communications and automated decision making, and to regulate the flow of information across the borders of South Africa (Tiffin, George and Lefevre, 2019). According to Muhlberg (2019), the POPIA will impact universities because they collect, store, process, and disseminate personal information related to university communities and external stakeholders as part of their business activities (Muhlberg, 2019). Early in 2020, the office of the information regulator approached the President of South Africa

requesting that the final sections of the Act commence on the 1st April 2020, meaning that compliance will be mandatory, following a year grace-period, on the 31st March, 2021 (POPI, 2013; SAICA, 2016)

Having briefly discussed some of the information security regulations that are required by South African universities to comply with, the focus of this current study is on the last two regulations discussed, the GDPR and POPIA, and specifically in relation to the sections that relate to protection of sensitive information such as health information.

2.4.2 Information Security in Universities and some of the challenges

As seen with other organizations in society, universities are increasingly acknowledging the importance of information security to protect business and research information. This acknowledgment is underpinned by the recognition of information as an invaluable asset and strategic resource which understandably requires appropriate protection. Having effective information security control mechanisms in place to ensure the availability, confidentiality and integrity of information is therefore critical to the process of security management (Fulford and Doherty, 2003).

While a simple concept, the practical implementation of activities associated with information security processes in universities is not necessarily straightforward. According to Vectra (2017), the author claimed that education campuses are like mini-cities, with many students living on the campus, a variety of vendors providing services, and large numbers of visitors. This environment gives cyber-intruders numerous mechanisms to successfully infiltrate higher education networks. Recent analyses regarding data incidents at institutions revealed that higher education accounted for roughly 1.35 million identities exposed in a year alone (CREATe, 2016). Another analysis by Barker (2015), claimed that higher education is breached at an occurrence of one per week, with more than 500 security instances having been recorded since 2005. This analysis was corroborated by Judy (2016) who estimates that a higher education institution are breached every week.

The function of security management in universities tends to operate with corporate mandates associated with the business of providing education on one side and the culture and pedagogical pursuit of academic, learning, and research on the other side (Sporn, 1996a; Joshi and Singh, 2017). Information security becomes somewhat of an art form in this environment, requiring steering through the various complexities of university culture and challenges (Vectra, 2017).

2.4.2.1 University Culture as an issue

Universities represent a complex environment of culture and technologies. On the cultural side, universities are complex organizations with unique culture and different features (Smart and St. John, 1996; Sporn, 1996a; Flowers *et al.*, 2015; Kaufman, 2016) described by Mintzberg (1982, cited in Sporn, 1996b) as 'expertocracies'. Cohen and March (1974, cited in Sporn, 1996b) viewed it as organized anarchies, while (Weick, 1976) characterized universities as loosely coupled systems due to complexities and distinctive culture. Baldrige *et al.* (1977) explained that unlike profit-making organizations, universities have specific characteristics that need to be understood, and these characteristics control the culture of academic institutions (Baldrige *et al.*, 1977). The authors elaborated that the universities' goals are ambivalent, unclear and non-routine with problematic standards for goal attainment. Unlike the other collective manufacturing organizations, it is easy to define segmented and routinized procedures, but when most people are involved- as in universities - it is hard to develop one adequate standard for delivering (Sporn, 1996a; Kyobe, 2010). The different objectives and standards in teaching, research, and service, as well as lack of agreement on guidelines for goal achievement, results in an ambiguous decision-making process (Flowers *et al.*, 2015). Universities are to a large extent, "people-oriented" institutions. Different constituencies need to be recognized in order for universities to fulfil their functions. The professionals (i.e., the lecturers) working at universities tend to be experts with a strong wish for autonomy and freedom. This makes it difficult to establish a coordinated initiative for governing and managing the university. The decision-making processes at universities are often complicated and extended due to the involvement, and different interests, of academic and administrative staff. Universities are vulnerable to their environment and changes in political, economic, social demand, governmental regulations, and technological conditions can significantly affect these institutions.

2.4.2.2 Changes in Environmental Settings as an issue

Aside from the internal issues which constitute the university culture, universities also face dynamic changes in their external environment. For instance, in many developing countries such as South Africa, universities are struggling with different forms of environmental changes such as social demands and government demands. These have direct or indirect effects on universities either by an increased demand for education that leads to mass education or by a decreased supply of necessary resources leading to financial constraints, or both (Sawyer, 2004). As a result of these financial constraints, universities have less to spend on infrastructure projects, expanding their facilities, appointing additional competent staff, and

spending on technologies to protect information on networks and databases (Sawyer, 2004; Teferra and Altbach, 2004; Bakari *et al.*, 2005; Ayyagari and Tyks, 2012; Teferra, 2013)

2.4.2.3 Technology complexity and open network access as an issue

Universities are reliant on information to support their core activities and business operations (Cascio and Montealegre, 2016). There is a dependence on activities associated with creating, using and sharing information for core teaching, learning and research functions (Baldwin, 2019). As a result of this, universities operate in dynamics, complex and diverse information systems (Lupu *et al.*, 2008). Different stakeholders use these systems with varying requirements and the complexities and challenges that exist involve changing and different technologies, openness to the internet, explorative student research bases, and business goals and objectives that are not always understood or accepted by all stakeholders. Open access to the internet coupled with 'bringing your own device' policies (academic freedom), results in a high number of connected users and devices on the networks (Khanna, 2013; Crossler *et al.*, 2014) In addition, decentralization of information technology services within faculties, and stringent security rules, controls and requirements increases security risk (Lupu *et al.*, 2008; Vectra, 2017)

2.4.3 Summary and conclusion of the Literature Review

This literature review chapter has explored four critical areas of information security, with a view to highlight and understand some existing issues within information security management in universities. The first part presented an analysis of Information Security and information security Management Systems (ISMS) as an active management approach. The second section explored the importance of policy, while highlighting issues related to content, development and implementation. The third part defined security awareness and its importance and discussed the concept of creating a culture of compliance to information security. The final section of this chapter centred on data and information regulations. Here, some of the essential information regulations that concerned South African universities were briefly discussed. From the review above, it can be established that although the need for information security has been acknowledged and deemed necessary, in many cases, information security is not prioritized in line with its importance (Netshakhuma, 2019). This is reflected by a lack of commitment, inadequate funding and a general lack of understanding by top management due to several factors (EDUCAUSE, 2018), including a lack of awareness of information security issues (Netshakhuma, 2019), a lack of adequate security management governance (Hagen, Albrechtsen and Hovden, 2008), and a generally reactive approach

based on perceived impacts on users regarding their work practices. Additionally, the fact that top management has not incorporated information security as part of corporate governance impedes prioritization of resources towards information security. This, in turn, affects how much effort is put towards raising awareness and ensuring compliance, leading to less acknowledgment of the value of information security overall (Netshakhuma, 2019).

Chapter Three

Research Methodology and Motivation

3 Introduction

This chapter provides a description of the research methodology, beginning with an overview of the research design followed by a detailed description of the methods used for the data collection and data analysis.

3.1 The standard for scientific empirical research methodology

The research method performed in this study is based on the method proposed by (Jacobsen, 2000), which is also aligned with Janesick's (2000) concepts, where the writer divided Jacobsen's (2000) different phases into three stages. The table below gives an overview of the methodology stages been used.

Table 5: Showing a methodology standard of an empirical research study

Stage (Janesick)	Phase (Jacobsen)	Done in this study
A. Research Design	Phase 1 - Develop research criteria	<ul style="list-style-type: none">• Identification and formulation of the research problem.• Extensive literature survey to develop the research topic
	Phase 2 – Choose a research method	<ul style="list-style-type: none">• Choosing the most appropriate research methodology
	Phase 3 – Choose a strategy	<ul style="list-style-type: none">• Identified and developed an appropriate research strategy for the study• An exploratory case study found suitable for the study.
B. Data Collection	Phase 4 – Select Sample	<ul style="list-style-type: none">• Sampling Plan• Identified appropriate institutions for the case studies approach

	Phase 5 – How to collect data	<ul style="list-style-type: none"> • Conduct the interviews with the appropriate participant • Observation through participant
C. Data Analysis	Phase 6 – Analyse Data	<ul style="list-style-type: none"> • Process and record data • Analyse data • Data reduction • Identified meaningful patterns and themes • Data display
	Phase 7 – Interpret results and conclusion	<ul style="list-style-type: none"> • Conclusion and Verification • Coding software used • Ethical Considerations

3.2 Stage A- Research Design

Research design can simply be described as a plan that contains the outline for the gathering, computation, and examination of data. Yin (2003), described a research design as the logical plan to interrelate the research question to gather data prior to interpreting data and drawing conclusions. Research design clearly states what type of data is required in a study, what methods would be used in collecting and analysing such data and how these methods work in answering the research question(s) attached to the study. The following sub-sections highlights some of the major steps employed in this empirical research study.

3.2.1 Phase 1

3.2.1.1 Identification and formulation of the research problem

The first step in this study was to identify and determine the research problem. At the initial stages of this study, information security management and practices amongst the South African higher education institutions were carefully considered and the following items were identified as a motivation for the current study;

1. Ineffective information security management and practices amongst the South African institutions should be analysed to determine if an intervention is required
2. Information security policies within the higher institution may need to be improved upon

3. To date, there has been limited published academic literature, specifically in the area that focuses on information security management in South African universities. This demonstrates a gap in knowledge

3.2.1.2 Extensive Literature survey to develop the research topic

According to Jacobsen (2000), development of a research topic refers to a process of reviewing the literature to have broader and deeper knowledge about the broad subject matter, identify research gaps in the domain, and make a possible topic to study based on the research domain (Jacobsen, 2000).

To develop an appropriate research topic for this study, suggestions, guidelines, and frameworks that centred on the development of the research topic was presented in chapter 2 and covered topics in the area of technology, organization, and environmental influencing the management, practices, and compliances of information security.

3.2.2 Phase 2

Choosing the most appropriate research method

According to Mühl, (2014) and ; Kumar Ranjit, (2019), there are two main types of research methods in empirical studies- quantitative and qualitative methods. As suggested by Pardede, (2018) both methods have merit, but they differ in their essential characteristics, hence it is essential for the researcher to know both pros and cons of each method and decide which one is more suitable to use for the research problem identified in phase 1.

3.2.2.1 Qualitative Method

Qualitative research is a research method that usually accentuates words rather than quantification in the collection and analysis of data (Bryman 2008a: 366 cited in (Hammersley, 2013). Sandelowski (2004), defined qualitative research as an umbrella term for a collection of attitudes and strategies for conducting an inquiry that is aimed at discovering; how human beings understand, experience, interpret and produce in the social world. Qualitative research relies on the views of the participants; asks wide broad questions, gathers data that mostly words or text from respondents, labels these words in themes; and conducts the analysis in an exceedingly subjective prejudiced manner (Creswell, 2012).

Qualitative methods are more flexible – that is, they allow greater spontaneity and adaptation of the interaction between the researcher and the study participant(s) (Pardede, 2018). Qualitative methods ask mostly “open-ended” questions that are not necessarily worded in exactly the same way with each participant (Pope, 2000).

As such, this exploratory research study employed the merits of qualitative methods in order to understand participant's thoughts, opinions, and perceptions about the topic at hand. This study used a series of open-ended questions to provide participants with the opportunity to respond in their own words, rather than requiring the respondents to choose from fixed responses, as quantitative methods do. The semi-structured interviews coupled to the use of open-ended questions also permitted more elaborate responses which provided greater detail.

3.2.3 Phase 3 Choose a strategy

The next stage in this study was to choose a strategy for data collection based on the qualitative research method. According to Vyas (2015), there are four major strategies under qualitative research methods that are commonly used. They are:

1. Phenomenology
2. Ethnography
3. Ground theory
4. Case study.

A detailed description or discussion of these four approaches are beyond the scope of this study, however, the case study strategy which was used in this study is briefly discussed below

3.2.3.1 Case study

According to Avison and Pries-Heje (2005), Thomas (2017), Ben-basat *et al.*, (1987), and Yin (2003), case study originates in the social sciences, particularly in the fieldwork of anthropology and sociology. Today it is being widely used in almost all the academic disciplines e.g. education (Stake, 1978), political science (Gerring, 2004), business (Eisenhardt and Graebner, 2007), operation management (McCutcheon and Meredith, 1993), marketing (Easton, 2010a), information systems (Benbasat, Goldstein and Mead, 1987), information technology (Tellis, 1997; Cooper, 2000) and information security (Khalfan, 2004; Chen, Shaw and Yang, 2006). Case studies in general “examine a phenomenon in its natural setting, employing multiple methods of data collection to gather information from one or a few entities” (Benbasat, Goldstein and Mead, 1987; Yin, 2003). The use of the case study as a type of qualitative method is well presented by much of the existing literature as an appropriate research method for answering ‘how’ or ‘why’ questions (Yin, 2003). The approach is known with its strength to facilitate an understanding of complex real-life situations, by studying the situation in context. Case studies provide an opportunity for the researcher to gain a deep holistic view of the research problem and may facilitate describing, understanding and explaining a research problem or situation (Tellis, 1997; Baxter and Jack, 2008).

Since the aim of this study is to have an in-depth understanding of the influential factors under Technology, Organization and Environment that may be disrupting the effective implementation of information security within an institutional setting, the case study strategy is the most appropriate method. Additional factors which support the decision to utilise this strategy include; aims of the study, the nature of the problem statement, the research questions, and time-frame for the study.

3.2.3.1.1 Determining the Type of Case Study to Use

Yin (2003) categorizes case studies as explanatory, exploratory and descriptive and Stake, (1995) outlines intrinsic, instrumental, and multiple-case study categories. Despite the use of different terms and approaches to describe the various types of case studies that exist, Baxter & Jack (2008), claimed that all target the same goals - to ensure that the topic of interest is well investigated, explored and revealed (Baxter & Jack 2008). The table below presents the descriptions of each, and includes some published examples of these types of case studies.

Table 6: Types of case study

Type of case study	Description
Explanatory	An explanatory case study is suitable in a study that seeks or aims to answer a question that required to explain the presumed causal links in the real-life interventions that are too complex for the survey or experimental strategies (Yin, 2003). This implies that a case study with a person or group would not be explanatory, as, with humans, there will always be variables. There are always small variances that cannot be explained (Baxter, Susan Jack and Jack, 2008).
Exploratory	An exploratory case study is usually the precursor to a formal, large-scale research project. The case study's goal is to prove that further investigation is necessary. In other words, this type of case study is used to explore those situations in which the phenomenon being evaluated has no clear, single set of outcomes (Yin, 2003).
Descriptive	This type of case study is used to describe an intervention or phenomenon and the real-life context in which it occurred (Yin, 2003).

Intrinsic	<p>An intrinsic case study is the study of a case wherein the subject itself is the primary interest (Baxter, Susan Jack, and Jack, 2008). Stake (1995) uses the term intrinsic and suggests that researchers who have a genuine interest in the case should use this approach when the intent is to better understand the case. It is not undertaken primarily because the case represents other cases or because it illustrates a particular trait or problem, but because in all its particularity and ordinariness, the case itself is of interest.</p> <p>The purpose is NOT to come to understand some abstract construct or generic phenomenon. The purpose is NOT to build theory (Baxter, Susan Jack, and Jack, 2008)</p>
Instrumental	<p>An instrumental case study uses a case to gain insights into a phenomenon. In other words, this type of case study is used to accomplish something other than understanding a particular situation. It provides insight into an issue or helps to refine theory. The case is of secondary interest; it plays a supportive role, facilitating our understanding of something else. The case is often looked at in-depth, its contexts scrutinized, its ordinary activities detailed, and because it helps the researcher pursue the external interest. The case may or may not be seen as typical of other cases (Stake, 1995).</p>
Multiple-case studies	<p>A multiple case study enables the researcher to explore differences within and between cases. The goal is to replicate findings across cases. Because comparisons will be drawn, it is imperative that the cases are chosen carefully so that the researcher can predict similar results across cases, or predict contrasting results based on a theory (Yin, 2003).</p>

The current study was conducted by interviewing the three consenting participants (one at each institution) within the designated IT domain to investigate and understand relationships between technological, organizational and environmental factors, and the subsequent impact

on effectiveness and implementation of information security practices and compliances. Moreover, the study also aimed to assess whether any of these institutions had proper and reliable information security measures, practices, policies, and management in place. Furthermore, the study investigated if information security practices were in line with both national and international standard such as POPIA and GDPR, respectively.

The current research study can therefore be classified as an exploratory case study [according to Yin (2003)] and a multiple-case study [according to Stake (1995)].

Rowley (2002) remarks that one of the argumentative interrogations posed on a case study approach is related to what number of cases are adequate for a study? Eisenhardt and Graebner (2007), and Easton (2010b), argued that a single – or multiple - cases can be adopted in a case study, depending on the objective of the research. As such, there may be no ideal number of cases. Charmaz (2006) points out that using a large sample size does not guarantee the originality of a research contribution. This implies that sample size (or the number of cases) used to carry out a particular research study does not automatically correlate to result reliability. For this particular study four universities were invited to participate in the study. Three out of the four invited institutions responded and agreed to participate in the study to explore the influence of technology, organization and environmental factors on information security policies and compliance.

3.3 Stage B - Data collection.

McMillan and Schumacher (2010), identified various collection techniques which can be used for data collection in a qualitative study. These techniques are, observation, document and artefact collection, field observation and supplementary techniques and in-depth interviews.

There are three major types of interviews, structured, unstructured and semi-structured. Structured interviews are, essentially, verbally administered questionnaires, in which a list of predetermined questions are asked, with little or no variation, and with no scope for follow-up questions to responses that warrant further elaboration (Drew, 2019). Thus, by their very nature, they only allow for limited participant responses. Unstructured interviews do not reflect any preconceived theories, and are performed with little or no arrangement (Miller and Brewer, 2015). Unstructured interviews are usually very time-consuming (often lasting several hours) and can be difficult to manage, and to participate in (Drew, 2019). Semi-structured interview formats consist of several key questions which define the areas to be explored, but also allows the interviewer or interviewee to diverge in order to pursue a response in more detail (Pope, 2000). Bernard (1988) cited in (Cohen and Crabtree, 2006; Stuckey, 2013) added that semi-

structured interviews are most appropriate in a situation where the interviewer may not have an additional opportunity to interview the participant. This study utilised semi-structured interviews to gather data, motivated by 1) the flexibility of the approach, 2) the potential to discover important information regarding themes not designed in the original questionnaire, 3) the opportunity for the researcher and participants to ask for clarification if an answer/ question is vague, and 4) the opportunity for participants to express and share their views in their own terms.

3.3.1 Phase 4 Sampling Plan

According to Yin (2013), purpose-based sampling provides for participant recruitment and selection based on the objectives of the study. Baskarada (2014) postulated that a purposeful sampling ensures that the study population delivers adequate information needed for the study directives, and further stated that three participants or respondents would be acceptable, to produce a reliable, adequate and valuable data that is appropriate for a study (without relying on a large sample size). Having considered the suggestion by Baskarada (2014), the current study used a purposeful sampling methodology to recruit participants from three South African institutions, based on the eligibility criteria below;

1. The participant must be a Chief Information Security Officer or IT Director or equivalent position in the university.
2. He or she must be fully employed i.e. full-time contract in one of the South African universities within the ICT domain.
3. He or she must be actively involved in the day to day functions or activities that are going on in the ICT setting within the institution.

3.3.2 Phase 5 Conducting the interview

Despite the flexibility of semi-structured interviews rigorous preparation is required. Before recruiting potential participants and conducting interviews, ethical clearance from the Research Ethics Committee Officer, University of the Western Cape (UWC) was granted with Ethics Reference Number BM18/7/11. Privacy of the participant information and data obtained from the interviews had to be protected. Participants were informed during the consent process that their responses would be used as data input for the current study, the potential risks, benefit sharing and return, and what it meant to participate in the research study was explained to ensure that individuals made an informed and conscious decision to participate.

A key contact person in each chosen institution was identified and contacted in order to recruit participants. Interviewees were selected on the basis of the role they played within the institution in terms of information security management or a similar role (IT Director or equivalent and/or the Chief Information Security Officer (CISO) or equivalent). This provided input from the perspective of a senior CISO or IT Director's position and responses from these individuals could be considered high value due to the expertise of these individuals. The table below summarises all the interview processes.

Table 7: Participant recruitment and interview processes

S/N	Interview process
1	Preliminary contact with the interviewee
2	Establish dates/ times with interviewees for further communication concerning interviewing the interviewee.
3	Interviewing the respondent one-on-one
4	Each respondent to be given access to the study's findings.

An interview guide was developed to maintain the direction of the interview within the area of interest and ensure the consistency of the data collected. The researcher followed the guidelines as suggested by Badara (2007), Whiting (2008) and Turner (2010) on how to develop interview questions and procedures that the interviewer must follow. For instance, the writers suggested that 1) the interview questions must be clear and unambiguous, 2) the respondent should be at ease, 3) the interviewer must be alert and sensitivity to any new insight that may arise during the interview, and 4) the interviewer should probe further when required or take a different angle, which can influence the quality of data gathered from the interview significantly. Face-to-face interviews were used to provide the opportunity to clarify unclear questions and to explore complex issues (Sedera, Gable, & Chan, 2003).

A list of predetermined questions guided around the TOE framework was developed and used to guide the interviews to avoid deviation from the topics that would not add value to the research objectives. The principles for semi-structured interview procedures were followed (McGrath, Palmgren and Liljedahl (2019). The total time requested for the interviews was 60 to 90 minutes and care was taken to ensure that the time limit was not exceeded. Each interview was arranged and performed at the convenience of the interviewee, to maximize cooperation

Semi-structured interviews which usually contain open-ended questions, can result in discussion which may deviate from the interview questions, and as such, the conversations were recorded and later transcribed for analysis as suggested by Cohen & Crabtree (2006). Prior to commencement of interviews, the respondents were again informed about the mode of data collection (audiotape recorder) and assured of the confidentiality of the data. The recording device was checked regularly during the interviews to ensure correct functioning. All data was securely stored on a password-protected computer which belongs to the institution. Physical records such as notes made during and after the interview are kept in a locked filing cabinet with restricted access in the institution. All research data is retained and securely stored for a period of five years. The aforementioned is in-line with UWC Research Ethics Policy Section 9, under Data protection policy 12.6 and the National Data Protection Act of 1998. After the five-year storage period, all identifying information will be removed from the data and the de-identified data may be archived either at the South African Data Archive or the UWC Data Archive.

3.4 Stage C- Data Analyse

Seale (1999), highlighted some issues related to transcribing audio to text, which includes difficulty in capturing the spoken words, omissions and mixing words. In order to avoid these errors, the recorded data was transcribed by two researchers (the research fellow and the co-PI) to ensure accuracy of the data capture. Recommendations of a qualitative data analysis techniques and steps written by The Pell Institute and Pathways to College Network (The Pell Institute for the Study of Opportunity in Higher Education, 2018), were employed. As soon as data is collected, data processing took place. Detailed notes which included time and date minutiae, highlights from the interaction and other remarks were included. The interviews produced over 34,000 words of text, however, not all these transcribed texts or words are meaningful or applicable to the study and as such a data reduction process was undertaken in order to identify meaningful and relevant information to transform the data into a simplified format that can easily be understood in the context of the research questions (Castellan, 2010; Miles & Huberman, 1994).

In order to analyse the qualitative data, it must first be grouped into patterns and/or themes (Kawulich, 2004). This process is usually conducted in two major ways: content analysis and thematic analysis. The type of analysis to employ is highly dependent on the nature of the research questions and the type(s) of data collected. This study employed the thematic analysis approach to classify the data, group the data in a way that facilitates analysis, identify

and examine themes from the data in a credible and transparency manner. To achieve the transparency and credibility, the researcher allowed the data to 'speak' rather than per-defining how themes may be sub-divided. After the data had been thoroughly reviewed, the researcher returned focus to the research questions to consider themes that were expected to be drawn from TOE framework (deductive approach). However, the researcher endeavoured to consider new and unexpected ideas or themes that emerged from the data (inductive approach). Data was displayed in a matrix format and allowed for the identification of patterns and relationships observed within groups, and across groups. Each respondent was given the opportunity to review the data obtained and all the comments, changes, and modifications required by the participants were considered in the final interview report.

3.5 Coding Software

A Computer Assisted Qualitative Data Analysis Software (CAQDAS) package called ATLAS.ti was used for coding. Coding is a core function in ATLAS.ti that allows the users to communicate with the software where the interesting things are in the uploaded or imported data. According to Richard and Morse (2013), coding is the strategy that moves data from diffused and disordered text to organized ideas (Richard and Morse, 2013). It can also be referred to as attaching labels to segments of data which depicts data relationship of each segment. In ATLAS.ti, a labelled segment is referred to "Super Code" while code based density is related to the number of links between super codes (these terms were used in the discussion sections in this thesis).

That being said, ATLAS.ti is useful for the automation of the coding processes and provides a formal structure for writing and storing codes, quotations, and memos (Barry, 1998). Moreover, the software facilitates conceptual thinking about the data through an in-depth inspection of data relationships and improves the integrity of the study by making the data processes more transparent and reproducible (Hwang, 2008). However, as suggested by Barry (1998) and Frise (2014), it is essential to incorporate risk-mitigation while using CAQDAS such as ATLAS.ti. To prevent software 'hijacking' of the analysis process (Friese, 2014), this study ensured in-depth and rigorous text analysis prior to actual coding. Interview text and data analysed with ATLAS.ti was graphical represented using the Freeplane application.

3.6 Summary of the Chapter

This chapter presents the methodological approach employed in the current research project. The qualitative data design analysis approach was discussed in detail, including the data sampling case studies, data analysis, and the software used for the analysis. A summary of

the chapter is presented in the diagram below and highlights the major decision made in order to conduct this research.

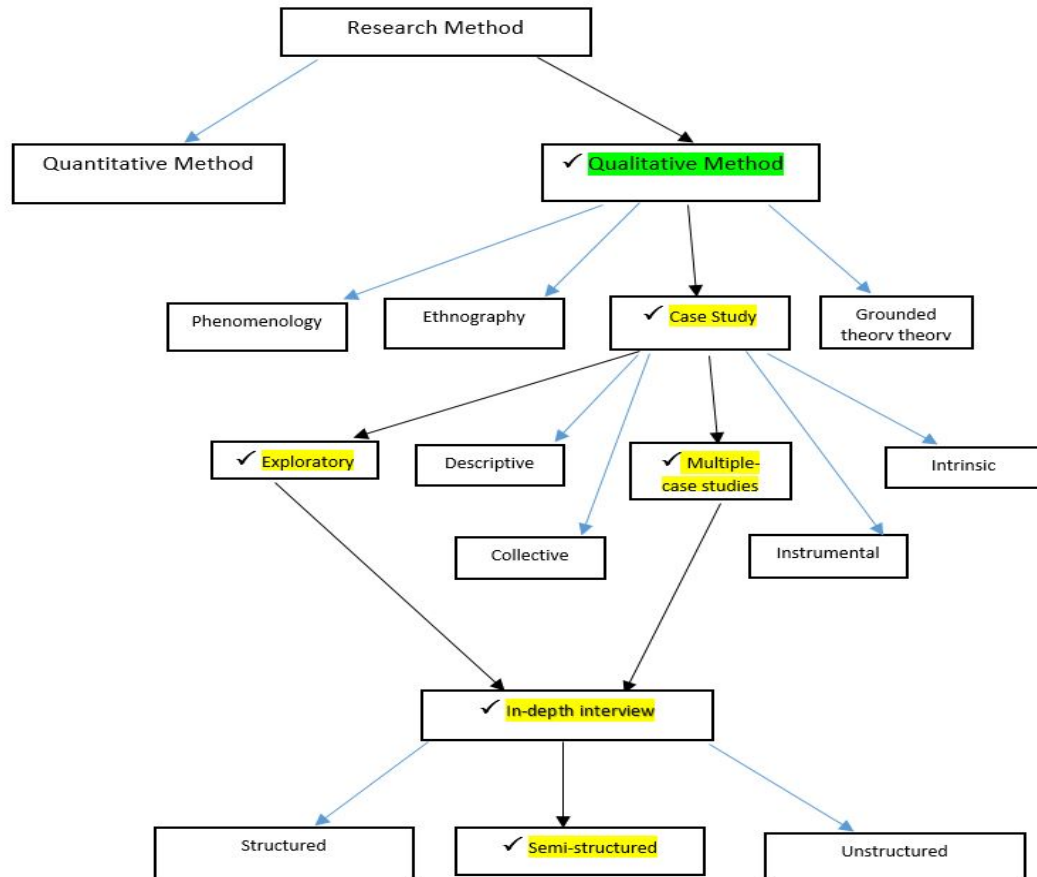


Figure 3: Summary of methodology processes employed in this study

Chapter Four

Findings and Discussion

4 Introduction

This chapter is in two parts: first, a brief overview of the key findings of the study and how they answered the research questions of this particular study. Second, a discussion of the key findings or results in an elaborately way for a better understanding and presentation. That being said, the results of the interviews provide valuable information regarding the current status of information security management, and compliance to information security standards and information regulations such as POPIA and GDPR. This information provided a foundation to explore and identify the major influencing factors and issues impacting the effectiveness of information security management, practices, policies and compliance.

A comprehensive gap analysis which identifies important factors in this way, allowed for the development of proposed information security policies to assist the biomedical practitioners within the institutional setting in securing and protecting sensitive biomedical data. This proposed policy is presented in the appendix 1 of this thesis.

4.1 Demographic features of the participating institutions

The three universities were labelled as X, Y, Z and the interviewed CISO (participant from each of the universities) were labelled CISO 1, 2, 3 respectively, to ensure ethical confidentiality and protect the identity of the interviewees as agreed in the signed informed consent forms. An equal number of respondents were interviewed from each university.

Table 8: Summary of demographic features of the participated institutions.

Demography information	University X	University Y	University Z
Type of organizational structure practiced	Top-down approach	Top-down approach	Top-down approach
Percentage of authenticated devices as at the date of interview	Less than 15%	Less than 20%	More than 60%

Information security standard implemented	COBIT 5- for governance and management. ISO 27001- for information security management.	COBIT 5 and ISO 27001	NIST and ISO 27000
Accredited with the information security standard	No	No	No
Number of data breaches experienced lately	Undisclosed	Undisclosed	Undisclosed

4.1.1 Coding Results

As stated in Chapter 3, coding of over 34,000 words generated from transcription of the interviews was performed using the ATLAS.ti software program. The textual coding generated several tables and network views illustrating code-based density and coding relationships. Table 9 below, presents a summary of all the ‘super-code’ extracted from of the interviews data using the adopted framework (TOE) to group them. Similarly, Figure 4 presents all the generated or assigned codes in the form of cloud words.

Table 9: Super codes summary with respective density.

Technology Factors (Issues)	
Code	Density
Network Patches	12
The complexity of the system	14
Poor Data classification	18
Maintenance	19
Authentication Issues	20
Poor data management mechanism	22
Poor security infrastructure	24
Lack of adequate budget	35

Organizational Factors (Issues)	
University Policies	10
Organization Structure	13
Lack of competent IT staffs	15
Organization Culture	18
Lack of coherent Strategies	20
IT directors not part of board decision-makers	23
Lack of top management support	25
Lengthy approval of time IT policies	27
Lack of prioritization of information security as core functions	30
Decentralization systems	32
Difficulties to develop an effective security culture and compliance	36
Difficulties in quantifying return of investment	37
Money or Funding Constraint	40
Users' Altitude Towards InfoSec	45
Lack of awareness and training	48
Environmental Factors	
Lack of training and information from the regulation body	12
Lack of external pressure from the government	13
Lack of motivation or incentive	15
Uncertainty on the implementation date	16
Lack of practical regulatory guidance	18

An interesting finding was that the “Chief Information Officer or equivalent role” were often not part of the decision-making executive. Two out of three interviewed participants highlighted this at their respective institution, demonstrating a structural disconnect between an institution's highest-ranking IT official and the top management. In addition to this, the Chief information security officer often occupied a ‘non-senior’ position within the central IT department since the role is not classified in a similar way to the academics, despite having wide-ranging responsibilities for security across the university. This post would require a person with highly specialized knowledge of IT security and its impacts, but was not always regarded as having authority over process and people.

Another critical finding on the status of the universities concerning information security was that the adopted method to manage information security was quoted as being based mainly on incident management, reflecting a reactive approach. Comments and thoughts expressed by participants supported the notion that a relatively unstructured and responsive approach to managing security existed within the institutions and reflected by a ‘make-do’ approach to managing security, lack of strategic security plans and lack of full integration of security within the organizational processes and budgets for IT.

2. What are the major factors which influence the effectiveness of information security management and practices? (Identified issues classified under, Technology, Organizational and Environmental issues or factors)

The findings revealed that all three classification factors i.e. technology, organizational, and environmental factors, contributed to the effectiveness of information security management and practices in the educational settings. However, organization factors appeared to be the most critical factors when compared to the other two. The essential findings under organizational factors were; lack of structure in managing information security which impacted its effectiveness across the organization, a lack of top management support which contributed to low prioritization of security, long approval times for IT policies by the councils, poor allocation of funding to information security, and low acceptance of the reality of risk. This, in turn, impacted attitude and perception of staff and students towards information security processes. Other organisational factors which were highlighted included a lack of practical awareness training, a lack of competent staff as result of limited resources (IT staff are on contractual role and work-study), IT directors not being included in decisions by the executive, and difficulties in quantifying return of investment for information security. Moreover, the

decentralization system was a critical factor coupled with the bring-your-own-device (BYOD) and 'bring-all-your-devices' (BAYD) policy.

The primary concern under technological factors is the poor security infrastructure. Network patches were not updated as they should be, authentication challenges were common-place, the systems complexity was high, data management remained poor, classification mechanism were lacking, and there was very little budget to acquire needed technology tools, staff, and devices to perform routine maintenance.

Issues identified under the environmental context are; lack of external pressure from the South African government to enforce organizations to comply with the regulations, uncertainty regarding the date of implementation of POPIA (at the time of the interviews), lack of incentive or motivation from the government to encourage compliance and a lack of practical regulatory guidance and training from POPIA information regulators.

3. *How could developments or improvements in information security management be attained at these universities?*

A structured and coordinated approach was needed to improve the effectiveness of current information security management approaches. Effective information security policies are the key to a successful information security management plan. By having a well-written, active and effective information security in place, tasks related to, and management of information security would be more straightforward and accessible. Moreover, developing more formal, well-written and compelling information security policies for the biomedical practitioners within the university community was seen as an essential step in delivering improved security management, as this group of people collects, processes and stores highly sensitive data and information to perform research functions in the university.

In addition to the policies and procedures, the human element of information security – identified as organizational factor in this study - was seen as the most critical, significant barrier to improving security and therefore, enhancing the organizational culture towards security should be one of the key focus areas for improvement.

4.2 Discussion

In this section, an in depth explanation of the key findings highlighted in section 4.1.2 will be discussed. This section provides discussion specific to each of the three major contexts of the TOE framework (i.e. Technology, Organizational and Environmental) as they related to each participant university on the subject matter.

The discussion of these key findings is used to further provide two recommendations, presented in the next chapter (chapter 5) and the appendix 1 of this thesis. The first recommendation addresses the communication gaps between the CISOs, decision makers and users, which was identified from the findings. While the second recommendation is the development of several proposed information security policies to assist biomedical practitioners within the institutional setting to secure and protect sensitive biomedical data (Appendix 1).

4.2.1 University X

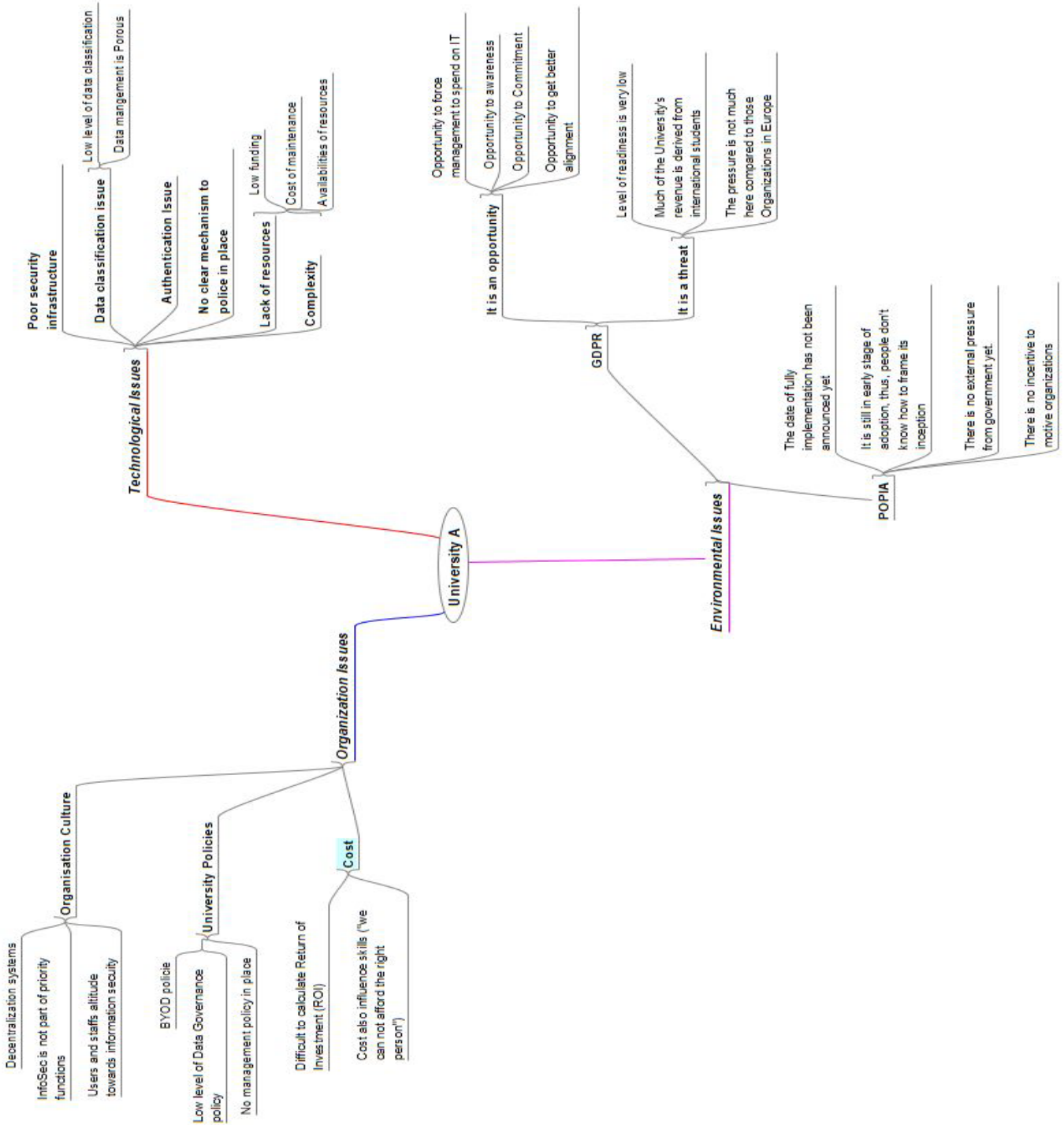


Figure 5: Technology, Organizational and Environmental (TOE) issues identified in univeristy X

4.2.1.1 Technology Issues

A lack of data classification mechanisms was one of the major constraints facing this institute. All data was given the same level of data encryption, with the exception of financial data, which is prioritised as one of the most sensitive data types. Data encryption methods are very expensive, and using the same encryption for all data, or the incorrect encryption for the wrong application is considered unsafe. The participant is quoted as saying, *“at the moment we know that all the financial data are sensitive, so we protected all our non-academic systems, but in the case of others, we don’t know where all the sensitive data is. So it is quite difficult for us to protect data going in, or coming from them.”*

According to Humer and Finkle (2014), personal health information may be 50 times more valuable on the black market (Harker’s market) than financial information, and stolen biomedical data or records can fetch upwards of \$60 per record (which is 10-20 times more expensive than credit card information). Interestingly, at the time of the interview, the participant at this institution also stated that no data management policy was in place and as such, no formalised data management strategy was implemented. Another identified concern was related to authentication issues due to a high number of devices being connected to the institution networks on a daily basis as a result of the BYOD policy. Out of about 17,000 devices that constantly made use of the network, only 15% were authenticated, a number far below standards averages. At this facility, the cost associated to Information Technology and security maintenance also influenced the level of compliance to information security practices. Other issues categorized under technology themes identified at the institution included systems complexity and poor security infrastructure.

4.2.1.2 Organization Issues

Unfortunately, security issues are often not prioritised by higher administration levels at this institution. Despite data protection and privacy being identified as a top risk, cyber management remained neglected. Since security is not part of the core function, the level of capability which was dedicated to protection and access to information was very low. There was negligible focus on device (PC’s and laptops, mobile devices) management in terms of installed software, and how the data could be copied, or shared between devices. Few technologies and mechanisms were in place to monitor and manage PCs and mobile devices in terms of access and auditing and it was perceived that all these issues would be solved if there was sufficient funding from the university. One of the recorded responses in relation to this states, *“...because the university has limited funding and as a result, when it comes to infrastructure investment or capability investment, the university is limited”*

The greatest challenges to the implementation of practices and compliance to security regulations, was the financial limitations, further highlighted by the response *“based on the funding that is available, most cases at university it is a “best effort” and I think it’s a big challenge in terms of how we can manage information security”*.

Policy development and implementation at this university was further hampered by the fact that CISOs are not part of the decision-making executive of the university. While they may inform and advise committees with regards to policy, they are not part of the council that approves, or, declines policies within the institution. A popular quote states that “the information security battle can only be won in the boardroom, not on the keyboard”, however, it appears that at this institution, IT specialists are excluded in important decision making structures, resulting in detrimental information security policy delays and ultimate rejection following multiple reviews and consultations. Additionally, a communication chasm exists, whereby committee representatives are expected to make informed decisions but have limited IT exposure and knowledge of cybersecurity. The participant was quoted as saying, *“I and my colleague developed management information security policies. It took two years to pass the policies through the system (university councils). It was unbelievable”*. The participant elaborated further on this aspect, stating, *“it is difficult for us to just quickly develop another policy. Since the one we developed took good two years just for approval, not to mention implementing it. Some of our policies are 10 to 15 years old. So, somethings just stay the same”*.

The participant highlighted the issue of a lack of staff, which negatively influencing their capability to implement and adhere to effective information security policies at the institution, saying *“we have few numbers of staff and they have to wear multiple caps, if you see a firewall guy, he will not just be doing firewall, he will do a whole bunch of other things. So supporting IT is a problem itself, now putting security on top of that makes it extremely tedious. We don’t have a formal security team, for instance, and I have multiple roles which am playing.”* This issue again, appears to be as a result of limited availability of resources (budget) within the university, and information security staff are additionally not seen to bring revenue into the university, when compared to researchers.

The participant identified other issues in the organizational themes including, 1) students and staff behavioural attitude towards information security practices, 2) decentralization of systems or policy, 3) lack of governance policy in place 4) lack of management policy in place and 5)

inadequate awareness campaigns. All these issues are possibly the result of information security not being part of the priority functions at this university.

4.2.1.3 Environmental Issues

The GDPR was perceived as both an opportunity as well as a threat. Our participant believed that GDPR would serve as an opportunity to compel management to spend adequately on IT, as the pressure from the external regulatory bodies would be beyond the control of IT and ICS. In this way, GDPR would be a driver for management to start thinking about compliance or face the consequences of not doing so. The participant also perceived that GDPR would serve as an opportunity to create greater awareness amongst students, staff and board members, providing an opportunity to gain commitment from both the IT users, and management, thereby creating better alignment within their institution. The participant added that *“until they are aware, they may not be informed and if they are not informed, they will not acknowledge the importance of information security and compliance.”*

However, GDPR was also perceived as a big threat at this institution due to the very low level of readiness, with policies that drive awareness for infrastructure users, yet to be put in place. Another concern by the participant at the time was that the university appeared to be too relaxed about the regulation, as compliance pressure was not as high when compared to companies and organizations in Europe. This would prove to be detrimental, as major revenues do stem from international guarantors and university will need to be complaint with data regulations. Therefore, a failure to be compliant with this regulation would negatively impact university revenue and research output. In this study, the POPIA data regulation was also identified as an external factors (pressure) that may influence adoption and effective implementation of information security practices and policies amongst the South African universities. However, due to continuous implementation delays by government and the regulatory body, POPIA seemed to have less of a driver for information security compliance at this university. One of the major reasons mentioned by our respondent was that government had not been pressurizing organizations about POPIA and the date of its full implementation had not yet been announced (In January 2020, the office of the information regulator approached the South African president to approve a commencement date of 1 April 2020). Moreover, POPIA was still the early phase of adoption, people did not know how to frame its inception and were somewhat unfamiliar with the context. The respondent further added that if the government could organize awareness training and provide motivations (incentive), this would encourage action by organizations and increase the POPIA adoption rate.

4.2.2 University Y

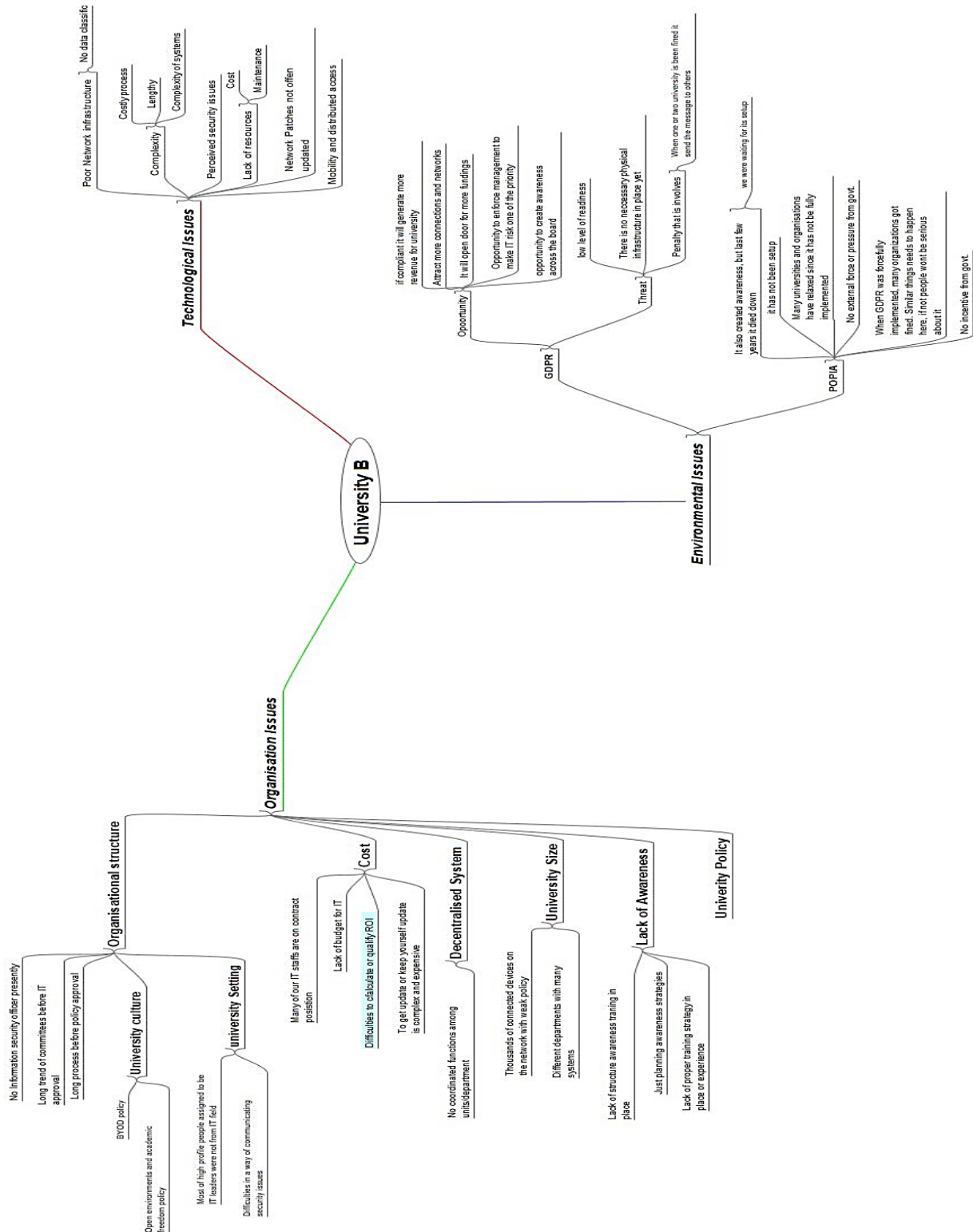


Figure 6: Technology, Organizational and Environmental (TOE) issues identified in university Y

4.2.2.1 Technology Issues

Again, at this institute, the lack of data classification mechanisms featured as a major constraint under the technological context. No data classification scheme was yet in place and data owner (each department or units) seemed to have their own data classification schemes. This is as a result of a decentralized system at this University, highlighted by this response from the participant - *“everyone has their own processes, I think one of the challenges in many educational institutions would be that there’s a lot of processes that happen in silos, so there’s no, as far as I am concerned, uniform way of how data is being managed”*

4.2.2.2 Organization Issues

At the time of the interview, this institution did not have an information security officer and the information security role was distributed amongst other staff. This contributed greatly to their inability to implement information security practices. Moreover, there existed no formalized procedure to deal with information security incidence, although some plans had been put in place to build information security capability internally. This institution was in the process of employing an information security officer soon after the interview. Another constraint to information security practices at this institution was that its information security policy had not been reviewed for a substantial period, as highlighted by the participant stating, *“we have an information security policy but look it hasn’t been reviewed in a while. Actually, it is one of the core functions of the new information security officer that’s going to come on board”*. This was a concern because these policies need to evolve and be updated as new technologies arise. Information technology is a rapidly evolving field and as such, the security policy must move at the same pace. Failure to remain current poses a larger threat to privacy, confidentiality, intellectual rights, security, reliability, accountability and responsibility (Mutongi and Marume, 2016).

As with University X, a lack of funding was another identified issue and the respondent claimed that the financial constraints meant that the facility could not afford an information security officer for at least three years - *“We’ve tried for the last three years to get an information security officer, we can’t get it from external because we don’t have the funding, we can’t pay the people”*. The prior allocated budgets assigned to the IT department have not been sufficient enough to run IT maintenance and procure certain tools and skills.

Information security professionals are considered to be valuable, skilled personnel and do expect a certain compensation, in line with industry levels. This was supported by the participants statement, *“We can’t get them on the salaries we are offering which means that it*

makes it difficult because funding is definitely one of the key factors on why I think universities are adopting policy a bit slower, because there's no dedicated resources". According to cybersecurity ventures prediction, cybersecurity engineers are the highest paying IT jobs in 2019, with an average annual salary of \$149,000. It will continue to be a challenge to afford such expertise for this university, and others, which experience budgetary constraints despite the obvious need for these engineers in the tertiary education setting.

In addition to this, and also identified in University X, the problem of quantifying the return on investment on information security, is not an easy task. The value proposition of information security is likened to insurance, asking the management to spend a certain amount of money on particular tools where a tangible return on investment to the university system is difficult to demonstrate is not trivial. In addition, information security spend is generally perceived to be necessary once something significant has occurred. These aforementioned issues were taking place at university Y, because information security was not part of the core function of the management structures, contributing to a lack of support from the top management and the decision-making bodies. As with University X, individuals at the decision table were not from the IT background, thereby making justification on IT spending increasingly difficult. The respondent made the following comments in this regard.

"The IT director would then often report to the DVC academic and the DVC academic is an academic, so they do not come from our background, they do not really have that insight into IT operational methods which is difficult and that often gets reflected in how budgets are allocated. It is also reflected in the amount of attention a particular issue gets. So if information security is not high on the agenda of that particular academic group then it won't get the necessary budget whereas if you had an IT executive and one IT representative sitting as part of the executives, it make a lot of sense because then those challenges are being brought to the executive directly".

Other organizational issues identified included a lack of effective and consistent awareness training, and complexity of the information security domain which requires broad skill sets which requires both a time-spend and a financial spend in order to stay up to date. Furthermore, improper infrastructure and a lack of systems compatibility for information security are further issues experienced at the institution.

4.2.2.3 Environmental Issues

As with University X, GDPR was recognized as both a threat and an opportunity. It was seen as a threat because of the penalties which surrounds non-compliance. This threat is further

amplified for this university because a new proposed strategy to generate more revenue is to extend teaching and learning system to distance learning, allowing for enrollment of international students, including those domiciled in Europe. To achieve this checks and balances will have to be put in place to accommodate the new system and the international students, however, at this current stage the necessary physical or basic infrastructure to accommodate this system, especially in terms of compliance, is not in existence.

Where GDPR was seen as an opportunity, was reflected by the above revenue stream, in that if compliance was attained and maintained, the extended distance learning would bring in needed finances. In addition, the opportunity for GDPR to create definite awareness and influence perspectives on information security issues, not only as an IT problem but a general issue for decision makers and users in the university, was identified.

With regards to POPIA, the respondent believed that POPIA and GDPR are very closely aligned and both are recognized data protection regulations. Both regulations can serve as tools to send a message of security awareness to the individuals, universities and organizations, specifically those in South Africa. Implementation and enforcement of POPIA has not been active in South Africa and as a result, organizations may be too 'relaxed' and this sentiment was echoed by the statement from the participant - *"I think that's just the human nature, until something happens you will not start thinking it is so real. For instance, when GDPR was launched and I think in the first week some big company was targeted, and they got fined with some crazy amount. So that needs to happen. As soon as those kinds of things start happening and you hear about it in the news and everywhere then there's going to be a lot bigger push"*

Additional issues which the participant raised with relation to POPIA is that government needs to create more awareness about the Act, and organize an incentive to motivate universities, perhaps in the form of ranking or accreditation for those that comply - *"I think if government does that there is going to be a lot more, not just financial incentives but if you have some ranking for instance "the greener University or the most compliant University", then I'm pretty sure there is some monetary value attached that or the institution might get opportunity to partner with Universities."*

4.2.3 University Z

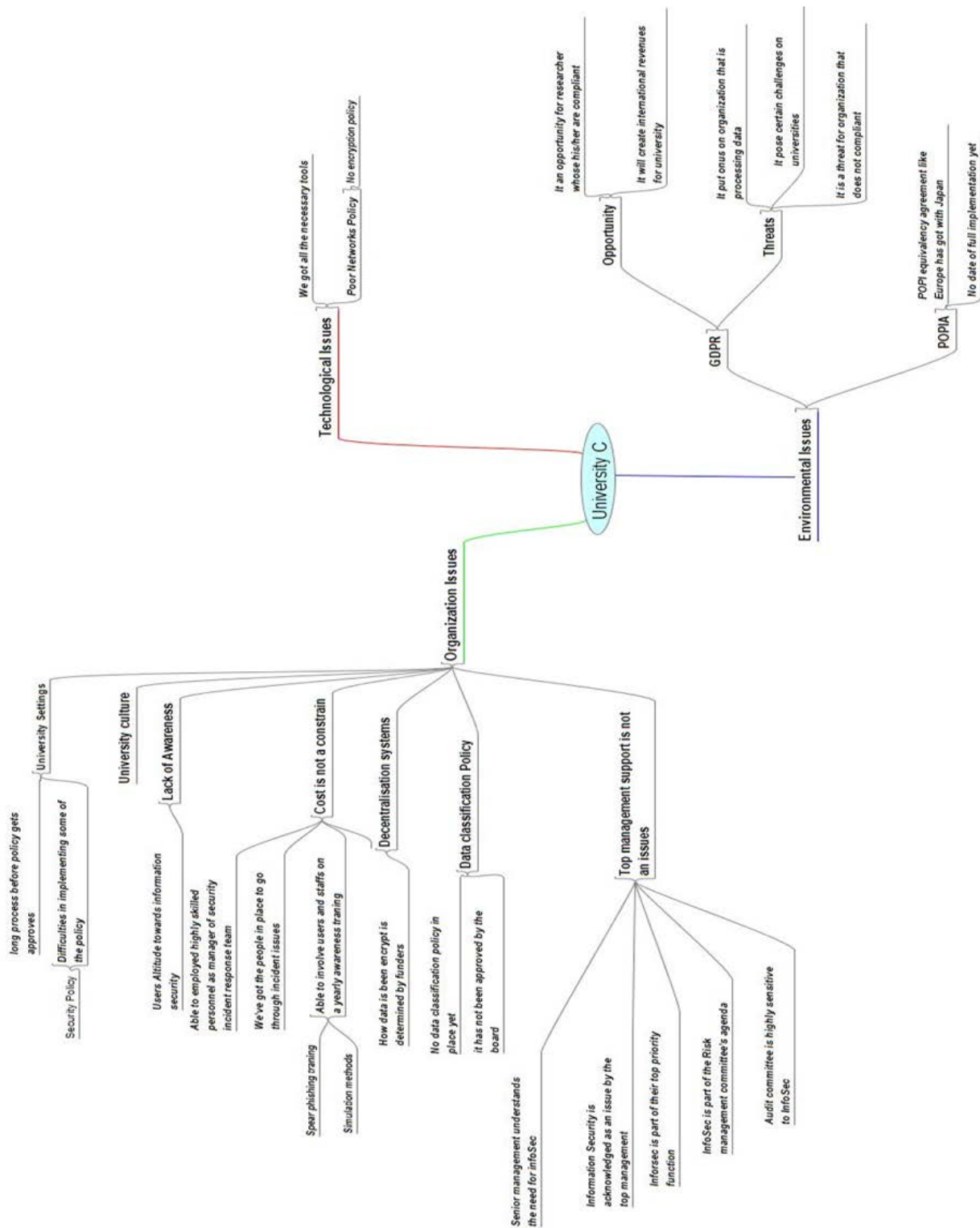


Figure 7: Technology, Organizational and Environmental (TOE) issues identified in university

4.2.3.1 Technology Issues

Unlike the other two universities, this institution does not have many technological issues obstructing them from practicing information security in the university. The participant stated, *“We’ve got all the tools that we need and we can have a good look at the system and get a feel for what is going on with it or not going on with it”*. The network patches were constantly assessed for vulnerabilities and the same applies to servers and other pieces of software. After assessing the software, if there are any issues which need be addressed, it is done without any budget or funding constraint. The management had signed a maintenance agreement on behalf of the IT department, thereby making allowance for emergency items to be repaired. As a result of full support from the top management and decision markers, University Z was not hindered by a lack of tools to protect information and data.

4.2.3.2 Organization Issues

In similarity with University X and University Y, this institution is faced with time-based delays in policy, procedure and process approvals. However, a major difference between this institutions when compared to the other two universities is a quicker approval timeframe. Interestingly, this institution did not have an encryption policy, data policy and data classification policy in place at the time of the interview, as highlighted in the statement *“Policy-wise has been a challenge. I wrote an initial policy and that took a bit of flak, so we are trying to make a change on a wide front at the moment, thus, presently we don’t have an encryption policy as yet. That is once the security policy is adopted that will be one of the policies that needs to be implemented as part of or alluded to as part of the data protection policy”*.

Information security awareness was the biggest challenges this university was facing. However, much had already been done by the IT teams and management to raise awareness relating to security threats and keep users and staff up to speed. A security awareness campaign was performed each month for staff, and every year during induction week, basic information related to information security is communicated to students. This training includes, but is not limited to, how to identify phishing attempts and spear phishing, by running simulations. However, despite efforts and campaigns, the level of awareness was not yet satisfactory. After asking the respondent about the main challenges faced by university Z in the implementation of an effective information security policy, the response below was received.

“Academia – that’s the challenge. Academics do not want to be constrained. If you make academia aware that you are going to be monitoring, then you are going to get a lot of questions. So, we’re working on that. Even though we’ve done a lot of things, as I’ve mentioned before, we’ve done some interventions, but I think there is still a lot more to be done.”

University Z appears to be in a better position to undertake process and campaign interventions with relative ease. This can be attributed to the fact that the IT teams have full support from the top management, sentiments echoed in the response, *“I must say that we are fortunate – the reason why we are making some progress and I qualify it as some rather than a lot is that our senior management, Vice-Chancellor included, are fully on board and understand the need for information security, and cyber security.”* This appears to be a result of information security and risk management being a priority on the committee’s agenda and as such, IT teams are provided with all the necessary mechanisms, tools and support to enable them to make greater progress. With information security issues being part of the core function of the management at this institution and therefore acknowledged as critical, this University provides the IT teams with required funding to address urgent and immediate needs. Furthermore, because decision makers have insight about information security, there is less difficulty in quantifying the Return on Investment, and the participant highlighted this in the statement, *“How we try to reflect back to them the value is the reports that we provide them with, some metrics and unfortunately, sometimes those metrics don’t always show an improvement. It is a reality. It shows things are going backwards and the reason why that is because one is starting to discover more and more of what is going on because there’s a focus on it. However, the value is the knowledge which is created”*. Other beneficial implementations at University Z include competent information security staff, and an incidence response team to investigate incidents by carrying out a full forensic audit and documenting incident handling.

4.2.3.3 Environmental Issues

Similar to the respondents at University X and Y, GDPR is perceived as an opportunity and, at the same time as a threat. For a university that is compliant, the opportunity exists to collaborate with other universities especially from Europe. This will also benefit the researchers in such an institution because it will create an avenue for international funding

and project collaboration. However, for an institution that is not compliant, the threat will be great. With respect to POPIA the respondent believed that the two regulations were similar, a view expressed by the respondent from university Y. These similarities may imply that, an organizations compliance to GDPR, would make compliance to POPIA easier but not vice versa. This is a challenge to organizations in South Africa, considering the need to comply with both regulations which may not be an easy task for the universities. The respondent from University Z suggested that the South African government needs to take a similar approach to these regulations as the Japanese government has with European government. These two government entities met and evaluated the respective data protection regulations and an agreement was reached, allowing for the Japan policy privacy legislation to be recognised as equivalent to the GDPR. If a similar concession can be proposed for POPIA, it would increase its adoption rate amongst university and organizations as a whole.

4.3 Overview of identified technology issues

The major concern under technological factors is poor security infrastructure. The focus of security infrastructure relates to the ability to best use the new or existing technological solutions to monitor security processes such as authorization mechanisms, system patching, firewalls and anti-virus software. Findings from this research study show that two out of the three participating intuitions have poor security infrastructure. Both application and network patches were not in good standing at the time of the interview. Some of the reasons that contributed to this included; network patches were not updated as they ought to be, authentication challenges, the complexity of the systems, poor data management, lack of classification mechanism, lack of adequate budget to acquire needed tools, staff and mechanisms, and perform routine maintenance.

This study has shown the value of maintaining the security infrastructure as it facilitates management of security within the university network. For example, tools such as firewalls, encryption mechanisms, authentication mechanisms, and non-repudiation mechanisms are essential for a university system. Therefore, they need to be continuously checked for consistency and proper functionality. In order to achieve this, emphases should be placed in the information security management processes such as risk analysis, architecture review, code inspection, and security testing. In addition, this needs to be monitored on a regular, consistent basis as malfunction of these tools can lead to failure of effective security management

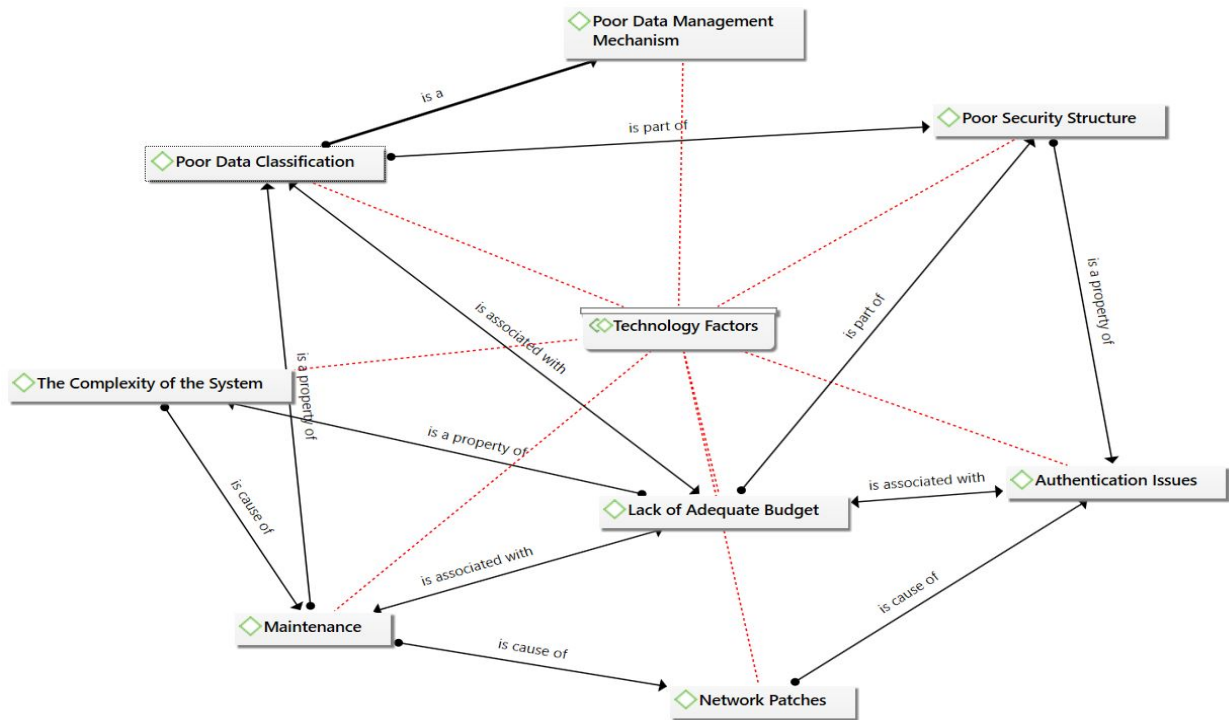


Figure 8: An overview of themes on technology issues identified.

4.4 Overview of identified Organizational Issues

Organizational factors define the influential factors that contribute to the success or failure of information security according to the users. In the context of this study, we investigated the common factors that contribute to the failure of effective implementation of security policies, practices, and compliance in the institutions. Findings from this study demonstrated that organizational factors were the most critical factors when compared to the technological and environmental contexts which were examined. Some of the major issues identified under the organizational context are; Lack of top management support, funding or financial constraints, lack of effective awareness training, information security practices not being part of the management core priority functions, lack of coordinated functions among units and departments, long approval times for IT policies by the councils, decentralization of systems, staff behaviour and perception towards information security processes, lack of competent staff as a result of limited resources, IT top staff not being a part of university decision making bodies, and difficulties in quantifying return of investment for information security spending.

From the issues listed, it was apparent that human error contributed the most to the information vulnerabilities that occurred in an organization. Human errors may be due to

negligence or a lack of awareness and leads to dramatic consequences for the organizations. That is, vulnerabilities or breaches happen not because security is difficult, but rather, it occurs because people *think* security is not hard. Human behaviour is therefore identified as the weakest link and greatest threat to information security within the organization. However, with consistent and effective security awareness training, these issues can be decreased with a view to mitigate the threat it poses. In addition, security should not be an IT problem alone, but rather a social problem. If this can be achieved, then the decision makers will possess the knowledge to add information security to their core function issues to be addressed. Lastly, security professionals should always present security issues to the management in a language they will understand (in form of business-oriented metrics and not in technical operational metrics). In information security, communication is key.

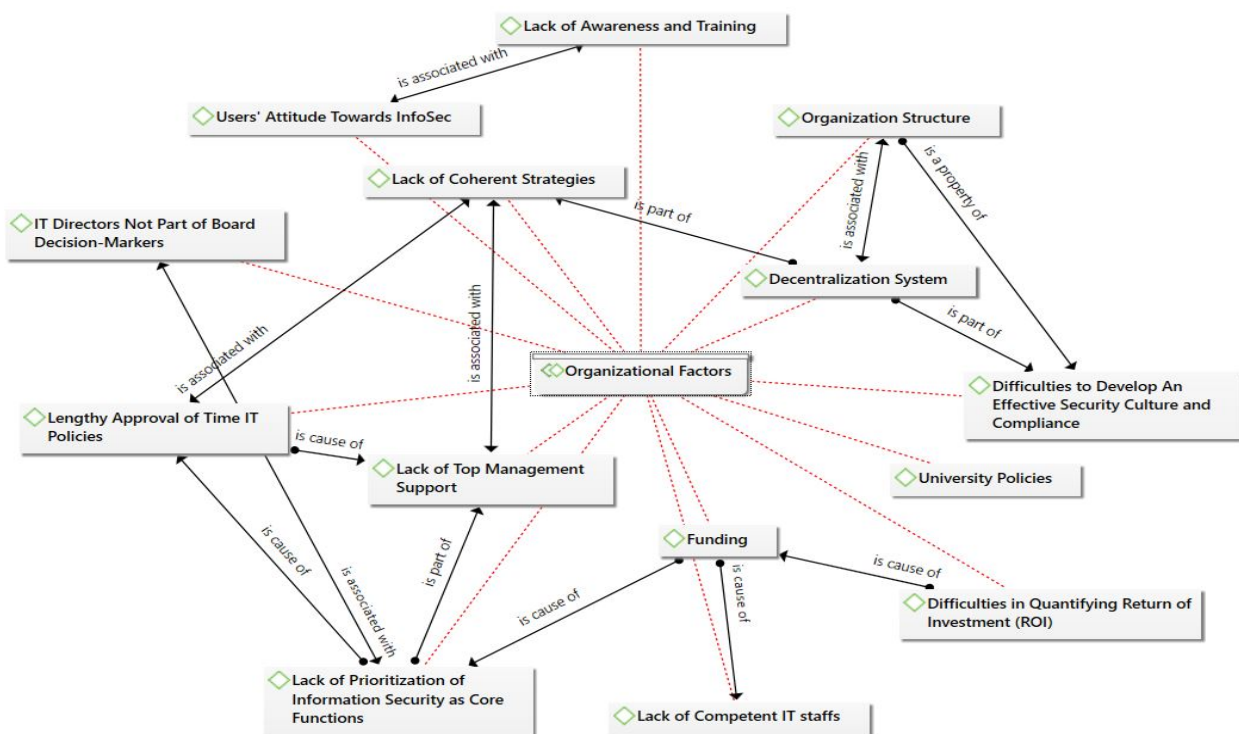


Figure 9: An overview of identified themes on organisational issues

4.5 Overview of Environmental Factors

As stated in chapter one of this thesis, external factors such as pressure from governmental regulatory agencies impact security implementation and standards, and may influence the effectiveness of information security practices in organizations (Kam *et al.*, 2013; Albuquerque Junior and Santos, 2015b; Klein and Luciano, 2016). Similarly, a study by Ma and Ratnasingam (2008), also claimed that some industries such as healthcare, finance and government organizations, tend to be dedicated to compliance with external agencies in the matter of information security. Based on these claims, in this study, our environmental factors measured the effect of regulatory pressure which examines the audit, security policies and standards imposed to manage information security in a proper and acceptable way, in line with international and local standards.

4.5.1.1 GDPR:

- a. The pressure to comply with regulations is not a high priority in Africa when compared to the advanced countries such as those in Europe. However, this may prove detrimental to international collaboration in the future.
- b. There exists a low level of readiness.
- c. Two of the three participating institution do not yet have the physical infrastructure in place.

4.5.1.2 POPIA

- a. While both regulations exhibit similarities, there remains an agreed level of compliance connection between the two regulations and some uncertainty exists.
- b. No certainty of the date of implementation (at the time of the interviews).
- c. Considering the early stage of adoption, organization do not know how to frame its inception.
- d. No incentive or motivation from the Government to encourage its adoption, but rather a level of confusion from all stakeholders.
- e. Lack of practical regulatory guidance and training from POPIA regulators and government is leading to poorly implemented and unenforceable security controls. Moreover, since there is inadequate training and awareness from the law enforcement and judiciary fraternity, this makes fining of this regulation seem impossible.

- f. When GDPR was forcefully implemented, many organizations were fined. It would appear that the POPIA regulation would not be taken seriously until such time that non-compliance is similarly fined.

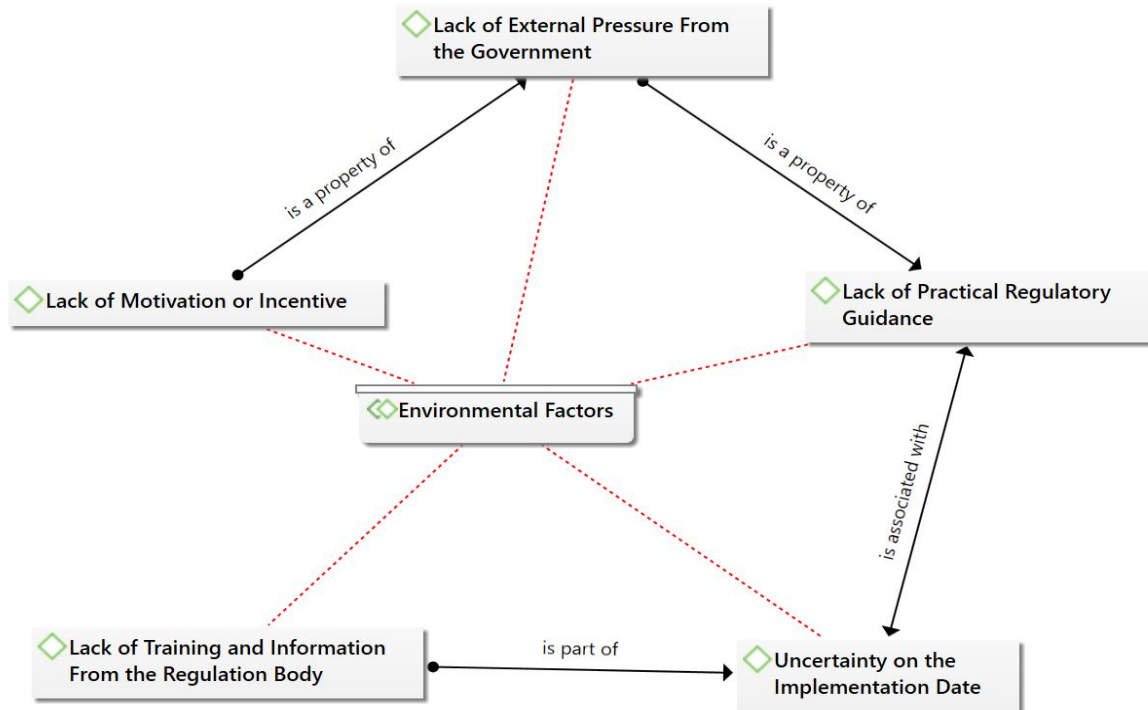


Figure 10 : An overview of identified themes on environmental factors.

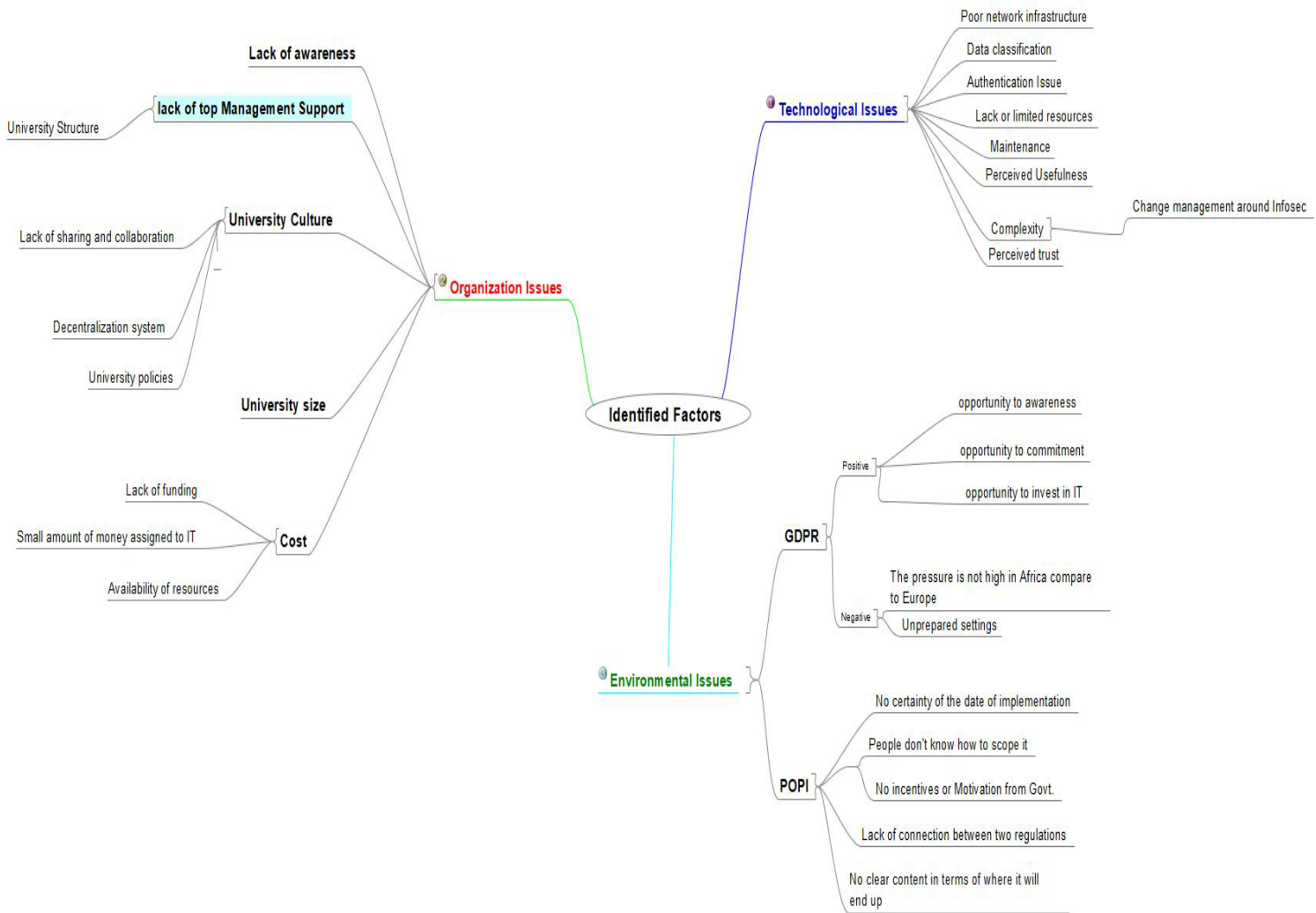


Figure 11: Combined trait issues identified from the extracted themes amongst the three universities

Chapter Five

Observations and Recommendations Related to Addressing the Communication Gaps.

5 Introduction

Effective management of information security policies and procedures for securing valuable organizational information, relies on the harmonious interaction between ‘people’, ‘processes’ and ‘technology’. While the technical measures which are utilised to secure information are important, there is more to keeping information secure than simply the installation and configuration of technical tools. Information assets of an organization cannot be protected from unauthorized access, use, disclosure, disruption, modification or destruction by only applying technical controls. In this study some influential factors which hinder the effectiveness of information security practices and compliance amongst the South African universities were investigated and the results of this current study revealed that amongst the three contextual factors examined, organisational factors, appeared to be the most critical. Some of the major issues identified in relation to organizational factors have been discussed in chapter 5, and from this, we identify that a communication gap exists between the decision-makers (board members of the universities or the management), the CISOs (the cybersecurity teams, IT security teams) and the users (students, teaching and non-teaching staff, researchers or academics).

In this chapter, we aim to provide some recommendations on how to bridge the communication gaps between the decision-makers, CISOs, and the users, firstly by categorising groups in the context of their roles and responsibilities with regards to information security in the academic setting. Secondly, this chapter will also highlight some of the common errors each of these groups of people commit, which exacerbates the disconnect in communication between them. Finally, the chapter will highlight some suggestions and recommendations for mitigation of errors with a view to decrease the communication gap and ultimately improve information security practices within the academic settings. A draft policy on InfoSec is proposed for consultation with university stakeholders (see Appendix 1)

5.1 How can a university protect and secure their information?

Dlamini, Eloff, & Eloff (2009), surmise that the notion of protecting information from hazards, unauthorized access, and other vulnerabilities has been in existence prior to the development of the computer. Warren & Brands (1979) ascertained, that the concept of securing information began as far back as early eighteenth century when Julius Caesar developed a cipher code to protect messages of military importance from being accessed by unauthorized people (Liu, Zhang, Jin, & Cheng, 2015; Zhao & Dong, 2017; Warren & Brands (1979). This concept of a secret code was adopted and modernized to what is referred to as encryption code today. Significant changes have occurred due to the constant evolution of technology and innovation, driven by development in the internet of things (IoT), cloud computing, robotic process automation and cognitive computing. Ultimately in the current era of big data, people will also need to change and adapt their behaviour.

The protection of information is multifaceted and highly complex. Achieving a 100 percent guaranteed protection of information and data, is neither feasible, nor should it be the ultimate goal (Lacey, 2011, Whitman & Mattord, 2012, Gelbstein, 2011). Information security is not a product, but a process, and a way of thinking (Sookdawoor, 2002, Whitman & Mattord, 2012). Failure in data protection occurs when blind spots exist, a vulnerability is overlooked and subsequently exploited. As such, the best approach to information security is to consider each asset in the context of its associated risk, and its value, as well as to consider the relationships among all assets and risks.

In the organizational context, each possible vulnerability should be managed in order to achieve the protection of data and information to acceptable levels. This can be accomplished using a layered, comprehensive approach to mitigate hacking risks, even if one control fails. Comprehensive protective measures must be developed, implemented, practiced and benchmarked (Caballero, 2013; Rao and Nayak, 2014b). However, all of these cannot be achieved without human intervention, as such, anthropogenic factors must be considered from the development phase to the implementation and benchmarking phase. Everyone in the organization must work together, know their responsibilities and share the same mind-set about securing the organizational information. All the stakeholders, including users must be informed, trained and communicated with, when deciding on methods to eradicate or mitigate information vulnerabilities in an organization.

However, in universities, some common mistakes are made by the executives, security teams and the users, resulting in tedious and sometimes ineffective information security practices.

This will be presented in section 5.2, highlighting some suggestions on how to decrease common errors and prevent their reoccurrence. The common errors described in the section below were extracted from the data collected through the three interviews with three CISOs of South African universities. The suggestions relating to error mitigation were additionally informed by discussions with IT experts at a security conference, in combination with other online data sources.

5.2 The executive members and some of the common mistakes committed in information security decisions

In this study, decision-makers are referred to as the top executive management members in the university structure such as the Rector or Vice-Chancellor, Deputy Vice-Chancellors, Registrars, the Chief Financial Officers, and Deans of the faculties. This group of people are responsible for the execution of the Strategic Plan and implementation of council decisions and institutional policies. They are also responsible for decision-making in respect of staffing matters, procedures that support council approved policies, changes and amendments to organizational structure and evaluation of performance management reports (McCaffery, 2010; Price, 2018). The role of this group of people in the university environment can be compared to driver of a car – even if the vehicle is in excellent condition, if the driver cannot pilot the car, it will not get to its destination – simply put, and the mandate will fail.

Clearly, the role of the executives in achieving the objective of information security within an institution cannot be underestimated. They approve or disapprove any security policy formulated by security teams. Many of their decisions are influenced by business objectives without critically considering the information security consequences, leading to detrimental implications for the university. Below are some of the common errors interpreted from our data in relation to information security decision making in the university setting.

5.2.1 Primarily depend on firewall instead of the 'human-wall'.

A properly deployed, configured and maintained firewall can be an excellent part of the organization's overall network security (Kisin, 1996). Moreover, it can also be used to provide analytical data on the amount of hostile intention the network is receiving, as well as the nature of attempted attacks thereby providing some insight into areas prioritisation (Fithen, Allen, & Stoner, 1999; Kisin, 1996). However, it cannot be relied upon as the sole security measure. Protection of information has evolved passed the era of only using a firewall (a technical tool) as a means of data protection, and now days, harnessing the 'human-wall' (commitment of a group of employees to follow best practices to prevent as well as report any data breaches or

suspicious activity), in combination with the firewall, under well-executed processes, is becoming common place. For the university to have a realistic opportunity to protect information against data breaches and vulnerabilities, the executive management need to understand and embrace this principle.

5.2.2 IT security approval duration and delays.

Technology is advancing at a rapid pace, as are the related issues. Unfortunately, the executives' decisions on information security policies are moving sluggishly and, in many instances, by the time an IT security policy has been approved, it is already obsolete. One of the CISOs interviewed expressed concern on this issue stating;

“Me and my colleagues developed management information security policies. It took two years to pass the policies through the system. It was unbelievable. It is difficult for us to quickly develop another policy. Since the one we developed took two good years before approval, not to speak of implementing it”.

Clearly, employing state-of-the-art security technology tools in combination with outdated policies, make both interventions void.

5.2.3 Lack of understanding in relating information security to the organizational issue

Executives have an excellent understanding of physical security but fail to recognise the consequences of poor information security. For instance, in a situation where a threat (riot) from the users (students or employees) is tangible, it easier to deploy security officers to protect the physical assets and personnel of the university, irrespective of the cost. However, the protection of data assets is far more difficult to justify to executives, making the financing of IT spend, a complicated and contested issue.

5.2.4 Ignoring information security issues in the hopes they will resolve themselves

Technology is here to stay (Arimoto & Cummings, 2014) and the existence of cyberattacks will remain an issue with a definite increase in frequency (Morgan, 2018). Organizations will continue to rely on technologies to carry out various functions and as such, cyber security will remain an important and critical risk factor. Failure to except this will ultimately result in a resource and financial burden to any university.

5.2.5 Failing to realize how much money the information and organizational reputations are worth.

To quote Stephane Nappo, “It takes 20 years to build a reputation and few minutes of a cyber-incident to ruin it.” In any functional business, it is very important to maximize the return on investment (Breedt-Maree, 2017), and as a result, managers (the executives) are more willing to motivate budget spend on items with a calculated return on investment (ROI). Unfortunately, the concept of ROI has not fared very well in the information security discipline (Layton, 2007). Therefore, finding a way to keep costs down while maximizing protection against potential security breaches has been a tough battle (Cho, 2003). The difficulty in justifying IT spending, often lies in the paradox that one is essentially investing in something that has not yet occurred or may never occur. This principle can be applied to the protection of valuable assets through insurance. The immediate benefits of his/her investment would not be apparent, until the day something has occurred. Interestingly, the purchasing of insurance is easily justified, but Information security spending appears to be far less so, despite the fact that effective data protection would safeguard an organization from the negative impact of data breaches such as financial losses (Van Niekerk, 2017), legal consequences of information breaches (GDPR, POPIA) (Voigt & Von dem Bussche, 2017), and detrimental reputational damage (Lacey, 2011).

5.2.6 Assigning CISO without given them necessary authority over people and organization processes

When CISO are placed in the wrong departments, with ineffective reporting lines, and limited authority, information security receives inadequate priority in organization activities and objectives (Kooliyankal, 2017). This was observed at two of the three intuitions during the interviews conducted for this study. The two CISOs were not part of the decision-making committees and in addition, the board members responsible for decision making were not from the IT field. As a result of this, the CISOs have neither the authority, budget, resources nor reach, to ensure an end-to-end security.

CISO 2

Question: *“Are you a part of the decision makers in the university?”*

Response: *“I’m just a contributor to the motivation and justification of policy investment but I don’t make decision on the policy or investment.”*

5.3 Some suggested responsibilities for the executives in order to have efficient and effective information security practices within their university settings.

It is possible that most if not all, of the abovementioned errors are unknowingly being committed and may also be a result of the responsibilities of their jobs. The executive positions are very tightly scheduled, full of meetings, goal setting, community relations, academic affairs, fundraising, budgeting and more. With so many responsibilities requiring the attention of these executives, a cyber-based discussion may be perceived to be inaccessible and filled with technical jargon, resulting in being side-lined by more familiar and seemingly important matters. Additionally, the majority of the top management members ascend to the position of institutional leadership through the ranks of academia and many of them have limited exposure to, and fluency in, cyber issues and the potential business impact on an institution. As a result of this, issues relating to information security rarely appear on board-level agendas, except if there is a major breach. However, by then it might be too late to take the necessary action and the cost to the university may be so great, that it would be difficult to recover from. The above errors can be avoided, controlled and improved upon if the executives understand what proactive steps to take to prevent risk occurrence. Below are six suggested recommendations that will assist the executives and help them in taking a proactive approach towards information security effectively in their institution.

1. The executives must understand that the information security issue has crossed the line of 'just being technological issue'. It must be addressed as an organization-wide risk management issue.
2. It is recommended that the management should have a fundamental understanding of the legal implications of cybersecurity risks and how they relate to the university environment.
3. The executives must seek regular advice on cybersecurity from their CISO, engaging discussions about cybersecurity risk management should be undertaken regularly and be allocated adequate time in the board meeting agenda.
4. It is also advisable that the executives establish an organization-wide cyber-risk management framework with adequate staffing and budget.

5. Finally, since majority of the executives were ascend to the position of institutional leadership through the ranks of academia and many of them have limited exposure to, and fluency in, cyber issues and the potential business impact on an institution. Thus, it is highly recommended that the executives should delegate appropriate and qualify staffs to develop, communicate and publish a comprehensive set of information security policies. The policies should be written in a simple, standardized and structured format and must be reviewed and updated regularly (and timeously) with appropriate version control.

5.4 The Security teams (CISOs) and some of the common mistakes committed on information security decisions

The role of CISOs and security teams are also essential to the functions of the organization, and before any organization can succeed in its information security objectives, the security teams should be consulted with. Their experience and knowledge on the security of systems and infrastructure cannot be underestimated. In this section, we refer to CISOs and security teams as skilled personnel that are responsible for overseeing the overall activities of information security in the university. They are responsible for designing architecture for computer platforms and networks, as well as overseeing the development and management of software systems (Cho, 2003). To illustrate the significant value of CISOs and their teams, we continue with the previous analogy of a car. The CISOs and their security teams are like an engine of a car, no matter how the perfect the driver of the car, if there is no engine, or if the engine is faulty, the car will not move. Therefore, errors committed by this group of people will have detrimental effects on the organization. Below are some of the common errors extracted from interviews conducted in this study.

5.4.1 Lack of a holistic approach

Lack of a holistic approach leads to addressing of information security issues in a superficial manner (Kooliyankal, 2017). From the results in the study, this appeared to be one of the most common mistakes committed by CISOs and security teams. Instead of understanding the root causes of security issues in order to implement a corrective action, CISOs often look at the security issues from technical point of view only. For instance, two out of the three interviewed CISOs (university CISO), claimed that the major factor which impeded information security implementation at their respective institutions, was a financial one (inadequate of funding or budget). While this is an important factor, the role of user awareness and training with regards to information security was underestimated.

CISO 1

Question: *“Do you think population is one of the major constraints to an effective information security practice?”*

Response: *“Money is a factor for everything within the university context. So, if you remove the money factor then size doesn’t matter. So the problem is money.”*

Question: *“What can you say about security awareness in your university especially among the staff?”*

Response: *“Yes absolutely it is very low.”*

CISO 3

Question: *“Do you have student and staff awareness training? And do they know about the awareness?”*

Response: *“Yes, we have, and they do. So what we do is every year during induction we actually use the induction process at the university (orientation week) to communicate with the students some of the basic information security that they need to know about. So we would advise them on how to try and identify phishing attempts, spear phishing, all the flavours of these things.”*

Question: *“What are the challenges your university are facing in implementing effective information security practices?”*

Response: *“Academia (users) – that’s the challenge. Academics do not want to be constrained...”*

Question: *“How do you solve issue on ROI on information security in your university?”*

Response: *“Here management acknowledged that Information Security is an issue. It has actually provided us with project funding to address some of the urgent and immediate”*

It can be observed from the responses of CISO 3, funding support from the management to procure necessary security tools at the institution is used in combination with yearly awareness training for the users. Interestingly, the major challenge at the time of the interview was identified to be the user. This demonstrates that even if the other two institutions (CISO 1 & 2) had a greater amount of funding to procure security mechanisms, they would still experience what the third institution (CISO 3) has. Therefore, the funding constraint is not the only factor which should be considered by CISOs and security teams. Cybersecurity cannot be achieved only by IT procurement and implementing the most advanced technology. Successful

information security must be holistic and include correct processes and procedures, and stakeholder awareness and training.

CISO 2

Question: *“What are the challenges your university is facing in implementing an effective information security practice?”*

Response: *“If you look at the IT budget within university, if you look at what they need to do with the budget maintaining infrastructure doing those kinds of things information security often doesn’t get the budget that it needs to get I mean you don’t have the budget to able to implement certain tools.”*

Question: *“What are you doing or what have you done on staff awareness and training?”*

Response: *“We are actually launching an information security awareness program early next year. So we shall basically send out an email campaign (phishing campaign).”*

5.4.2 Failure to organize consistent security awareness training programs

Linked to the section above, an awareness security training program that will educate users on their responsibilities with regards to potential security problems, should be implemented in a consistent manner. According to the European Network and Information Security Agency (ENISA), an awareness information security program can be defined as follows (ENISA cited by (Marinos, 2011);

1. Provide a focal point and a driving force for a range of awareness, training and educational activities related to information security. Some may already be in place but would require better coordination to be more effective.
2. Communicate important recommended guidelines and practices required to secure information resources and motivate individuals to adopt the recommended guidelines or practices.
3. Provide general and specific information about information security risks and controls, to relevant stakeholders.
4. Make individuals aware of their responsibilities with regards to information security.
5. Create a stronger culture of security, with a broad understanding and commitment to information security.

6. Help enhance the consistency and effectiveness of existing information security (Kearney, 2010.)

Communication informs users and the executives on information security and advises stakeholders of their respective roles and responsibilities. Awareness training provides an opportunity for users to learn basic concepts of information security.

5.4.3 Ignoring the fundamental services and focusing on the extravagant

Kooliyankals observed that security professional frequently get distracted by overly elaborate security solutions, and this may result in neglecting the essential security services (Kooliyankal, 2017). This was detected during this study, with two out of the three interviewed CISOs neglecting fundamental information security solutions or services, and focussing on more extravagant, advanced solutions (running unnecessarily services). Some of these fundamental security solutions left unattended to, include data classification, digital forensic services, and incident response team services.

CISO 2

Question: *“Do you have any plan in place to mitigate or response to any incidents?”*

Response: *“At the moment we don’t have a formalized way of dealing with information security incidence.”*

5.5 Suggested responsibilities for the CISOs and the security teams to minimize or avoid the above-mentioned mistakes to have effective information security practices within the university settings.

The most important responsibility of the CISOs and the security teams is to build a healthy information security culture within an organization. Ferriss (cited in Romeo, 2018), defined security culture as “what happens when people are left to their own devices”. If we insert “with security” into this definition it will become; “security culture is what happens with security when people are left to their devices (Romeo, 2018). In any organisational system, human behaviour has been recognized as the main factor resulting in errors. Security culture is primarily for humans, not for computers, as the computers do exactly what the human has instructed them to. For example, a human being may select links they receive in an email without checking or verifying the sources, download applications and software from unsafe sites and fail to install or update antivirus. Therefore, in an organization such as a university, there is a need for a framework that will assist the users, the executives, and even the security

team to understand preventative and corrective action. CISOs and the IT security teams must invest time and effort into fostering better information security behaviour of users as healthy security cultures can change one-time events into a lifecycle regularly embedded in day-to-day activities, ultimately producing effective security practice.

1. There is a need for the CISOs and the IT security team to communicate that security is the responsibility of all stakeholders who make use of the IT systems. Each stakeholder who makes use of the university resources, owns a piece of the university's security solution.
2. According to the European Security Forum (1993), information security awareness is defined as "the degree or extent to which every member of staff understands: 1) the importance of information security 2) the levels of information security appropriate to the organization 3) their individual security responsibilities, and acts accordingly". Ngo (2008), proposed that "giving individual knowledge of IT security basics such as threats, risks, and their consequences will allow individuals to gradually adapt to constant change and hence allow us to predict expected behaviour". Most users, and the executives within the institution want to do the right thing as far as security is concerned, but they just need to be taught. It is important to understand that accountability cannot be enforced before awareness is created.
3. The CISOs with their security teams should investigate opportunities to incentivise healthy security culture.
4. Filzen (2001), postulated that the key to any successful security awareness program is to make information security both informative and highly engaging. Many users, including the executives, disassociate themselves from being involved in security process based on their perception of technical people - being referred to as 'boring' and 'using too much jargon', therefore, anything being delivered by a technical person will surely be tedious and difficult to learn. It is the responsibility of the security teams to erase this perception by building an entertaining, interesting and informative process to create a healthy security culture. Uber's Davison states that, *"Security can be so much more than PowerPoints and videos. Pick a fun theme and parody it - we did Game of Thrones. Give gamification a try. Throw a phishing writing workshop and have your employees write a phishing email for the company. The options are endless when you start to think outside the box."*

5. The CISOs need to communicate with executives in a manner that will allow for better understanding of information security issue so that it can be easily related to business continuity aspects of university operations. One question which executives or board members will ask is, “Are we secure?” For the CISOs, this is a very difficult question to answer. According to Andrew Rose’s (Chief Security Officer, Vocal ink) opinion the answer to this will combine peer comparison, maturity assessment, and real-world examples in order to demonstrate the applicability in the university sphere. In this way, executives will understand that their institutions are not immune from cyber-threats.
6. Universities remain prey to cybersecurity vulnerabilities due to disjointed operations both within and between universities. It is highly recommended that the CISOs of each university work together to build a security community, which is the backbone of a healthy information security culture. Incentivizing enhanced collaborative behavior, will increase community participation whereby monthly meetings which discuss the latest security issues, may manifest into a yearly conference, with participants from each university being given the opportunity to share their knowledge and skills to a wider audience.

5.6 Users and some of the common mistakes committed on information security

It is widely acknowledged that users or employees of an organization are often a weak link in the protection of information assets (KPMG, 2013; Tang, Li and Zhang, 2016; Bada, Sasse and Nurse, 2019). In this study, we define users as those who make use of university network resources to complete day-to-day tasks. Users include, but are not limited to, the staff (teaching and non-teaching), researchers, students (undergraduate, postgraduate, postdoc) and visitors. Users are analogous to the body of a car. Without the body to house the engine (CISOs) and the driver (executives), the car is not a complete system. Users want both security and flexibility, finding a balance between these two is not a trivial task (Metalidou et al., 2014). In the constant battle between cyber-attackers and security professionals, users can swing the balance one way or the other: regrettably, the unpredictability of human behaviour can make the most secure information systems, obsolete (Metalidou et al., 2014). Users and their behaviour are the “Achilles heel” of information security (Gonzalez & Sawicka, 2002, Koh et al., 2005).

Previous studies which investigate user attitude and behaviour towards information security have demonstrated that some users circumvent information security controls to complete their

job tasks (Hagen, Albrechtsen, & Hovden, 2008; Rahim, Hamid, Kiah, Shamshirband, & Furnell, 2015). Users may neglect information security due to a lack of knowledge on information security and some transgressions may be intentional (Mitnick & Simon, 2003). Albrechtsen (2007), claims that a lack of general awareness also influences the behaviour of users. Furthermore, to motivate users to embrace a security culture, management should identify ways of including users in decision making related to implementation of, and adherence to, security procedures (Koh, Ruighaver, Maynard, & Ahmad, 2005).

In the university setting, users commit very reckless errors, which inherently increase the risks of information vulnerabilities threats. All of the user-based errors identified in this study can be grouped into themes, previously identified in other studies i.e. lack of awareness, lack of motivation, intentional and unintentional behaviour, lack of threat perception and poor security culture. Below are some common user errors extracted from interview data from the three CISOs. Some of these identified errors are commonly identified in the SANS Institute (System Administration, Networking and Security) lists of user error which interrupts operations and slows down the implementation of secure operating environments.

5.6.1 Inappropriate use of technology devices as a result of BYODs policies.

Based on findings from the interview data, incorrect usage of technology by the users due to the Bring Your Own Devices Policy appeared to be one of the major challenges faced by the CISOs in the university settings. Students and employees take advantage of this (BYOD) policy without considering the risks to information assets of the university. Some examples of negative BYOD behaviour include weak passwords on devices (in some cases passwords are completely absent) and using the same password for all devices. Considering that the average students or staff member may have two or three devices connecting to the network on a daily basis, one can understand how non-adherence to simple password best practice can create information security vulnerability. In addition to this, some users connect to unsafe public free networks when accessing sensitive or confidential information from their student or staff accounts. Some of the users even share their passwords with friends or colleagues over unsecured Wi-Fi networks. This behaviour creates easy access to confidential or sensitive information by cyber-intruders.

5.6.2 Improper use of university accounts e.g. staff or student email account.

This includes, but is not limited to, opening unsolicited e-mail attachments without verifying the source, checking the content first and using staff or student email address with default passwords for personal communication, or to register for online sites. Any breach to an online site will not only directly affect the sites but also poses a high risk to every other site linked to

the user via the same email address and password. One of the CISOs commented on how this habit exposed the university to big threats by stating, “*So there was company online called XXXX, there were roughly about 2million accounts on there, so 24 accounts from the school email accounts registered into this online site or company with school email user account and password. So these 24 accounts were breached because this company was breached*”.

5.6.3 Installing applications from unknown sources or unsafe sites.

Many of the users take advantage of the network to download movies, games, and other unlicensed software and applications. Some may use torrent for downloads, and this creates a high-risk vulnerability to the user and the university networks due to content download, and associated upload. The most common risks associated to torrent use, is malware, embedded viruses contained within the downloaded torrent file, which can easily cripple computer systems (Haddin, 2016). Furthermore, the use of unsafe download sites, or peer-to-peer file sharing sites results in a high possibility of online cyber-attacks and unauthorized access to the user’s data. When a user downloads, uploads, or shares a file on any of these unsafe sites, the online hackers are able to collect information about the users’ activities and apply this data to their advantage. If the same laptop or computer contains confidential or sensitive information like ID numbers, bank card numbers, confidential research data, and payroll slips, easy access to this information can be obtained.

5.6.4 Failing to install or update security patches.

Grimes claimed that unpatched software is the leading reason for computer exploitation (Grimes, 2016). A report from Microsoft Security Intelligence stated that approximately 6,000 new vulnerabilities surface per year (average of 15 per day) (Microsoft, 2013), and each operating system or application may have hundreds of new vulnerabilities per year. These vulnerabilities are generally addressed by software patches and updates, allowing the users system to remain protected from newly identified security threats. Unfortunately, most of the students, often disable or ignore auto-update routines and this could result in a surge of malware risk which may wipe a users’ documents as well as transmit it from the users’ computer to a remote server. A very good example of this scenario was the Sony Pictures hack in 2014, where confidential information including private employee information, salary information and unreleased movies were stolen and released onto the web. In addition to this, the sophisticated malware then wiped Sony’s computer infrastructure (de Saxe, 2017). Closer to home, a recent report revealed the ‘WannaCry’ ransomware attack which targets computers running on the Microsoft Windows operating system (Warren, 2019, Brewer, 2016). WannaCry was used to attack a company responsible for powering the biggest city in South Africa –

Johannesburg - and encrypted all their databases, applications and networks, resulting in power outages in the city (Kumar, 2019). The report further highlighted the cost associated to repairing infrastructure damage even after the initial attack has ended.

5.7 Some suggested responsibilities for the users for an effective information security practices within the university settings.

User error is one of the major contributing factors to information vulnerabilities. Statistical analysis in a study conducted by the Computer Security Institute, revealed that more than 40% of security breaches through firewalls occurred due to mismanagement, while only 5% was attributed to inadequate technology (Zadelhoff, 2016). Another study from Deloitte (2009), revealed that of all the data breaches investigated in 2009, 86% were a result of user errors (Melek, 2009). The author further stated that unless robots replaced the entire human workforce (which is impossible), error from the users would continue to be a point of contention which organization would have to deal with. There is very little that a university organization can do to completely abolish user (employees and students) error apart from awareness and training. This would help to create a cohesive mind-set, where all stakeholders share the same vision and mission for information security. Below is a list of suggestions for users to consider.

1. Always be careful
2. Do not carry any more data with you than is needed
3. Encrypt disks and other data storage devices
4. Perform daily back-ups, and update security features regularly
5. Do not leave computers, documents and other devices that contain sensitive information or data, unattended to
6. Use student or staff email accounts for academic or university purposes only.
7. Copying software is illegal
8. Be aware of the source of content
9. Adhere to best practices with regards to passwords
10. Read security awareness articles, newsletters and emails (Filzen, 2001)

Chapter Six

6 Conclusion and Future Directives

As explained in Chapter 2 of this thesis that information Security is a complex topic with broad, polymorphous and multi-dimensional scope. As such issues related to it are often complicated and cannot be elucidated in a single research study. The limitations of this research study point towards areas to be addressed in future directives. This study has highlighted that technological aspects are not the only resource required for effective information security controls and as such, there is a need to evaluate the impact of organisational, and environmental factors (Jr et al., 2002; Beznosov and Beznosova, 2007; Botta et al., 2008). While this study examined all three factors, only three universities, out of a total of twenty-six universities in South Africa participated in the study. A better understanding of how different factors such as technological, organisational, and environmental factors influence the implementation and effectiveness of information security policies and compliance at tertiary education institutions is invaluable, as it sheds light on the current, and real-world, challenges being faced by these facilities. We suggest that future studies conducted in this area should include all universities in order to identify other factors that impact the effective implementation of information security practices and policies within the broader academic settings. The results from such a larger study could provide an overall understanding of issues which may be impeding implementation of security management at South African universities, and would also allow for investigation into strategies which have resulted in successful outcomes. Moreover, results could also be useful in benchmarking information security management within the university sector, by comparing efforts between peer institutions. This may not only rank information security at institutions, but may also provide a valuable opportunity for cross-institutional collaboration and capacity development.

It must be noted that universities are not exempt from compliance requirements to legislative directives such as GDPR and POPIA. As such, universities will need to develop and implement information security policies and procedures, clearly define roles and responsibilities, and introduce focussed training in line with information security and management standards. The effort required to identify and implement practical solutions for basic data collections, can be exponentially amplified when dealing with biomedical data collections. This study has addressed this by developing an initial draft information security policy for the biomedical and research institutes. While we acknowledge that this policy is not a 'one-size-fits-all' solution, we suggest exploring the implementation of this proposed information security policy within

the biomedical and research institutes. Further work in this area should involve multi-stakeholder investigation into customising various levels in the focus areas of the proposed information security policies, thereby resulting in a mature policy, which is more appropriate for each institution and can be readily updated. Studies which address overall compliance should also include proper measures of data legislation, such as POPIA, to assess impact, adequacy, and operation in practice.

Part of this study has been published in the international peer-reviewed journal “International Data Privacy Law Journal”. (See Appendix 2, supplementary data for the publication).

References

- Al-Dhahri, S., Al-Sarti, M. and Abdul, A. (2017) 'Information Security Management System', *International Journal of Computer Applications*, 158(7), pp. 29–33. doi: 10.5120/ijca2017912851.
- Albert (2015) *History of Computers and Computing, Birth of the modern computer, Personal computer, Apple Macintosh*, *history-computer.com*. Available at: <https://history-computer.com/ModernComputer/Relays/Zuse.html> (Accessed: 1 December 2019).
- Albuquerque Junior, A. E. de and Santos, E. M. dos (2015a) 'Adoption of Information Security Measures in Public Research Institutes', *Journal of Information Systems and Technology Management*, 12(2), pp. 289–315. doi: 10.4301/S1807-17752015000200006.
- Albuquerque Junior, A. E. de and Santos, E. M. dos (2015b) 'ADOPTION OF INFORMATION SECURITY MEASURES IN PUBLIC RESEARCH INSTITUTES', *Journal of Information Systems and Technology Management*, 12(2). doi: 10.4301/S1807-17752015000200006.
- AlHogail, A. (2016) 'Managing human factor to improve information security in organization', (c), pp. 2–6.
- Alnatheer, M. A. (2015) 'Information security culture critical success factors', in *Proceedings - 12th International Conference on Information Technology: New Generations, ITNG 2015*, pp. 731–735. doi: 10.1109/ITNG.2015.124.
- Alotaibi, M., Furnell, S. and Clarke, N. (2017) 'Information security policies: A review of challenges and influencing factors', in *2016 11th International Conference for Internet Technology and Secured Transactions, ICITST 2016*. Institute of Electrical and Electronics Engineers Inc., pp. 352–358. doi: 10.1109/ICITST.2016.7856729.
- Alshaikh, M. *et al.* (2015) 'Information security policy: A management practice perspective', in *ACIS 2015 Proceedings - 26th Australasian Conference on Information Systems*. Available at: <https://arxiv.org/abs/1606.00890> (Accessed: 2 December 2019).
- Andress, J. and Winterfeld, S. (2014a) *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice: Second Edition, The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice: Second Edition*. Available at: www.elsevier.com/permissions. (Accessed: 4 February 2021).
- Andress, J. and Winterfeld, S. (2014b) *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice: Second Edition, The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice: Second Edition*. Available at: www.elsevier.com/permissions. (Accessed: 27 March 2020).
- Arko-Cobbah, A. (2008) 'The Right of Access to Information: Opportunities and challenges for civil society and good governance in South Africa', *IFLA Journal*. SAGE PublicationsSage UK: London, England, 34(2), pp. 180–191. doi: 10.1177/0340035208092154.
- Ashenden, D. (2008) 'Information Security management: A human challenge?', *Information Security Technical Report*, 13(4), pp. 195–201. doi: 10.1016/j.istr.2008.10.006.
- Atchinson, B. K. and Fox, D. M. (1997) 'The Politics of the Health Insurance Portability and Accountability Act', *Health Affairs*. Project HOPE, 16(3), pp. 146–150. doi: 10.1377/hlthaff.16.3.146.

- Avison, D. and Pries-Heje, J. (2005) *Research In Information Systems: A Handbook For Research Supervisors And Their Students*. Available at: [https://books.google.co.za/books?id=MCLTJKqk2xMC&pg=PA246&lpg=PA246&dq=Walsham+and+Waema+1994\)+case+study&source=bl&ots=RmcJ5voUnR&sig=ACfU3U0mtQerFiqxSsqE5Bk5uWtjN6dSTA&hl=en&sa=X&ved=2ahUKEwiNod3a_t_nAhUPrxoKHakSCUAQ6AEwD3oECAGQAQ#v=onepage&q=Walsham an](https://books.google.co.za/books?id=MCLTJKqk2xMC&pg=PA246&lpg=PA246&dq=Walsham+and+Waema+1994)+case+study&source=bl&ots=RmcJ5voUnR&sig=ACfU3U0mtQerFiqxSsqE5Bk5uWtjN6dSTA&hl=en&sa=X&ved=2ahUKEwiNod3a_t_nAhUPrxoKHakSCUAQ6AEwD3oECAGQAQ#v=onepage&q=Walsham an) (Accessed: 20 February 2020).
- Ayyagari, R. and Tyks, J. (2012) 'Disaster at a University: A Case Study in Information Security', *Journal of Information Technology Education: Innovations in Practice*, 11, pp. 085–096. doi: 10.28945/1569.
- Bacik, S. (2008) *Building an Effective Information Security Policy Architecture, Building an Effective Information Security Policy Architecture*. doi: 10.1201/9781420059069.
- Bada, M., Sasse, A. M. and Nurse, J. R. C. (2019) 'Cyber Security Awareness Campaigns: Why do they fail to change behaviour?' Available at: <http://arxiv.org/abs/1901.02672> (Accessed: 2 December 2019).
- Bakari, J. K. *et al.* (2005) 'State of ICT security management in the institutions of higher learning in developing countries: Tanzania case study', in *Proceedings - 5th IEEE International Conference on Advanced Learning Technologies, ICALT 2005*, pp. 1007–1011. doi: 10.1109/ICALT.2005.243.
- Baldrige, J. V. *et al.* (1977) 'Diversity in Higher Education: Professional Autonomy', *The Journal of Higher Education*, 48(4), p. 367. doi: 10.2307/1978649.
- Baldwin, R. (2019) *Technology in Education - Higher Education - Learning, Educational, Students, and Technologies - StateUniversity.com*. Available at: <https://education.stateuniversity.com/pages/2496/Technology-in-Education-HIGHER-EDUCATION.html> (Accessed: 31 March 2020).
- Baloch, R. (2017) *Ethical Hacking and Penetration Testing Guide, Ethical Hacking and Penetration Testing Guide*. doi: 10.4324/9781315145891.
- Bar Ilan, J. (2008) 'The History of Information Security: A Comprehensive Handbook 2008' Edited by Karl de Leeuw and Jan Bergstra. *The History of Information Security: A Comprehensive Handbook*. Oxford: Elsevier 2007. 887 pp. (hard cover), ISBN: 97804444516084', *Library Hi Tech*, 26(4), pp. 682–683. doi: 10.1108/07378830810920987.
- Barker, I. (2015) *35 percent of all security breaches take place in higher education*, *Betanews*. Available at: <https://betanews.com/2014/12/17/35-percent-of-all-security-breaches-take-place-in-higher-education/> (Accessed: 2 December 2019).
- Barnard, L. and Von Solms, R. (2000) 'Formalized approach to the effective selection and evaluation of information security controls', *Computers and Security*, 19(2), pp. 185–194. doi: 10.1016/S0167-4048(00)87829-3.
- Barry, C. A. (1998) 'Choosing qualitative data analysis software: Atlas/ti and Nudist compared', *Sociological Research Online*, 3(3). doi: 10.5153/sro.178.
- Baskarada (2014) 'Qualitative Research : Case Study Guidelines', *The Qualitative Report*, 19(40), pp. 1–25. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2559424 (Accessed: 18 November 2016).
- Baskerville, R. and Siponen, M. (2002) 'An information security meta-policy for emergent organizations', *Logistics Information Management*, 15(5/6), pp. 337–346. doi: 10.1108/09576050210447019.

- Baxter, P. and Jack, S. (2008) 'Qualitative Case Study Methodology : Study Design and Implementation for Novice Researchers Qualitative Case Study Methodology : Study Design and Implementation', 13(4), pp. 544–559.
- Baxter, P., Susan Jack and Jack, S. (2008) 'Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers', *The Qualitative Report Volume*, 13(4), pp. 544–559. doi: 10.2174/1874434600802010058.
- Bayuk, J. et al. (2012) *Cyber Security Policy Guidebook*, John Wiley & Sons, Inc., Publication.
- Beckers, K. and Beckers, K. (2015) 'The CAST Method for Comparing Security Standards', in *Pattern and Security Requirements*. Cham: Springer International Publishing, pp. 51–83. doi: 10.1007/978-3-319-16664-3_4.
- Benbasat, I., Goldstein, D. K. and Mead, M. (1987) 'Strategy in Studies of', *MIS Quarterly*, 11(3), pp. 369–386. doi: 10.2307/248684.
- Bieker, F. et al. (2017) 'Privacy Technologies and Policy', *Proceedings of the 4th Annual Privacy Forum, (APF 2016)*, 10518(October), pp. 21–37. doi: 10.1007/978-3-319-67280-9.
- Bindu, C. S. (2015) 'Secure Usable Authentication Using Strong Pass text Passwords', *International Journal of Computer Network and Information Security*, 7(3), pp. 57–64. doi: 10.5815/ijcnis.2015.03.08.
- Blitzer, E. and Wilkinson, A. (2009) *Higher Education as a Field of Study and Research, Higher Education in South Africa - A scholarly look behind the scenes*. doi: 10.18820/9781920338183/17.
- Botha, R. A. and Gaadingwe, T. G. (2006) 'Reflecting on 20 SEC conferences', *Computers and Security*, 25(4), pp. 247–256. doi: 10.1016/j.cose.2006.04.002.
- Braman, S. (2002) 'Defining information', *Telecommunications Policy*, 13(3), pp. 233–242. doi: 10.1016/0308-5961(89)90006-2.
- Bulgurcu, B., Cavusoglu, H. and 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), pp. 523–548. doi: 10.2307/25750690.
- Bulgurcu, Cavusoglu and Benbasat (2017) 'Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness', *MIS Quarterly*, 34(3), p. 523. doi: 10.2307/25750690.
- Caballero, A. (2013) 'Information security essentials for IT managers: Protecting mission-critical systems', in *Managing Information Security: Second Edition*, pp. 1–45. doi: 10.1016/B978-0-12-416688-2.00001-5.
- Cascio, W. F. and Montealegre, R. (2016) 'How Technology Is Changing Work and Organizations', *Annual Review of Organizational Psychology and Organizational Behavior*. Annual Reviews, 3(1), pp. 349–375. doi: 10.1146/annurev-orgpsych-041015-062352.
- Castellan, C. M. (2010) 'Quantitative and Qualitative Research: A View for Clarity', *International Journal of Education*, 2(2). doi: 10.5296/ije.v2i2.446.
- Charmaz, K. (2006) 'Constructing grounded theory: A practical guide through qualitative analysis (Introducing Qualitative Methods Series)'. Available at:

<http://www.citeulike.org/group/7276/article/2806115> (Accessed: 17 November 2016).

Chen, C. C., Shaw, R. S. and Yang, S. C. (2006) 'Mitigating Information Security Risks by Increasing User Security Awareness: A Case Study of an Information Security Awareness System', *Information Technology, Learning & Performance Journal*, 24, pp. 1–14. Available at: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.102.5945&rep=rep1&type=pdf> (Accessed: 20 February 2020).

Chen, J. and Shen, L. (2010) 'Assessment model of corporate governance with COBIT-based IT governance', in *Advanced Materials Research*, pp. 550–557. doi: 10.4028/www.scientific.net/AMR.121-122.550.

Cheng, V. S. Y. and Hung, P. C. K. (2006) 'Health Insurance Portability and Accountability Act (HIPPA) Compliant Access Control Model for Web Services', *International Journal of Healthcare Information Systems and Informatics (IJHISI)*. IGI Global, 1(1), pp. 22–39. doi: 10.4018/jhisi.2006010102.

Cherdantseva, Y. and Hilton, J. (2013) 'A Reference Model of Information Assurance & Security. Availability, Reliability and Security (ARES)', in *Proceeding of the 18th International Conference*. Available at: <https://ieeexplore.ieee.org/abstract/document/6657288/> (Accessed: 28 May 2019).

Cherdantseva, Y. and Hilton, J. (2015) 'Information Security and Information Assurance', in *Standards and Standardization*, pp. 1204–1235. doi: 10.4018/978-1-4666-8111-8.ch058.

Cho, M. (2003) 'Mixing Technology and Business: The Roles and Responsibilities of the Chief Information Security Officer'.

Clements, A. (2006) *Principles of computer hardware*. Available at: <https://books.google.co.za/books?id=wUecAQAQAQBAJ&pg=PA12&lpg=PA12&dq=1948,+machines+used+vacuum+tubes,+but+after+1948,+transistors+were+introduced,+and+by+the+end+of+1960&source=bl&ots=mq4xCXgP-N&sig=ACfU3U0k2C7gQqgiRv3aBYaZB1LQfndSbA&hl=en&sa=X&ved=2ahUK> (Accessed: 25 March 2020).

Cohen, D and Crabtree, B. (2006) 'Qualitative research guidelines project'. Available at: [http://www.sswm.info/sites/default/files/reference_attachments/COHEN 2006 Semistructured Interview.pdf](http://www.sswm.info/sites/default/files/reference_attachments/COHEN%202006%20Semistructured%20Interview.pdf) (Accessed: 18 November 2016).

Cohen, D. and Crabtree, B. (2006) *Semi-structured Interviews*. Available at: [moz-extension://b63f3363-bd76-4e59-ba14-8669246e8b96/enhanced-reader.html?openApp&pdf=https%3A%2F%2Fsswm.info%2Fsites%2Fdefault%2Ffiles%2Freference_attachments%2FCOHEN%25202006%2520Semistructured%2520Interview.pdf](https://www.sswm.info/sites/default/files/reference_attachments/COHEN%202006%20Semistructured%20Interview.pdf) (Accessed: 20 February 2020).

Coleman, L. and Purcell, B. M. (2015) 'Data Breaches in Higher Education', *Journal of Business Cases and Applications*, 15(15), pp. 1–7. Available at: <http://www.aabri.com/copyright.html>.

Cooper, R. B. (2000) 'Information technology development creativity: A case study of attempted radical change', *MIS Quarterly: Management Information Systems*, 24(2), pp. 245–276. doi: 10.2307/3250938.

Cram, W. A., Proudfoot, J. G. and D'Arcy, J. (2017) 'Organizational information security policies: A review and research framework', *European Journal of Information Systems*, pp. 605–641. doi: 10.1057/s41303-017-0059-9.

- Crawley, K. (2017) *Information Security, Cybersecurity, IT Security, Computer Security... What's the Difference?, The State of Security*. Available at: <https://www.tripwire.com/state-of-security/featured/information-security-cybersecurity-security-computer-security-whats-difference/> (Accessed: 11 April 2020).
- CREATe (2016) *Cyber Crime in Higher Education - CREATe.org*. Available at: <https://create.org/news/cyber-crime-higher-education/> (Accessed: 2 December 2019).
- Creswell, J. W. (2012) *Educational research: Planning, conducting, and evaluating quantitative and qualitative research, Educational Research*. doi: 10.1017/CBO9781107415324.004.
- Crossler, R. E. *et al.* (2014) 'Understanding Compliance with Bring Your Own Device Policies Utilizing Protection Motivation Theory: Bridging the Intention-Behavior Gap', *Journal of Information Systems*, 28(1), pp. 209–226. doi: 10.2308/isys-50704.
- Dabbagh, N. and Bannan-Ritland, B. (2005) *Online learning: Concepts, strategies, and application*. Available at: <https://rmuf.pw/online-learning-concepts-strategies-and-application.pdf> (Accessed: 1 December 2019).
- Dalacoura, K. (2010) 'Book Review: Barry Buzan and Ana Gonzalez-Pelaez (eds), International Society and the Middle East: English School Theory at the Regional Level (Basingstoke: Palgrave Macmillan, 2009, 304 pp., £63 hbk)', *Millennium: Journal of International Studies*, 39(2), pp. 567–568. doi: 10.1177/0305829810382536.
- Davis, J. (2019) *Patients Sue UConn Health over Data Breach Caused by Phishing Attack*. Available at: <https://healthitsecurity.com/news/patients-sue-uconn-health-over-data-breach-caused-by-phishing-attack> (Accessed: 25 March 2020).
- Dell'Amico, M., Michiardi, P. and Roudier, Y. (2010) 'Password strength: An empirical analysis', in *Proceedings - IEEE INFOCOM*. doi: 10.1109/INFOCOM.2010.5461951.
- Denley, A., Foulsham, M. and Hitchen, B. (2019) *GDPR – How to Achieve and Maintain Compliance, GDPR – How to Achieve and Maintain Compliance*. doi: 10.4324/9780429449970.
- Dhillon, G. and Backhouse, J. (2000) 'Information system security management in the new millennium', *Communications of the ACM*, 43(7), pp. 125–128. doi: 10.1145/341852.341877.
- Dimitriadis, K. (2011) 'Feature Information Security From a Business Perspective A Lottery Sector Case Study', 1, pp. 1–6.
- Dinu, M.-S. (2018) 'New Data Protection Regulations and Their Impact on Universities', in *Elearning Challenges And New Horizons, Vol 4*, pp. 26–33. doi: 10.12753/2066-026X-18-218.
- Disterer, G. (2013) 'ISO/IEC 27000, 27001 and 27002 for information security management'. Available at: https://serwiss.bib.hs-hannover.de/files/938/ISOIEC_27000_27001_and_27002_for_Information_Security_Management.pdf (Accessed: 2 December 2019).
- Dlamini, M. T., Eloff, J. H. P. and Eloff, M. M. (2009a) 'Information security: The moving target', *Computers and Security*, 28(3–4), pp. 189–198. doi: 10.1016/j.cose.2008.11.007.
- Dlamini, M. T., Eloff, J. H. P. and Eloff, M. M. (2009b) 'Information security: The moving target', *Computers and Security*. Elsevier Ltd, 28(3–4), pp. 189–198. doi: 10.1016/j.cose.2008.11.007.

- Drew, P. (2019) *Research methods in social network*. Available at: <https://books.google.co.za/books?id=sePEDwAAQBAJ&pg=PA73&lpg=PA73&dq=Structure+d+interviews+are,+essentially,+verbally+administered+questionnaires,+in+which+a+list+of+predetermined+questions+are+asked,+with+little+or+no+variation+and+with+no+scope+for+follow> (Accessed: 20 February 2020).
- Easton, G. (2010a) 'Critical realism in case study research', *Industrial Marketing Management*, 39(1), pp. 118–128. doi: 10.1016/j.indmarman.2008.06.004.
- Easton, G. (2010b) *One Case Study is Enough (Working paper, No 2010/034)*. Available at: <https://eprints.lancs.ac.uk/id/eprint/49016/> (Accessed: 20 February 2020).
- EDUCAUSE (2018) 'Elevating cybersecurity on the higher education leadership agenda Increasing executive fluency and engagement in cyber risk'.
- Eisenhardt, K. and Graebner, M. (2007) 'Theory building from cases: Opportunities and challenges', *Academy of management journal*. Available at: <http://amj.aom.org/content/50/1/25.short> (Accessed: 17 November 2016).
- Eisenhardt, K. M. and Graebner, M. E. (2007) 'Theory building from cases: Opportunities and challenges', *Academy of Management Journal*. Academy of Management, 50(1), pp. 25–32. doi: 10.5465/AMJ.2007.24160888.
- Eminağaoğlu, M., Uçar, E. and Eren, Ş. (2009) 'The positive outcomes of information security awareness training in companies - A case study', *Information Security Technical Report*. Elsevier Advanced Technology, 14(4), pp. 223–229. doi: 10.1016/j.istr.2010.05.002.
- Fairhurst, M. C. and Stephanidis, C. (1988) 'An evaluation of the information interface in the design of computer-driven aids for expressive communication', *International Journal of Bio-Medical Computing*, 23(3–4), pp. 177–189. doi: 10.1016/0020-7101(88)90012-8.
- Feltus, C., Petit, M. and Dubois, E. (2009) 'Strengthening employee's responsibility to enhance governance of IT - COBIT RACI chart case study', in *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 23–31. doi: 10.1145/1655168.1655174.
- FICA (2019) *Enhanced Reader, No. 2019/1*. Available at: <moz-extension://b63f3363-bd76-4e59-ba14-8669246e8b96/enhanced-reader.html?openApp&pdf=https%3A%2F%2Fwww.fic.gov.za%2FDocuments%2FFIC%2520Act%2520Booklet%2520202012.pdf> (Accessed: 23 February 2020).
- Filzen, K. (2001) 'Information Assurance The Human Factor', pp. 1–37.
- FindingDulcinea (2011) *On This Day: Robert Tappan Morris Becomes First Hacker Prosecuted for Spreading Virus*. Available at: <http://www.findingdulcinea.com/news/on-this-day/July-August-08/On-this-Day--Robert-Morris-Becomes-First-Hacker-Prosecuted-For-Spreading-Virus.html> (Accessed: 1 December 2019).
- Firesmith, D. (2003) *Common concepts underlying safety, security, and survivability engineering*, *Engineering*. Available at: <https://apps.dtic.mil/docs/citations/ADA421683> (Accessed: 28 May 2019).
- Flowers, L. A. et al. (2015) 'Assessing organizational culture and engaging faculty diversity in higher education', in *Positive Organizing in a Global Society: Understanding and Engaging Differences for Capacity Building and Inclusion*, pp. 163–168. doi: 10.4324/9781315794648.
- Fomin, V. V., Vries, H. J. de and Barlette, Y. (2008) 'ISO/IEC 27001 Information System

Management Standard: Exploring The Reasons for Low Adoption', in *Proceedings of The third European Conference on Management of Technology (EUROMOT)*. Available at: https://www.researchgate.net/profile/Henk_J_De_Vries/publication/228898807_ISOIEC_2701_Information_Systems_Security_Management_Standard_Exploring_the_reasons_for_low_adoption/links/0c96052b5441d2be49000000/ISO-IEC-27001-Information-Systems-Security-Manag (Accessed: 2 December 2019).

Forsey, C. (2018) *What Organizational Culture Is & Why It Matters*, HubSpot. Available at: <https://blog.hubspot.com/marketing/organizational-culture> (Accessed: 23 February 2020).

Fox, C. (2009) *Internal Document*.

Friese, S. (2014) *Qualitative data analysis with ATLAS.ti*. Available at: <https://books.google.com/books?hl=en&lr=&id=EvWGAwAAQBAJ&oi=fnd&pg=PP1&dq=Friese,+2014&ots=xcKLAXOtd&sig=szIPzZXDFfykv5bTChrN9fXyPhg> (Accessed: 18 November 2016).

Fulford, H. and Doherty, N. F. (2003) 'The application of information security policies in large UK-based organizations: An exploratory investigation', *Information Management and Computer Security*, 11(2–3), pp. 106–114. doi: 10.1108/09685220310480381.

Furnell, S. and Clarke, N. (2005) 'Organizational security culture: Embedding security awareness, education, and training', *Proceedings of the 4th World Conference on Information Security Education*, 11(Dti), pp. 67–74. Available at: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.678.9294&rep=rep1&type=pdf> (Accessed: 2 December 2019).

Gelbstein, E. (2011) 'Data Integrity—Information Security's Poor Relation', *ISACA Journal*, 6, p. 20. Available at: <http://m.isaca.org/Journal/Past-Issues/2011/Volume-6/Documents/11v6-Data-Integrity-Information-Securitys-Poor-Relation.pdf>.

Gerring, J. (2004) 'What is a case study and what is it good for?', *American Political Science Review*, 98(2), pp. 341–354. doi: 10.1017/S0003055404001182.

Gikas, C. (2010) 'A general comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards', *Information Security Journal*, 19(3), pp. 132–141. doi: 10.1080/19393551003657019.

Glaspie, H. (2018) 'Assessment of Information Security Culture in Higher Education', (2018), p. 155. Available at: <https://stars.library.ucf.edu/etd/6009> (Accessed: 4 February 2021).

Glaspie, H. W. and Karwowski, W. (2018a) 'Advances in Human Factors in Cybersecurity', 593(July). doi: 10.1007/978-3-319-60585-2.

Glaspie, H. W. and Karwowski, W. (2018b) 'Human factors in information security culture: A literature review', in *Advances in Intelligent Systems and Computing*. Springer Verlag, pp. 267–280. doi: 10.1007/978-3-319-60585-2_25.

Goosen, R. and Rudman, R. (2013a) 'The development of an integrated framework in order to address King III's IT governance principles at a strategic level', *South African Journal of Business Management*. Sabinet, 44(4), pp. 91–103. doi: 10.4102/sajbm.v44i4.171.

Goosen, R. and Rudman, R. (2013b) 'The development of an integrated framework in order to address King III's IT governance principles at a strategic level', *South African Journal of Business Management*, 44(4), pp. 91–103. doi: 10.4102/sajbm.v44i4.171.

Graham, V. F. (2011) 'The literature review: a step-by-step guide for students', *Evaluation &*

Research in Education, 24(3), pp. 224–225. doi: 10.1080/09500790.2011.583140.

Gray, B. C. (2010) '13 essential steps to integrating control frameworks'. Available at: <https://www.csoonline.com/article/2125317/13-essential-steps-to-integrating-control-frameworks.html> (Accessed: 25 March 2020).

Gray, C. (2003) 'Review: Information Security Policies, Procedures and Standards: Guidelines for Effective Information Security Management', *The Computer Bulletin*, 45(2), pp. 30–30. doi: 10.1093/combul/45.2.30-b.

Gregory, A. (2011) 'Data governance Protecting and unleashing the value of your customer data assets: Stage 1: Understanding data governance and your current data management capability', *Journal of Direct, Data and Digital Marketing Practice*. Palgrave Macmillan UK, 12(3), pp. 230–248. doi: 10.1057/dddmp.2010.41.

Gupta, M. and Sharman, R. (2008) *Handbook of research on social and organizational liabilities in information security, Handbook of Research on Social and Organizational Liabilities in Information Security*. doi: 10.4018/978-1-60566-132-2.

De Haes, S. *et al.* (2019) 'COBIT as a Framework for Enterprise Governance of IT', in: Springer, Cham, pp. 125–162. doi: 10.1007/978-3-030-25918-1_5.

De Haes, S., Van Grembergen, W. and Debreceny, R. S. (2013) 'COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities', *Journal of Information Systems*, 27(1), pp. 307–324. doi: 10.2308/isys-50422.

Hagen, J. M., Albrechtsen, E. and Hovden, J. (2008) 'Implementation and effectiveness of organizational information security measures', *Information Management and Computer Security*, 16(4), pp. 377–397. doi: 10.1108/09685220810908796.

Hamid, R. (2011) *Information Security and Ethics, Information Security and Ethics*. doi: 10.4018/978-1-59904-937-3.

Hanus, B. and Wu, Y. "Andy" (2016) 'Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective', *Information Systems Management*, 33(1), pp. 2–16. doi: 10.1080/10580530.2015.1117842.

Hasbini, M. A., Eldabi, T. and Aldallal, A. (2018) 'Investigating the information security management role in smart city organisations', *World Journal of Entrepreneurship, Management and Sustainable Development*, 14(1), pp. 86–98. doi: 10.1108/wjemdsd-07-2017-0042.

Hassan, W., Wan, B. and Widyarto, S. (2016) 'A Formulation and Development Process of Information Security Policy in Higher Education', in *Proceeding the 1st International Conference on Engineering and Applied Science (InCEAS) 2016, ISBN : 978-602-14930-8-3*, pp. 125–139. Available at: <http://digilib.ump.ac.id/files/disk1/35/jhptump-ump-gdl-wanhassanb-1722-2-017.wan-n.pdf> (Accessed: 2 December 2019).

He, W., Zha, S. and Li, L. (2013) 'Social media competitive analysis and text mining: A case study in the pizza industry', *International Journal of Information Management*, 33(3), pp. 464–472. doi: 10.1016/j.ijinfomgt.2013.01.001.

Health Insurance Reform Act (1995) *A BILL*. Available at: <moz-extension://b63f3363-bd76-4e59-ba14-8669246e8b96/enhanced-reader.html?openApp&pdf=https%3A%2F%2Fwww.govinfo.gov%2Fcontent%2Fpkg%2FBILLS-104s1028is%2Fpdf%2FBILLS-104s1028is.pdf> (Accessed: 30 March 2020).

Heitsmith, R. (2016) *63,000 Personal Records Compromised in UCF Breach*. Available at: <https://www.bitsight.com/blog/63k-personal-records-compromised-ucf-breach> (Accessed: 25 March 2020).

Hero, C. (2020) *Seven Primary Characteristics of Organizational Culture o Seven primary*. Available at: <https://www.coursehero.com/file/p9afh/Seven-Primary-Characteristics-of-Organizational-Culture-o-Seven-primary/> (Accessed: 23 February 2020).

Hina, S. and Dominic, P. D. D. (2018) 'Information security policies' compliance: a perspective for higher education institutions', *Journal of Computer Information Systems*. Taylor & Francis, 00(00), pp. 1–11. doi: 10.1080/08874417.2018.1432996.

HIPAA Guide (2018) *HIPAA for Dummies*. Available at: <https://www.hipaaguide.net/hipaa-for-dummies/> (Accessed: 30 March 2020).

Höne, K. and Eloff, J. H. P. (2002) 'What makes an effective information security policy?', *Network Security*, pp. 14–16. doi: 10.1016/S1353-4858(02)06011-7.

Hsu, C., Lee, J. N. and Straub, D. W. (2012) 'Institutional influences on information systems security innovations', *Information Systems Research*, 23(3 PART 2), pp. 918–939. doi: 10.1287/isre.1110.0393.

Humer, C. and Finkle, J. (2014) 'Your medical record is worth more to hackers than your credit card', *Reuters*. Available at: <https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924> (Accessed: 22 May 2019).

Hwang, S. (2008) 'Utilizing Qualitative Data Analysis Software A Review of Atlas.ti', *Social Science Computer Review*, 26(4), pp. 519–527. doi: 10.1177/0894439307312485.

IDSA (2019) *Enhanced Reader, No. 2019/1*. Available at: moz-extension://b63f3363-bd76-4e59-ba14-8669246e8b96/enhanced-reader.html?openApp&pdf=https%3A%2F%2Fcdn.ymaws.com%2Fwww.iodsa.co.za%2Fresource%2Fresmgr%2Fking_iii%2FKing_Report_on_Governance_fo.pdf (Accessed: 23 February 2020).

IFIP (2004) *Security and Protection in Information Processing Systems, Security and Protection in Information Processing Systems*. doi: 10.1007/b98992.

intellectsoft (2017) *COBIT vs ITIL: Selecting The Right IT Governance Framework*. Available at: <https://www.intellectsoft.net/blog/cobit-vs-til/> (Accessed: 2 December 2019).

Isaca (2012) 'COBIT 5 for information security', *Information Systems Audit and Control Association*.

Ismail, W. B. W. *et al.* (2017) 'A generic framework for information security policy development', in *International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*. IEEE, pp. 1–6. doi: 10.1109/EECSI.2017.8239132.

ISO/IEC (2016) 'ISO/IEC 27000:2016(E) Information technology — Security techniques — Information security management systems — Overview and vocabulary', *ISO.org [Online]*, p. 42. Available at: <https://www.iso.org/standard/63411.html> (Accessed: 1 December 2019).

ISO (2005) *Information Security based on ISO 27001/ISO 27002 - Alan Calder - Google Books*. Available at: https://books.google.co.za/books?hl=en&lr=&id=DN1EBAAQBAJ&oi=fnd&pg=PT11&dq=ISO+27002:2005&ots=QlwgzjFLuG&sig=vCiwq_bojQQ0G8UmVDofJzF8CI0#v=onepage&q=l

SO 27002%3A2005&f=false (Accessed: 28 May 2019).

ISO (2013) 'ISO 27001 - Information security management', *Iso.Org*. Available at: <https://www.itgovernance.co.uk/iso27001> (Accessed: 1 December 2019).

Israel, D. and Perry, J. (1991) *What is information?* Available at: https://www.researchgate.net/profile/John_Perry/publication/311693174_What_is_information_in_Philip_Hanson/links/585977de08ae64cb3d494112/What-is-information-in-Philip-Hanson.pdf (Accessed: 1 December 2019).

Jacobsen, D. M. (2000) (2000) 'Jacobsen, D.M. (2000). ACEC2000 paper, Melbourne Australia'. Available at: <https://people.ucalgary.ca/~dmjacobs/acec/> (Accessed: 19 February 2020).

Jagruti, P. (2008) 'INFORMATION SECURITY FRAMEWORK: CASE STUDY OF A Manufacturing Organization', *دلجمل* 49(1), pp. 69–73. doi: 10.11113/jt.v56.60.

Janesick, V. (2000) 'The Choreography of Qualitative Research Design: Minuets, Improvisations, and Crystallization', in *Handbook of Qualitative Research*, pp. 379–399. Available at: <https://ci.nii.ac.jp/naid/10008644813/> (Accessed: 19 February 2020).

Jennifer, R. (2000) *Using Case Studies in Research, Management Research News*. Available at: <http://www.emeraldinsight.com/doi/pdf/10.1108/01409170210782990> (Accessed: 17 November 2016).

Joshi, C. and Singh, U. K. (2017) 'Information security risks management framework – A step towards mitigating security risks in university network', *Journal of Information Security and Applications*. Elsevier Ltd, 35, pp. 128–137. doi: 10.1016/j.jisa.2017.06.006.

Jourdan, Z. *et al.* (2010) 'An Investigation Of Organizational Information Security Risk Analysis', *Journal of Service Science (JSS)*. Clute Institute, 3(2). doi: 10.19030/jss.v3i2.368.

Juan José, S. P., Eugenio, F. V. and Antonio, M. O. (2013) 'ITIL, COBIT and EFQM: Can They Work Together?', *International Journal of Combinatorial Optimization Problems and Informatics*, 4(1), pp. 54–64. Available at: <https://www.redalyc.org/pdf/2652/265225625006.pdf> (Accessed: 1 December 2019).

Judy, L. (2016) *2016 Data Breaches, Identity theft resource centre*. Available at: <https://www.identityforce.com/blog/2016-data-breaches> (Accessed: 2 December 2019).

Kairab, S. (2004) 'Information Security Standards', in *A Practical Guide to Security Assessments*. doi: 10.1201/9780203507230.ch9.

Kam, H.-J. *et al.* (2013) 'Information Security Policy Compliance in Higher Education: A Neo-Institutional Perspective', in *PACIS 2013 Proceedings*. Available at: <https://www.researchgate.net/publication/261063232> (Accessed: 21 June 2018).

Karyda, M. (2008) 'Investigating Information Security Awareness : Research and Practice Gaps Investigating Information Security Awareness : Research and Practice Gaps', *Information Security Journal: A Global Perspective*, 17(5/6), pp. 207–227. doi: 10.1080/19393550802492487.

Kaufman, J. (2016) 'Organizational Culture among Master's Colleges and Universities in the Upper Midwest', *Teacher-Scholar: The Journal of the State Comprehensive University*, 7(1), p. 2. Available at: <http://scholars.fhsu.edu/cgi/viewcontent.cgi?article=1045&context=ts> (Accessed: 2 December 2019).

- Kawulich, B. (2004) 'Qualitative Data Analysis Techniques', *Conference: RC33 (ISA)*, (January 2004), pp. 96–113.
- Kearney, P. (no date) *Paul Kearney*.
- Kelser (2019) *Everything We Know About the UConn Health Data Breach*. Available at: <https://www.kelsercorp.com/blog/everything-we-know-about-the-uconn-health-data-breach> (Accessed: 25 March 2020).
- Kessler, G. C. (2001) 'Nontechnical hurdles to implementing effective security policies', *IT Professional*, 3(2), pp. 49–52. doi: 10.1109/6294.918222.
- Khalfan, A. M. (2004) 'Information security considerations in IS/IT outsourcing projects: A descriptive case study of two sectors', *International Journal of Information Management*, 24(1), pp. 29–42. doi: 10.1016/j.ijinfomgt.2003.12.001.
- Khanna, R. (2013) 'Data breaches: The enemy within', *Computer Fraud and Security*, 2013(8), pp. 8–11. doi: 10.1016/S1361-3723(13)70071-X.
- Kim, F. (2019) 'How to Make Sense of Cybersecurity Frameworks - YouTube', in. Available at: <https://www.cuelogic.com/blog/cybersecurity-frameworks> (Accessed: 16 February 2021).
- Klein, R. H. and Luciano, E. M. (2016) 'What Influences Information Security Behavior? A Study with Brazilian Users', *Journal of Information Systems and Technology Management*, 13(3), pp. 479–496. doi: 10.4301/s1807-17752016000300007.
- Knapp, K. J. *et al.* (2009) 'Information security policy: An organizational-level process model', *Computers and Security*, 28(7), pp. 493–508. doi: 10.1016/j.cose.2009.07.001.
- De Koker, L. (2004) 'Client identification and money laundering control : perspectives on the Financial Intelligence Centre Act 38 of 2001', *Tydskrif vir die Suid-Afrikaanse Reg*, 2004(4), pp. 715–746. Available at: https://journals.co.za/content/ju_tsar/2004/4/EJC54925 (Accessed: 23 February 2020).
- Kooliyankal (2017) *10 Key Information Security Mistakes organizations Make! How to Fix Them?* Available at: <https://securereading.com/10-key-information-security-mistakes-organizations-make-how-to-fix-them/> (Accessed: 28 July 2019).
- KPMG (2013) *The five most common cyber security mistakes Management 's perspective on cyber security*. Available at: <https://assets.kpmg.com/content/dam/kpmg/pdf/2014/05/five-most-common-cyber-security-mistakes.PDF>.
- Kreicberga, L. (2010) *Internal threat to information security - countermeasures and human factor within SME, thesis*. Available at: <http://www.diva-portal.org/smash/record.jsf?pid=diva2:1019129> (Accessed: 21 June 2018).
- Kruger, H., Drevin, L. and Steyn, T. (2010) 'A vocabulary test to assess information security awareness', *Information Management & Computer Security*. Edited by S. M. Furnell. Emerald Group Publishing Limited, 18(5), pp. 316–327. doi: 10.1108/09685221011095236.
- Kumar Ranjit (2019) *Research Methodology: A Step-by-Step Guide for Beginners - Ranjit Kumar - Google Books, SAGE*. Available at: <https://books.google.co.za/books?hl=en&lr=&id=J2J7DwAAQBAJ&oi=fnd&pg=PP1&dq=In+addition+to+this,+it+is+a+way+to+validate+the+rationality+behind+the+selected+research+design+and+provide+justification+for+why+it+is+appropriate+in+solving+the+selected+research> (Accessed: 19 February 2020).

- Kumar, U., Joshi, C. and Gaud, N. (2016) 'Measurement of Security Dangers in University Network', *International Journal of Computer Applications*, 155(1), pp. 6–10. doi: 10.5120/ijca2016911584.
- Kyobe, M. (2010) 'Towards a framework to guide compliance with IS security policies and regulations in a university', *Proceedings of the 2010 Information Security for South Africa Conference, ISSA 2010*. doi: 10.1109/ISSA.2010.5588651.
- Landoll, D. J. (2016) *Information security policies, procedures, and standards: a practitioner's reference*. Available at: <http://ebookcentral.proquest.com/lib/Bournemouth-ebooks/detail.action?docID=4542930>.
- Laudon, K. C. and Traver, C. G. (2016) 'E-commerce 2016: business. technology. society', *Global Edition*. Available at: <http://41.33.248.151/handle/123456789/4464> (Accessed: 1 December 2019).
- Lebtinen, R. (2006a) 'Computer Security Basics', *O'Reilly*, p. 470. Available at: https://books.google.com/books?hl=en&lr=&id=BtB1aBmLuLEC&oi=fnd&pg=PR17&dq=Russell+D,+Gangemi+GT.+Computer+security+basics.+United+States+of+America:+O'Reilly+%26+Associates,+Inc.%3B+1991.&ots=qW0046nkGf&sig=FHfr1P3uxTsFNYoXWXie_rIITY0 (Accessed: 1 December 2019).
- Lebtinen, R. (2006b) 'Computer Security Basics', *O'Reilly*, p. 470. Available at: https://books.google.com/books?hl=en&lr=&id=BtB1aBmLuLEC&oi=fnd&pg=PR17&dq=understanding+of+security+basics&ots=qW106_ihOi&sig=ELjIXAPAW4WvuM_742fNnmNuNi4 (Accessed: 27 March 2020).
- Lee, C., Lee, C. C. and Kim, S. (2016) 'Understanding information security stress: Focusing on the type of information security compliance activity', *Computers and Security*. Elsevier Ltd, 59, pp. 60–70. doi: 10.1016/j.cose.2016.02.004.
- Lee, K. R. (2002) 'Impacts of Information Technology on Society in the new Century', *Structure*, pp. 1–6. Available at: <https://www.zurich.ibm.com/pdf/Konsbruck.pdf>.
- Lionel, S. (2018) *Prescriptive Fiduciary Duties*.
- Liu, Y. et al. (2015) 'Personal Privacy Protection in the Era of Big Data', *Journal of Computer Research and Development*, 52(01), pp. 229–239. doi: 10.7544/issn1000-1239.2015.20131340.
- Lopes, I. M. and De Sá-Soares, F. (2010) 'Information Systems Security Policies: A survey in Portuguese Public Administration', in *Proceedings of the IADIS International Conference Information Systems 2010*, pp. 61–69. Available at: <moz-extension://b63f3363-bd76-4e59-ba14-8669246e8b96/enhanced-reader.html?openApp&pdf=https%3A%2F%2Fcore.ac.uk%2Fdownload%2Fpdf%2F153404011.pdf> (Accessed: 1 April 2020).
- Lowry, P. B. et al. (2015) 'Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust', *Information Systems Journal*. John Wiley & Sons, Ltd (10.1111), 25(3), pp. 193–273. doi: 10.1111/isj.12063.
- Lundgren, B. and Möller, N. (2017) 'Defining Information Security', *Science and Engineering Ethics*, pp. 1–23. doi: 10.1007/s11948-017-9992-1.
- Lupu, A. R. et al. (2008) 'Integrated information systems in higher education', *WSEAS*

Transactions on Computers, 7(5), pp. 473–482. Available at: https://www.researchgate.net/publication/228374779_Integrated_information_systems_in_higher_education (Accessed: 31 March 2020).

Lyon, D. (2013) *The Information Society: Issues and Illusions*. Wiley. Available at: https://books.google.co.za/books?hl=en&lr=&id=lctFAAAAQBAJ&oi=fnd&pg=PT5&dq=we+are+in+information+society&ots=vs5lsey1RG&sig=ejuJSq2o1IBIClpJ7P1sFIBy7IU&redir_esc=y#v=onepage&q=we+are+in+information+society&f=false (Accessed: 21 November 2019).

Ma, Q. and Ratnasingam, P. (2008) 'Factors Affecting the Objectives of Information Security Management'.

Marinos, L. (2011) *European Network and Information Security Agency - ENISA*. Available at: <https://resourcecentre.savethechildren.net/publishers/enisa-european-network-and-information-security-agency> (Accessed: 23 February 2020).

Marshall, B. and Wesley, F. (2016) *Virus History | HowStuffWorks*. Available at: <https://computer.howstuffworks.com/virus2.htm> (Accessed: 1 December 2019).

Mason, R. (2016) 'MIS Quarterly', 10(1), pp. 5–12.

McCaffery, P. (2010) 'The higher education manager's handbook: effective leadership and management in universities and colleges', *Mccaffery2010Higher*, p. Routledge. Available at: https://books.google.co.za/books?hl=en&lr=&id=z1KOAgAAQBAJ&oi=fnd&pg=PP1&dq=Duties+of++Management+Committee+at+the+universities+&ots=UEJrGsJED-&sig=5qos0A4JDxYMxF_c8hqGXiBIPFM&redir_esc=y#v=onepage&q=Duties+of+Management+Committee+at+the+universities&f=f (Accessed: 1 April 2020).

McCutcheon, D. M. and Meredith, J. R. (1993) 'Conducting case study research in operations management', *Journal of Operations Management*, 11(3), pp. 239–256. doi: 10.1016/0272-6963(93)90002-7.

McGrath, C., Palmgren, P. J. and Liljedahl, M. (2019) 'Twelve tips for conducting qualitative research interviews', *Medical Teacher*. Taylor and Francis Ltd, 41(9), pp. 1002–1006. doi: 10.1080/0142159X.2018.1497149.

McMillan, J. H. and Schumacher, S. (2010) 'Research in Education: Evidence-Based Inquiry, 7th Edition. MyEducationLab Series.', *Pearson*. Pearson. One Lake Street, Upper Saddle River, New Jersey 07458. Tel: 800-848-9500; Web site: <http://www.pearsoned.com/>.

Mell, P. and Grance, T. (2011) 'The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology', *Nist Special Publication*, 145, p. 7. doi: 10.1136/emj.2010.096966.

Merhout and Joseph (2015) 'Enhancing the Control Objectives for Information and Related Technologies (COBIT 5) Framework for Sustainable IT Governance', *Journal of the Midwest Association for Information Systems*, 2015(2), pp. 5–13. doi: 10.17705/3jmw.00009.

Mesthene, E. G. (2014) 'How Technology Will Shape the Future', in *Information Technology in a Democracy*. doi: 10.4159/harvard.9780674436978.c25.

Meyer, M. J. and Lambert, J. C. (2007) 'Patch Management: No Longer Just an IT Problem.', *CPA Journal*, 77(11), pp. 68–72. Available at: <http://search.proquest.com/openview/3f622e1bc19a2e3e9767f2a29e865882/1?pq-origsite=gscholar&cbl=41798> (Accessed: 27 March 2020).

Mikkelinen, N. (2015) 'Analysis of information classification best practices'. Available at:

<http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A856360&dswid=-2051> (Accessed: 22 November 2019).

Miles, M. and Huberman, A. (1994) *Qualitative data analysis: An expanded sourcebook*. Available at: https://books.google.com/books?hl=en&lr=&id=U4IU_-wJ5QEC&oi=fnd&pg=PR12&dq=Miles+and+Huberman,+1994&ots=kDZI2MQWUU&sig=yPe eeFm0IK8v9Cy0QNPvYIQgOul (Accessed: 18 November 2016).

Miller, R. and Brewer, J. (2015) 'QUALITATIVE NURSING RESEARCH', in *The A-Z of Social Research*. doi: 10.4135/9781412986281.n286.

Mohapatra, S. (2000) 'E-commerce strategy', *American Printer*, (DEC.), pp. 155–171. doi: 10.1007/978-1-4614-4142-7_7.

Morimoto, S. (2009) 'Application of COBIT to security management in information systems development', in *4th International Conference on Frontier of Computer Science and Technology, FCST 2009*, pp. 625–630. doi: 10.1109/FCST.2009.38.

Mühl, J. K. (2014) 'Research methodology', in *Contributions to Management Science*. Emerald Publishing Limited, pp. 75–100. doi: 10.1007/978-3-319-04069-1_4.

Muhlberg, H. (2019) *Without prejudice : South Africa's corporate legal magazine.*, *Without Prejudice*. JetBlue Publishers (Pty) Ltd. Available at: <https://journals.co.za/content/journal/10520/EJC-161deb3d3b> (Accessed: 2 December 2019).

Mutongi, C. and Marume, S. B. M. (2016) 'The value of an Information Policy', 21(6), pp. 92–97. doi: 10.9790/0837-2106059297.

Nair, A. (2019) *Introduction to Information Security Risk Assessment using FAIR (Factor Analysis of Information Risk)*. Available at: www.aujas.com (Accessed: 5 February 2021).

Netshakhuma, N. S. (2019) 'Assessment of a South Africa national consultative workshop on the Protection of Personal Information Act (POPIA)', *Global Knowledge, Memory and Communication*, ahead-of-p(ahead-of-print). doi: 10.1108/gkmc-02-2019-0026.

Ngqondi, T. G. (2009) 'The ISO / IEC 27002 and ISO / IEC 27799 Information Security Management Standards : A Comparative Analysis from a Healthcare Perspective', *Dissertation Magister Technology of the Nelson Mandela Metropolitan University*, pp. 1–24.

Nicho, M. and Fakhry, H. (2013) 'Using COBIT 5 for data breach prevention', *ISACA Journal*, 5, pp. 23–30. Available at: www.isaca.com. (Accessed: 26 March 2020).

NIST (2015) 'National Institute of Standards and Technology (NIST)', in, pp. 77–87.

Page, B. B. (2017) 'Exploring organizational culture for information security in healthcare organizations: A literature review', in *PICMET 2017 - Portland International Conference on Management of Engineering and Technology: Technology Management for the Interconnected World, Proceedings*. Institute of Electrical and Electronics Engineers Inc., pp. 1–8. doi: 10.23919/PICMET.2017.8125471.

PANDEY, S. K. (2012) 'A Comparative Study of Risk Assessment Methodologies for Information Systems', *Bulletin of Electrical Engineering and Informatics*, 1(2). doi: 10.12928/eei.v1i2.231.

Pardede, P. (2018) 'Identifying and Formulating the Research Problem', *Reserarch in ELT*, 1(November), pp. 1–13. Available at:

https://www.researchgate.net/publication/329179630_Identifying_and_Formulating_the_Research_Problem.

Paul, F. et al. (2019) *Computer - Time-sharing and minicomputers* | *Britannica*. Available at: <https://www.britannica.com/technology/computer/The-personal-computer-revolution> (Accessed: 1 December 2019).

Peltier, T. R. (2008) *Information Security Policies, Procedures, and Standards: Guidelines for ...* - Thomas R. Peltier - *Google Books*. Available at: https://books.google.co.za/books?id=mM_LsS-W4f4C&pg=PA21&lpg=PA21&dq=The+cornerstone+of+an+effective++information+security+architecture+is+a+well-written+policy+statement&source=bl&ots=WgX0s3jzdg&sig=ACfU3U3pH6OhgGG1MD9p9PrYBNEEIC1nDA&hl=en&sa=X&ved=2ahUK (Accessed: 1 April 2020).

Pender-Bey, G. (2016) *The Parkerian Hexad - The CIA Triad Model Expanded*, *cs.lewisu.edu*. Available at: <http://cs.lewisu.edu/mathcs/msis/projects/papers/georgiependerbey.pdf> (Accessed: 4 February 2021).

Perdana (2018) *EU General Data Protection Regulation (GDPR) An Implementation and Compliance Guide*, *Journal of Chemical Information and Modeling*. doi: 10.1017/CBO9781107415324.004.

Pham, P. L. (2019) 'The Applicability of the GDPR to the Internet of Things', *Journal of Data Protection & Privacy*, 2(3), pp. 254–263. Available at: https://www.ingentaconnect.com/content/hsp/jdpp/2019/00000002/00000003/art00008?utm_source=TrendMD&utm_medium=cpc&utm_campaign=Journal_of_Data_Protection_%2526_Privacy_TrendMD_0 (Accessed: 31 March 2020).

Pope, C. (2000) 'Qualitative research in health care: Analysing qualitative data', *BMJ*, 320(7227), pp. 114–116. doi: 10.1136/bmj.320.7227.114.

POPI (2013) *Protection of Personal Information Act 2013*, *Government Gazette*. Available at: <https://popia.co.za/> (Accessed: 30 March 2020).

Price, N. (2018) *Roles & Responsibilities of a Board of Directors for a College* | *BoardEffect*, *Board Effect Blog*. Available at: <https://www.boardeffect.com/blog/roles-responsibilities-board-directors-college-university/> (Accessed: 1 April 2020).

Pyati, A. K. (2007) 'WSIS: Whose vision of an information society?', *First Monday*, 12(SpecialIssue8). doi: 10.5210/fm.v0i0.1795.

Rahim, N. H. A. et al. (2015) 'A systematic review of approaches to assessing cybersecurity awareness', *Kybernetes*. Emerald Group Publishing Ltd., 44(4), pp. 606–622. doi: 10.1108/K-12-2014-0283.

Rahul, T. (2013) *The first computer virus was designed for an Apple computer, by a 15 year old*. Available at: <https://blogs.quickheal.com/the-first-pc-virus-was-designed-for-an-apple-computer-by-a-15-year-old/> (Accessed: 1 December 2019).

Rao, U. H. and Nayak, U. (2014a) 'Key Concepts and Principles', in *The InfoSec Handbook*. Apress, pp. 29–61. doi: 10.1007/978-1-4302-6383-8_3.

Rao, U. H. and Nayak, U. (2014b) 'The InfoSec Handbook: An Introduction to Information Security'.

- Richardson, M. (2007) 'Age of information', *New Electronics*, 40(16), pp. 49–50.
- Rivera, C. (2015) 'Cal State data breach hits nearly 80,000 students', *LA Times*, p. 3. Available at: <https://www.latimes.com/local/lanow/la-me-ln-cal-state-data-breach-20150908-story.html> (Accessed: 25 March 2020).
- Robert, L. (2014) *What is information?: Propagating organization in the biosphere, symbolsphere, technosphere and econosphere*.
- Rouyet, Ruiz, J.-I. (2008) 'CobIT as a Tool for IT Governance: between Auditing and IT Governance', *The European Journal for the Informatics Professional*, 9(1), pp. 40–43. Available at: <http://www.cepis.org/files/cepisupgrade/2008-I-rouyetruiz.pdf> (Accessed: 1 December 2019).
- Rowe, F. (2014) 'What literature review is not: Diversity, boundaries and recommendations', *European Journal of Information Systems*. Nature Publishing Group, 23(3), pp. 241–255. doi: 10.1057/ejis.2014.7.
- Rue, R., Pfleeger, S. L. and Ortiz, D. (2007) 'A Framework for Classifying and Comparing Models of Cyber Security Investment to Support Policy and Decision-Making', *Workshop on the Economics of Information Security, 2007*, (2003), pp. 1–23. Available at: http://archive.nyu.edu/bitstream/2451/15018/3/ISR_Rue+Pfleeger.doc.txt (Accessed: 1 December 2019).
- Ruighaver, Maynard and Chia (2002) 'Understanding organizational security culture', *people.eng.unimelb.edu.au*. Available at: <https://people.eng.unimelb.edu.au/seanbm/research/2003SecCultChap.pdf> (Accessed: 2 December 2019).
- Safa, N. S. *et al.* (2015) 'Information security conscious care behaviour formation in organizations', *Computers and Security*, 53, pp. 65–78. doi: 10.1016/j.cose.2015.05.012.
- Safa, N. S., Solms, R. Von and Fitcher, L. (2016) 'Human aspects of information security in organisations', *Computer Fraud and Security*, 2016(2), pp. 15–18. doi: 10.1016/S1361-3723(16)30017-3.
- SAICA (2016) *Protection of Personal Information Act*. Available at: <https://www.pwc.co.za/en/services/advisory/pop.html> (Accessed: 16 July 2018).
- Sandelowski, M. (2004) 'Using qualitative research', *Qualitative health research*. Available at: <http://qhr.sagepub.com/content/14/10/1366.short> (Accessed: 17 November 2016).
- Sari, P. K., Nurshabrina, N. and Candiwan (2016) 'Factor analysis on information security management in higher education institutions', *Proceedings of 2016 4th International Conference on Cyber and IT Service Management, CITSM 2016*. doi: 10.1109/CITSM.2016.7577518.
- Sawyer, A. (2004) 'Challenges Facing African Universities: Selected Issues', *African Studies Review*, 47(1), pp. 1–59. doi: 10.1017/S0002020600026986.
- Scharnick, N., Gerber, M. and Fitcher, L. (2016) 'Review of data storage protection approaches for POPI compliance', in *2016 Information Security for South Africa - Proceedings of the 2016 ISSA Conference*, pp. 48–55. doi: 10.1109/ISSA.2016.7802928.
- Seale, C. (1999) 'Quality in qualitative research', *Qualitative inquiry*. Available at: <http://qix.sagepub.com/content/5/4/465.short> (Accessed: 18 November 2016).

Shah, S. and Mehtre, B. M. (2015) 'An overview of vulnerability assessment and penetration testing techniques', *Journal of Computer Virology and Hacking Techniques*. Springer-Verlag France, 11(1), pp. 27–49. doi: 10.1007/s11416-014-0231-x.

Silowash, G. et al. (2012) *Common Sense Guide to Mitigating Threats, CERT Program*. Available at: <http://www.sei.cmu.edu> (Accessed: 27 March 2020).

Singh, M. (2002) 'E-services and their role in B2C e-commerce', *Managing Service Quality: An International Journal*, 12(6), pp. 434–446. doi: 10.1108/09604520210451911.

Smart, J. C. and St. John, E. P. (1996) 'Organizational culture and effectiveness in higher education: A test of the "culture type" and "strong culture" hypotheses', *Educational Evaluation and Policy Analysis*, 18(3), pp. 219–241. doi: 10.3102/01623737018003219.

Solms, R. Von, Solms, S. H. Von and Caelli, W. J. (1993) 'A Model for Information Security Management', *Information Management & Computer Security*, 1(3), pp. 12–17. doi: 10.1108/09685229310041893.

Spinuzzi, C. I. (1997) 'Context and consciousness: Activity theory and human-computer interaction', *Computers and Composition*, 14(2), pp. 301–304. doi: 10.1016/S8755-4615(97)90030-X.

Sporn, B. (1996a) 'Managing university culture: An analysis of the relationship between institutional culture and management approaches', *Higher Education*, 32(1), pp. 41–61. doi: 10.1007/BF00139217.

Sporn, B. (1996b) 'Managing university culture: An analysis of the relationship between institutional culture and management approaches', *Higher Education*, 32(1), pp. 41–61. doi: 10.1007/BF00139217.

Stake, R. E. (1978) 'The Case Study Method in Social Inquiry', *Educational Researcher*. Sage Publications Sage CA: Thousand Oaks, CA, 7(2), pp. 5–8. doi: 10.3102/0013189X007002005.

Staunton, C., Slokenberga, S. and Mascalzoni, D. (2019) 'The GDPR and the research exemption: considerations on the necessary safeguards for research biobanks', *European Journal of Human Genetics*. Nature Publishing Group, 27(8), pp. 1159–1167. doi: 10.1038/s41431-019-0386-5.

Staunton and De Stadler, E. (2019) 'Protection of personal information act no. 4 of 2013: Implications for biobanks', *South African Medical Journal*. South African Medical Association, 109(4), pp. 232–234. doi: 10.7196/SAMJ.2019.v109i4.13617.

Stoneburner, G., Goguen, A. and Alexis, F. (2006) 'Risk Management Guide for Information Technology Systems', *Expert Opinion on Therapeutic Targets*, 10(2), pp. 289–302. doi: 10.1517/14728222.10.2.289.

Straub, D. W., Goodman, S. and Baskerville, R. (2008) 'Framing the information security process in modern society', *Information security: policy, processes and practices*, pp. 5–12. Available at: [https://repository.unikom.ac.id/49892/1/%5Bstraub%5D Information Security.pdf#page=16](https://repository.unikom.ac.id/49892/1/%5Bstraub%5D%20Information%20Security.pdf#page=16).

Stuckey, H. (2013) 'Three types of interviews: Qualitative research methods in social health', *Journal of Social Health and Diabetes*. Georg Thieme Verlag KG, 01(02), pp. 056–059. doi: 10.4103/2321-0656.115294.

Suganthy, A. and Maiti, M. (2014) 'Information Security Evolution, Impact and Design

- Factors', *International Journal of Computer Applications*, 100(2), pp. 14–19. doi: 10.5120/17496-8028.
- Sulaiman, H. A. *et al.* (2016) 'Advanced computer and communication engineering technology: Proceedings of ICOCOE 2015', in *Lecture Notes in Electrical Engineering*. doi: 10.1007/978-3-319-24584-3.
- Susanto, H. *et al.* (2011) 'I-SolFramework Views on ISO 27001 Information Security Management System: Refinement Integrated Solution's Six Domains'. Available at: <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.674.1388> (Accessed: 2 December 2019).
- Talabis, M. and Martin, J. (2012a) 'Information Security Risk Assessment: Data Analysis', in *Information Security Risk Assessments*. Syngress/Elsevier, pp. 105–146. doi: 10.1016/b978-1-59-749735-0.00004-x.
- Talabis, M. and Martin, J. (2012b) *Information Security Risk Assessments 1, Elsevier*.
- Talabis, M. R. M. and Martin, J. (2012) *Information security risk assessment toolkit : practical assessments through data collection and data analysis*. Syngress. Available at: https://www.academia.edu/37872885/Information_Security_Risk_Assessment_Toolkit?auto=download (Accessed: 2 December 2019).
- Tang, M., Li, M. and Zhang, T. (2016) 'The impacts of organizational culture on information security culture: a case study', *Information Technology and Management*, 17(2), pp. 179–186. doi: 10.1007/s10799-015-0252-2.
- Taylor, J. (2012) 'Doing Your Literature Review – Traditional and Systematic Techniques Jill K Jesson Doing Your Literature Review – Traditional and Systematic Techniques.', *Nurse Researcher*, 19(4), pp. 45–45. doi: 10.7748/nr.19.4.45.s7.
- Teferra, D. (2013) 'Funding Higher Education in Africa: State, Trends and Perspectives', *Jhea/Resa*, 11(1&2), pp. 19–51. Available at: moz-extension://b63f3363-bd76-4e59-ba14-8669246e8b96/enhanced-reader.html?openApp&pdf=https%3A%2F%2Fwww.jstor.org%2Fstable%2Fpdf%2Fjhigheducafri.11.1-2.19.pdf%3Fcasa_token%3Dd9F5UysUnAgAAAA%3AGYHu01JkNJGUTru-u2RMLea24qOeJfySqYSMsfh35jQX5YxO__uAl-mwyqj2-O (Accessed: 31 March 2020).
- Teferra, D. and Altbach, P. G. (2004) 'African higher education: Challenges for the 21st century', *Higher Education*. Kluwer Academic Publishers, 47(1), pp. 21–50. doi: 10.1023/B:HIGH.0000009822.49980.30.
- Tellis, W. M. (1997) 'Introduction to Case Study', *The Qualitative Report*, 3(2), pp. 1–14. doi: 10.1016/j.jvolgeoes.2009.02.004.
- Terroza, A. K. S. (2015) 'Information Security Management System (ISMS) Overview', *The Institute of Internal Auditors*, (May), p. 30. doi: 10.2514/6.2001-1370.
- The Pell Institute for the Study of Opportunity in Higher Education (2018) 'Analyze Qualitative Data « Pell Institute'. Available at: <http://toolkit.pellinstitute.org/evaluation-guide/analyze/analyze-qualitative-data/> (Accessed: 1 May 2020).
- Thomas, G. (2017) 'Progress in Social and Educational Inquiry Through Case Study: Generalization or Explanation?', *Clinical Social Work Journal*. Springer New York LLC, 45(3), pp. 253–260. doi: 10.1007/s10615-016-0597-y.
- Thomas, P. (2016) 'Information Security Policies, Producere, and Standards Guidelines for

effective Information Security Management.’, *The ABCs of IP Addressing*. doi: 10.1201/9781420031539.

Thomson, M. E. and Von Solms, R. (1998) ‘Information security awareness: Educating your users effectively’, *Information Management and Computer Security*, 6(4), pp. 167–173. doi: 10.1108/09685229810227649.

Tiffin, N., George, A. and Lefevre, A. E. (2019) ‘How to use relevant data for maximal benefit with minimal risk: Digital health data governance to protect vulnerable populations in low-income and middle-income countries’, *BMJ Global Health*, 4(2), p. 1395. doi: 10.1136/bmjgh-2019-001395.

Torres, J. M. *et al.* (2006) ‘Managing Information Systems Security: Critical Success Factors and Indicators to Measure Effectiveness’, in: Springer, Berlin, Heidelberg, pp. 530–545. doi: 10.1007/11836810_38.

Turner, D. W. (2010) ‘Qualitative interview design: A practical guide for novice investigators’, *Qualitative Report*, 15(3), pp. 754–760. Available at: [moz-extension://b63f3363-bd76-4e59-ba14-8669246e8b96/enhanced-reader.html?openApp&pdf=https%3A%2F%2Fwww.nixdell.com%2Fclasses%2FHCI-and-Design-Spring-2017%2FQualitative-Interview-Design.pdf](https://www.nixdell.com/classes/FHCI-and-Design-Spring-2017/Qualitative-Interview-Design.pdf) (Accessed: 20 February 2020).

VAHTI (2009) *Effective Information Security*. Available at: http://www.vm.fi/vm/en/04_publications_and_documents/01_publications/05_government_information_management/20090629Effect/name.jsp.

Varney, M. (2017) ‘European controls on member state promotion and regulation of public service broadcasting and broadcasting standards’, in *Free Speech in the New Media*. Taylor and Francis, pp. 291–318. doi: 10.4324/9781315255026-16.

Vectra (2017) ‘Protecting higher education networks from cyber threats’.

Da Veiga, A. and Eloff, J. H. P. (2007) ‘Information Systems Management An Information Security Governance Framework’, *Information Systems Management*, 24(4), pp. 361–372. doi: 10.1080/10580530701586136.

Veiga, A. and Eloff, J. (2019) ‘Information Security Governance: A Case Study of the Strategic Context of Information Security’, *Computers & Security*, 29(2), pp. 519–530. doi: 10.3390/fi8030030.

Verry, J. (2012) *How much does ISO 27001 Certification Cost?*, *PivotPoint Security*. Available at: <https://www.pivotpointsecurity.com/blog/iso-27001-cost-estimate-48000-information-security-confidence-priceless/> (Accessed: 23 February 2020).

Violino, B. (2010) ‘IT Risk Assessment Frameworks: Real-world Experience’, *CSO Online*, pp. 1–5. Available at: <https://www.csoonline.com/article/2125140/it-risk-assessment-frameworks-real-world-experience.html> (Accessed: 2 December 2019).

Vollmer, N. (2018) ‘Recital 14 EU General Data Protection Regulation (EU-GDPR)’. SecureDataService.

Vyas, A. V. (2015) ‘An Analytical Study of FDI in India’, *International Journal of Scientific and Research Publications*, 5(1), pp. 2250–3153. Available at: <http://www.indianresearchjournals.com/pdf/IJSSIR/2013/August/4.pdf> (Accessed: 19 February 2020).

Walter, R. (2015) ‘Cyber attacks on US companies since November 2014’, *The Heritage*

Foundation, 4487(4487).

Warwick, A. (2018) 'Top 10 cyber crime stories of 2018'.

Watuthu, S. N., Kimwele, M. and Okeyo, G. (2015) *The Key Issues Surrounding Electronic Commerce Information Security Management, International Journal of Soft Computing and Engineering (IJSCE)*.

Webster, J. (2002) '&R. Watson (2002). "Analyzing the Past to Prepare for the Future: Writing a Literature Review."', *MIS Quarterly*, 26(2), pp. 13–23. Available at: https://www.jstor.org/stable/4132319?casa_token=jlyqYkt9yQoAAAAA:_-4d7zmonB6koe-NkZw3K18Ry2y6xs45Cn9eif157oda8Pets8e_xghewUut1uthBvH8KL_659-t6x-n3aUQ3VCL9IQ9zS09m2Nb98srsjhQz_Zy8lw&seq=1#metadata_info_tab_contents (Accessed: 1 December 2019).

Weick, K. E. (1976) 'Educational Organizations as Loosely Coupled Systems', *Administrative Science Quarterly*, 21(1), p. 1. doi: 10.2307/2391875.

Whiting, L. S. (2008) 'Semi-structured interviews: guidance for novice researchers.', *Nursing standard (Royal College of Nursing (Great Britain) : 1987)*, 22(23), pp. 35–40. doi: 10.7748/ns2008.02.22.23.35.c6420.

Whitman, M. E. and Mattord, H. J. (2012) 'Principles of Information Security', *Cengage Learning*, p. 658.

Williams, B. L. (2016) *Information Security Policy Development for Compliance, Information Security Policy Development for Compliance*. doi: 10.1201/b13922.

Winkler, V. (J. R. . (2011) 'Security Criteria: Selecting an External Cloud Provider', in *Securing the Cloud*. Syngress, pp. 211–232. doi: 10.1016/b978-1-59749-592-9.00008-7.

Yazdanmehr, A. and Wang, J. (2016) 'Employees' information security policy compliance: A norm activation perspective', *Decision Support Systems*. Elsevier B.V., 92, pp. 36–46. doi: 10.1016/j.dss.2016.09.009.

Yin, R. K. (2003) 'Case study methodology R.K. Yin (2003, 3rd edition). Case Study Research design and methods. Sage, Thousand Oaks (CA)..pdf', in *Case Study Research: design and methods*, pp. 19–39; 96–106.

Yu, F., Peng, G. and Leng, X. (2010) *Research on Security Policy and Framework, Proceedings of the Second International Symposium on Networking and Network Security (ISNNS '10)*. Available at: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.403.5671&rep=rep1&type=pdf#page=224> (Accessed: 2 December 2019).

Zadelhoff, M. van (2016) 'The Biggest Cybersecurity Threats Are Inside Your Company', *Hbr*, pp. 2–5. Available at: <https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company> (Accessed: 23 February 2020).

Zafar, H. and Clark, J. G. (2009) 'Communications of the Association for Information Systems Current State of Information Security Research In IS', 24(34), pp. 557–596. doi: 10.17705/1CAIS.02434.

Zecurion (2017) *Top Breaches in Higher Education in 2015 -2016 | Zecurion*. Available at: <http://zecurion.com/2016/05/24/top-breaches-in-higher-education-in-2015-2016/> (Accessed: 17 November 2017).

Appendix 1

Proposed Information Security Policy

Background

The cornerstone of an effective information security architecture is a well-written policy statement (Bacik, 2008; Gupta and Sharman, 2008; Peltier, 2008; Lopes and De Sá-Soares, 2010). This is the source from which all other directives, procedures, guidelines, and additional supporting documents will be derived (Peltier, 2008). The information security policy is the foundation on which all other security measures and controls are built, and as such, the development of a strong information security policy should be prioritised (Gupta and Sharman, 2008). An established information security policy will define internal and external functions of an organization (Knapp *et al.*, 2009).

The internal functions inform employees what is expected of them and how their actions will be assessed. While the external functions demonstrate the organizations understanding that the protection of information assets is vital to the successful execution of its mandate.

The following chapter contains a proposed information security policy for biomedical or clinical research institutes which collect, store, and process sensitive and confidential Personal Health Information (PHI). This proposed policy is aimed at covering all critical aspects of data protection that biomedical researchers may require to comply with both national and international data protection regulations.

Policy Summary

The proposed information security policy is intended to assist biomedical researchers at Higher Education Institutions to protect sensitive and highly confidential research data from unauthorized access, usage, alteration, disclosure, disruption, recording or destruction. To achieve this, the proposed policy was formed with extensive insights from the well-known information security standards (such as ISO 27001:2013, NIST and HIPPA). Information that applies to biomedical research and its associated fields, was extracted and used to develop this policy. For simplicity, this proposed policy is grouped into three major parts namely A, B and C.

Part A addresses information security issues related to biomedical or clinical workstations which may cause a significant disruption of operational processes, leading to disturbance of computer-supported operations, compromised confidentiality of sensitive information, and diminished integrity of critical data.

Part B of the policy addresses issues related data protection during the data collection and processing phase. This part of the proposed policy outlines data protection morals and licit requirements that need to be observed by the biomedical or clinical research personnel when processing and sharing sensitive or biomedical data.

Part C of this proposed policy focuses on the use and disposal of electronic media devices containing sensitive information.

In addition to the potential benefits of this proposed policy to the biomedical researchers, the same policy has some business-related benefits which are highlighted below;

1. An assurance that biomedical research data and information will be secure and managed correctly.
2. An assurance that biomedical institutes are providing solutions to health-related issues in a secured and trusted environment which also helps in the management of information.
3. An assurance that sensitive and confidential information will only be accessible to authorized individuals.
4. It elucidates individual responsibilities expected of a researcher working on sensitive biomedical data with regards to information security.
5. It is a demonstration of best practice in information security

I. Policy

1. This policy is designed for biomedical researchers at Higher Education Institutions to secure and protect biomedical information, as defined hereinafter, in all its forms (written, printed or electronically recorded). Sensitive information must be protected from any form of danger, whether accidental or intentional, unauthorized alteration, destruction, exposure or breach throughout the data life cycle. This protection covers an appropriate level of security that is in line with both local and international standards over the use of software and equipment used to collect, store, process and transfer sensitive and confidential information.
2. All the requirements and limiting control or measures defined in this policy should be applied to network infrastructures, databases, encryption, reports (both in hard copies or in electronic format), and other forms which are shared and presented across all data transmission devices.
3. The policy should be made available to relevant stakeholders, as described herein, to aid the implementation processes and compliance. Moreover, it must be adhered to in order to protect the confidentiality, integrity, and availability of biomedical data.

II. Scope

1. The scope of the proposed information security policy for biomedical researchers covers the protection of confidentiality, integrity and availability of biomedical data and information.
2. The proposed policy is intended for application in biomedical and related institutes or organizations, and all involved people as defined hereinafter.
3. The policy and standards stated in this policy should be applied to protect health information and other classes of data in any format as defined in the information classification section.

III. Information Security Definitions:

1. **Availability:** Confidential data or information is accessible and usable upon request by an authorized person.

2. **Confidentiality:** Sensitive data or information is not made available or disclosed to unauthorized persons or processes.
3. **Integrity:** Data or information has not been altered or destroyed in an unauthorized manner.
4. **Involved Persons:** All the stakeholders working at any biomedical or clinical institute, irrespective of status. This includes, but is not limited to, the directors, biomedical researchers, research students, postdoctoral fellows, intern students, contract employees and volunteers. Moreover, clients and their users are also involved persons. This includes patients, research participants and so forth.
5. **Involved Systems:** All computer equipment and network systems that are operated within biomedical research labs or departments. This includes but not limited to all platforms (operating systems), all computer sizes (personal digital assistants, desktops, laptops), and all applications and data (whether developed in-house or licensed from third parties) contained on those systems.
6. **Protected Health Information (PHI):** PHI is health information, including demographic information, genomic data (DNA and RNA) and other data which could be used to identify an individual and which is created or received by the biomedical institute related to the past, present, or future physical or mental health of the individual.
7. **Risk:** (1) The probability of a loss of confidentiality, integrity, or availability of information resources. (2) A combination of the likelihood of a hazard occurring and the severity of the consequences should it occur; (3) an expression of the possibility and impact of an unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment in terms of potential severity and probability of occurrence.
8. **Vulnerability:** A weakness in a system that can be exploited to violate the system's intended behaviour relative to safety, security, reliability, availability, and integrity.
9. **Threat:** The potential danger that vulnerability may be exploited intentionally, triggered accidentally, or otherwise exercised.
10. **Hazard:** a source of potential harm.

11. **Asset:** A resource, process, product, or system that has some value to an organization and must, therefore, be protected.
12. **Personal data:** Data relating to a natural person (data subject) who can be identified by reference to an identifier such as a name, an identification number and location data (amongst others).
13. **Sensitive personal data:** Information relating to an individual's racial or ethnic origin; political opinions; religious beliefs; trade union membership; health data; sexual life; genetic data; biometric data and criminal offenses.
14. **Pseudonymized data which can also be referred to as de-identified data** (these are still personal data): Personal data that can no longer be attributed to a specific data subject without the use of additional information; this additional information must be kept separately.
15. **Anonymized data which can also be called de-linked data** (these are not personal data anymore): Information that does not relate to an identified or identifiable individual or personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

IV. Definition of different categories of information

A. Protected Health Information (PHI)

PHI is information, whether oral or recorded in any form or medium, that (a) is created or received by an individual, or group of biomedical researchers, clinical practitioners, healthcare provider, health plan, public health authority, employer, life insurer, school or university; (b) relates to past, present or future physical or mental health or condition of an individual and the provision of health care to an individual; and (c) includes demographic data, that permits the identification of an individual or could reasonably be used to identify an individual.

Therefore, unauthorized or improper disclosure, modification, or destruction of this information would violate both national and international health information confidentiality laws. Moreover, it can result in illicit penalties, and cause serious reputational damage, and disciplinary action on the institution and its collaborators,

B. Confidential Information

Confidential Information is important and highly sensitive material that is not classified as PHI. This information is private or otherwise sensitive in nature and is restricted to only those with

a legitimate and approved need for access. Examples of Confidential Information may include personnel information of the research participants, key financial information, system access passwords, and information file encryption keys.

Therefore, unauthorized disclosure of this information to people without a legitimate need for access may violate both national and international data regulation laws, and result in significant issues for both institutions and their respective collaborators. Decisions about the provision of access to this type of information must always be cleared through the top managements of the institution or the Board of Directors

C. Public Information

Information classified under this classification can be disclosed or disseminated with minimal restrictions on the content, audience or time of publication. In other words, information classified under this category can be disclosed outside the biomedical institute territory. However, it must have been approved by the information owner and information security officer or custodian as public information. Moreover, the disclosure of the information must not violate any applicable laws or regulations such as privacy. Also, modification is prohibited except for those who have been explicitly approved by information owners to modify such information.

D. Internal Information

Internal Information can be disclosed or disseminated by its owner to appropriate members, such as collaborators, business or technical partners, affiliated organizations, and other individuals, as appropriate by information owners without any restrictions on content or time of publication. This category of information can also be widely distributed among staff members, research colleagues or students within the institute without advanced permission from the information owner. However, unauthorized disclosure of this class of information is highly prohibited. Examples of internal information may include personal directories, internal policies and procedures, most internal electronic mail messages. Any information that is not classified as PHI, Confidential or Public should by default be classified as internal information.

V. Information Security Responsibilities

1. **Information Security Management Team (ISMT):** It would be worthwhile for biomedical institutes to have an Information Security Management Team. The team would consist of members with both biological, ethics and IT security background to bridge the gaps between Information technologists and biomedical researchers. These

teams will be responsible for the development and implementation of prudent security policies, procedures, and controls, subject to the approval of the management of the biomedical or clinical institutes and in line with funder requirements. The Information Security Management Team will also serve the role of custodian and user management in information security. Some of the specific responsibilities of the information officer at the biomedical or clinical institution will be;

- a) Ensuring that security policies, procedures, and standards are in place and adhered to by all the stakeholders at the institution.
- b) Providing basic security support for all systems, biomedical researchers, staff, and users.
- c) Advising on the identification and classification of data resources.
- d) Advising systems development and application developers in the implementation of security controls for information on systems, from the point of system design, through testing and production implementation.
- e) Providing consistent information security awareness training and education for biomedical researchers and other stakeholders.
- f) Performing security assessments and audits.
- g) Reporting regularly to other colleagues in the IT department, board executive and top management on the institution's status concerning information security.

2. **Information Custodian:** The owner of a collection of information is the biomedical researcher who is responsible for the creation of that information or the primary user of that information. He or she decides when and how information is released or made available to third party information processing organizations. He or she should be responsible for the integrity of the data and therefore has the responsibility to review lists of users with access to data with approval by an ISMT. However, information owners should be responsible for assigning specific classification data, while ISMT design, implement, and manage appropriate controls. Therefore, an effective data classification scheme should be established. In addition to this, the following are some of the specific responsibilities of information owner.

1. Knowing the information for which it is responsible

2. Determining a data retention period for the information, based on appropriate legal advice or institution policy.
 3. Ensuring appropriate procedures are in effect to protect the integrity, confidentiality, and availability of the information used or created within the institute.
 4. Reporting promptly to the appropriate people if there is a loss or misuse of the information to start corrective action
- 3. Biomedical or Clinical Institutions:** Any organization (either private or public) established to provide health research intended to produce knowledge valuable for understanding human disease, preventing and treating illness, and promoting health. This include medical faculty at the universities, academic health centres, private and public clinical research institutes, contract research organizations, health survey research organizations, federal government intramural research programs.

Section A of the Proposed Information Security Policy

The purpose of this part of the proposed policy is to establish a healthy security culture among biomedical researchers in the workplace. It has been demonstrated that in any organizational system, human behaviour and attitude towards security has been the main factor resulting in information security hazards. For that reason, this part of the policy was proposed to addresses all security concerns related to the biomedical workstations. Such concerns includes; physical and environmental control (e.g. prevention of unauthorized physical access, theft), information security and monitoring, incident management, software security, security training, and risk assessment and auditing.

Therefore, security culture is directed to human behaviour and it is expected that relevant biomedical staff and users familiarise themselves with the guidelines of this policy and conduct activities in a responsible manner.

1. Proposed policy on Physical and Environmental Control

Overview

Physical and environmental security addresses all aspects related to the prevention of unauthorized physical access, theft, damage and interference with information and IT systems /assets, which may result in business disruption and/or security breach (ISO 27001, 2013).

This section of the information security policy is an essential part of the information security management system (ISMS) especially if the organization would like to achieve certification such as ISO 27001 certification (ISO 27001, 2013).

Policy Statement

- i. A list of all sensitive areas should be maintained by the ISMT. Sensitive areas should be defined and marked as 'Restricted' area (such as inbuilt data centre premises or other critical IT infrastructure premises where sensitive information is stored or area information classified as internal, PII, confidential is stored or processed).
- ii. Appropriate access control devices should be installed for such restricted areas, and appropriate access level authorisation should be provided to employees and non-employees.
- iii. External visibility of the sensitive areas should be avoided where possible.
- iv. Incoming and outgoing IT equipment should be checked and registered.
- v. Information and Communication Services of the university should identify the location of the physical assets within the clinical or biomedical institute and inform security of this, through a well-documented procedure.
- vi. Any incident relating to physical security breach resulting in unauthorized access to an information asset should be recorded, investigated and the appropriate corrective action recommendations must be implemented.
- vii. Users who make use of mobile computing devices must ensure the physical safety of these devices at all times.
- viii. During extended periods away from a workspace, such as a lunch break, all sensitive working documents should be kept in locked drawers, and laptops should be shut down or placed in locked mode.
- ix. Infrastructure such as electrical, telecommunication and data cabling should be protected from theft and damage. The minimal distance between power and data cables shall be maintained as per best practices according to Cisco recommendations (Cisco, 2014).
- x. Important information assets should be maintained according to a preventative maintenance schedule to ensure their continued integrity and availability.

- xii. At the end of the working day, the employees must ensure all documents containing sensitive or confidential information are safely and securely stored.

2. Proposed Policy on information security Incident Monitoring, Management and Risk Assessment at the Biomedical Workstations

Overview

An effective control program for information security and business continuity requires a well-defined monitoring process (Krell, 2006). To ensure information security and business continuity, biomedical institutes have to be aware of the risks that face their information assets (Gray, 2003; Da Veiga and Eloff, 2007), which may lead to a significant disruption of critical operational processes, leading to disturbance of computer-supported operations, compromised confidentiality of sensitive information, and diminished integrity of critical data.

The objective of this proposed Information Security Policy is to ensure business continuity of biomedical or clinical institutions to decrease the risk of damage by monitoring, preventing or mitigating security incidents. This policy also defines the formal security organization structure that biomedical institutes could adopt with clearly well-defined roles, responsibilities, and accountability.

Policy Statement

- i. Information Communication Services (ICS) department (or any related department that performs the same duties as ICS) within an institution should collaborate with the biomedical or clinical department to give a clear directive with regards to management and IT support for information security initiatives, maintaining the commitment to information security policies by the biomedical staff and users, and providing advice during implementation.
- ii. Information Communication Services (ICS) should build or create an Information Security Management Team (ISMT) whose members have both biological and IT background. Their responsibilities should include (but are not limited to), documenting threats, risks and vulnerabilities, analysing identified threats and assessing the impacts on the organization, suggesting how such threats would be mitigated or controlled within the biomedical department or institute.
- iii. The ISMT should also ensure that;
 - a. Information and Information Systems are protected against any unauthorized access.

- b. Confidentiality, Integrity, and Availability of information and information systems for business processes of the biomedical or clinical department are maintained
 - c. Involved persons within the biomedical department or institute (irrespective of status) conform to rules and regulations of protecting sensitive information.
 - d. Consistent Information Security Awareness Training is available to all stakeholders.
 - e. All actual, or suspected, information security breaches within the institute are documented and investigated systematically.
 - f. The Information Security Management Team (ISMT) may seek specialist security advice from internal or external consultants where necessary e.g. attending information security conferences and attempting accreditation exams to update and upgrade their skills.
- iv. ISMT and ICS department will have the authority to frame, edit, update or upgrade the Information Security Policy which will be subject to approval by the Information Security Officer.
 - v. All critical devices such as servers and firewalls should be monitored and synchronized for reliable and meaningful logged information.
 - vi. List of access privileges of each authorized user for each information system and IT assets should be securely retained.
 - vii. The Information Communication Services department should be using all manners of communication techniques or skills to communicate the importance of information security to all the stakeholders. Moreover, emphasis should be made on the mandatory information security policy. Any violation or non-compliance of an information security policy by involved persons, contractors or third parties shall call for an investigation and formal disciplinary action.
 - viii. A formal information security incident management procedure should be designed, documented, implemented and maintained by the ISMT of the biomedical or clinical research institute.
 - ix. Information security incidents should be categorized, classified and prioritized to facilitate monitoring, assigning, and reporting.
 - x. All information security incidents must be reported in a timely manner to the ISMT for investigation and resolution, to avoid reoccurrence of such incidents and/or re-

established effective security control measures that will strengthen the biomedical network systems.

- xi. ISMT and ICS departments have the right to monitor, regulate and control the usage and access of all information services and facilities.
- xii. Involved personnel or information users must not disclose information security incidents with un-authorized users.
- xiii. Attempts to deter, obstruct, or interfere with reporting of actual or suspected information security incidents caused by accidental or intentional acts, should be dealt with by disciplinary action.
- xiv. Corrective actions resulting from information security incidents should be captured and communicated to all relevant teams or users.
- xv. A documented risk assessment methodology for the biomedical or clinical institute should be established, implemented and maintained. Risks should be assessed according to the probability of occurrence and impact of occurrence and a customised risk rating scale should be used to determine event tolerance
- xvi. The Risk Assessment should ensure that:
 - a) All information assets owned by the institute are covered
 - b) Existing effective information security controls are not impacted
 - c) Criticality and primacy should be defined for all assets so that corrective action plans will be implemented for sensitive information first.
- xvii. Information asset proprietors shall conduct a risk assessment for all information assets under their custodianship.
- xviii. Appropriate controls should be identified, designed and implemented to prevent or remove vulnerabilities within the biomedical settings. A risk treatment plan shall be prepared for the implementation of such controls.
- xix. The Information Security Management Team should ensure technical compliance checks like penetration testing and vulnerability assessment to identify vulnerabilities in IT systems. These assessments should be conducted periodically and when significant changes are applied to IT systems.

3. Proposed Policy on Audit, Outsourcing and Outsourcing and External Facility Management at the Biomedical Workstations

Overview

This section of the proposed policy provides the authority to the Audit Committee to conduct periodic audits to ensure compliance with ISO/IEC 27001:2013. Also, to ensure appropriate control over security exposures and risks regarding services provided by external or third parties.

Effective regulatory oversight requires the establishment of a mechanism to ensure compliance with relevant statutory registrations, contractual and regulatory obligations. The purpose of this policy is to provide a positive assurance, thereby avoiding breaches of security requirements.

Policy Statement

- i. ISMT in conjunction with the ICS department should develop an Audit procedure document, implement and maintain it for conducting periodic audits to ensure compliance to ISO 27001:2013 standards.
- ii. An Audit Committee should be established by ICS to organize periodic internal audits in the biomedical institutes to ensure compliance with clinical and biomedical security policies.
- iii. Audit reports of previous audits should be reviewed to verify the status of earlier findings of non-conformance.
- iv. Audit Committee shall submit an audit report to the ICS department after completion of each audit. Information and Communication Services department (ICS) should have managerial reviews of the audit and compliance report and ensure corrective actions for all information security incidents that are reported by the Audit Team.
- v. The biomedical Information Security Management Team (ISMT) shall take appropriate corrective and preventive actions on the findings in the audits report.
- vi. The selection or appointment of the third party for outsourcing or external facility management work will adhere to the institute's rules and regulations.
- vii. Information technology-related activities performed by external or third parties shall be assessed for security exposures and risks. Contracts with an external or third party shall be signed after all risks relating to outsourcing have been evaluated.

- viii. All outsourced contracts requiring third party access to critical information and systems of the institute should sign confidentiality agreements/non-disclosure agreements with the institute.
- ix. An agreement to comply with the Information Security policies of the biomedical or clinical institute during the exchange of information or data assets must be signed by the external or third party and appropriate penalties must be defined for noncompliance to the signed agreement.
- x. Periodic service assessment and review of all outsourced services shall be done for each service.
- xi. All external or third parties and their representatives shall inform the institute of any incidents relating to information security during the period of their contract.

4. Proposed policy on Software Installation, Patches and Security at the Biomedical Workstations

Overview

Infrequent and irregular patching and vulnerability testing may render the information technology infrastructure vulnerable to viruses and spyware, ultimately resulting in the exploitation of security weaknesses.

This section of the proposed policy aims to control the use of software in clinical or biomedical research institute settings to prevent violation of copyright, privacy, confidentiality, and license agreements.

Policy Statement

- i. Information and Communication Services in conjunction with the biomedical ISMT should establish a procedure to govern the deployment of all patches. Guidelines established in this procedure shall be strictly observed and adhered to during the installation of patches.
- ii. Patches shall be reviewed, evaluated, tested and verified for relevance and criticality before implementation. Critical patches must be installed on a priority basis and non-critical patches should be installed during planned maintenance schedules.
- iii. Only approved and licensed copies of system software and application software should be used.

- iv. Computer software developed or customized by vendors or developed in-house for the sole purposes of the biomedical or clinical research should remain the property of the institute.
- v. All applications developed or purchased for conducting biomedical operational functions should ensure the confidentiality, integrity, and availability of information in all operational processes.
- vi. Periodic audits should be conducted to determine the validity of software licenses installed on all desktops, laptops, workstations, servers and any information systems within biomedical labs and offices.
- vii. Unauthorized or pirated copies of software must be deleted/uninstalled without prior permission of the user.
- viii. All available source code and executable files of application software should be under version control. Changes to application software or operating system should be controlled through ISMT and ICS.
- ix. Original and copies of all current and archived software must be securely preserved along with related system documents and manuals.
- x. Security Patches for System and application software should be updated following IT security.
- xi. Any technical or functional vulnerabilities of the information system should be identified and addressed during the information audit and change management process.

5. Proposed Policy on Human Resources and Training at the Biomedical Workstations.

Overview

Management of human resources is the key to the success of any organization (Mak, 2006). Human resources are an asset and therefore require focused efforts, from the employee induction stage. This policy addresses the requirements of a sound human resource policy to achieve organizational objectives. Moreover, the policy outlines the minimum training for biomedical users and employees to make them aware of basic information security threats to protect both their sensitive information and that of research data on the network. This policy especially applies to the employees with access to sensitive or regulated data.

Therefore, the policy is designed to protect the organizational resources on the network and increase employee competence by establishing a policy for user training. When these categories of people are trained about basic information security and computer threats and know their roles and responsibilities they work more efficiently and are better able to protect sensitive and confidential organizational resources from unauthorized interference.

Policy Statement

- i. The roles and responsibilities related to information security should be properly defined and documented for biomedical staff.
- ii. All staff or employees of the biomedical institute should agree and sign the terms and conditions of appointment as stipulated in existing institute HR policies, including non-disclosure agreements related to sensitive and confidential information and information security policy and procedure documents, during and after the contract term.
- iii. All employees of the biomedical or clinical institute should be provided the necessary information security training to ensure that practices follow the information security policy of the biomedical institute.
- iv. The training categories should include, but not be limited to, the following fundamental areas:
 - a) Copying and storing files in a secure manner
 - b) Where to store files securely
 - c) Ways of handling sensitive data and information
 - d) Security threats on e-mail attachments
 - e) The purpose of the network drive and how to use their network drive
 - f) Protocols to be followed if a system has been compromised
 - g) Password hygiene
- v. The training should also teach the employees various malware virus infection paths which include but not limited to; email, browser, and installation of unapproved programs, how to avoid adware and spyware.
- vi. The training should also cover what E-mail viruses are, how they spread, how to identify spoofing senders, dangerous attachments, how to protect email address, and filtering spam.
- vii. There should be an official email identification for authorized employees (biomedical researcher, researcher students, post-doctoral fellow, and staff members) of the

- biomedical or clinical research institute. This email ID should be created and assigned by the ISMT or ICS team and should be strictly used for official purposes.
- viii. The decision to provide E-mail ID to non-employees will be determined by the Institution management.
 - ix. Information created, sent, or received (including E-mail messages and electronic files) via the official e-mail shall remain institution property.
 - x. In relation to (9) above, the institution, therefore, reserves the right to:
 - a) Deny an email ID of any individual or team.
 - b) Monitoring of official email communication for valid business purposes can be performed but must be clearly communicated to users in the mandatory policy agreement document.
 - c) Discard an email ID in accordance with the proposed policy on electronic media.
 - xi. The institution management may have access to all email messages whenever required it is to present to law enforcement agencies or third parties without the consent of the email user.
 - xii. Users should abide by copyright laws, ethics rules, and other applicable laws while using the institution's e-mail system.
 - xiii. Users should not use email facilities for unauthorized use. Unauthorized use of the email system includes but not limited to:
 - a) Transmitting or distributing E-mail containing offensive, provocative, insulting, abusive, or slanderous information about the institute, any other employee, client, research group or collaborator whatsoever.
 - b) Unnecessary overloading of the E-mail system (e.g. chain mail, spamming, executable graphics programs and junk mail are not allowed).
 - xiv. E-mail attachments with extensions, such as, ".exe", ".scr", ".vbs" & ".vir" etc. should be blocked by the ISC or ISMT for security reasons.
 - xv. E-mail users shall protect the right to the confidentiality of other users.
 - xvi. The use of the institution's E-mail system to solicit for commercial or personal benefit without appropriate authorization should be prohibited.
 - xvii. E-mails sent outside the organization shall have an appropriate disclaimer attached

- xviii. Users should report email security incidents as per the Information Security Incident Management Policy.
- xix. Email exchange servers and other necessary security patches should be frequently updated and installed.
- xx. Violation of Email Policy shall be investigated and may be followed by disciplinary action.
- xxi. Top management should ensure that consistent and effective IT Training is provided to biomedical researchers, staff or users periodically on the use of Email and passwords.
- xxii. All production system-level passwords must be in-line with the InfoSec administered global password management and should be changed, or expired, after 6 months. Although, the new NIST password guidelines show more 'relaxed' password hygiene, this proposed policy highly recommends that the information security password policy for biomedical data should be stricter when compared to general information security policy.
- xxiii. All user-level passwords (e.g. email, web, laptop or desktop computer, etc.) must be changed at least every 45 days. In addition, two-factor authentication is encouraged and recommended.
- xxiv. The Information and Communication Services (ICS) and Information Security Management Team (ISMT) should create a formal password management procedure for biomedical or clinical staff.
- xxv. The control must be enforced to change a temporary or default password at first log in by the user.
- xxvi. Systems Administrators must ensure all default passwords provided by the vendors are changed.
- xxvii. System Administrators should enforce appropriate password controls to ensure the use of complex passwords, change the password as required, prevent reuse of old passwords.
- xxviii. Password sharing must be prohibited, and password leakage should be viewed as an information security incident, reported, investigated and corrective action must be implemented

- xxix. Passwords should not be stored on computer systems in an unprotected form and appropriate levels of encryption must be included in password management systems.
- xxx. The characteristics of weak passwords must be documented in the password management procedure. Such passwords have the following features: less than six characters, the password is a word in the dictionary, commonly used words such as family names, pets, friends, birthday month, and computer name commands, number patterns like QWERTY, 123321.
- xxxi. As with (30) above, characteristics of strong passwords must be documented in the password management procedure. Strong passwords have the following features; both upper and lower case characters, digits and punctuation characters as well as letters e.g. 0-9,!@#\$%^&*()_+=?<>:~\, at least eight alphanumeric characters in length, not form a word in any language or dialect, is not based on personal information or stored on-line.
- xxxii. Annual performance evaluation on information security practices such as the use of Email and password management should be conducted for employees and should form part of performance measures and incentives.

Section B of the Proposed Information Security Policy

As stated earlier, data protection is crucial for biomedical or clinical researchers, particularly in the aspect of data collection, sharing and reuse of research data. Protection of this data during the data collection, processing phase and after the research study is mandatory. It protects the rights of study participants involved in the research throughout the research lifecycle. This part B of the proposed information security policy focuses on data protection standards and legal requirements that need to be respected by biomedical or clinical research personnel when processing and sharing sensitive clinical or biomedical data. Moreover, this part also define how the biomedical researcher can measure the effectiveness of the selected controls or group of controls and how these measurements are to be used to evaluate control effectiveness to produce comparable and reproductive results.

1. Proposed Policy on Data Protection and Measurement of Effectiveness Controls

Overview

This section of the proposed policy defines data protection standards and legal requirements that need to be respected by biomedical or clinical research personnel when processing and sharing sensitive clinical or biomedical data. Moreover, the policy aims to ensure that the legitimate concerns of participants regarding the use of their sensitive health data for research purposes are considered by biomedical researchers. In addition to being open and transparent, the biomedical researcher will seek to give participants as much as is reasonably possible, an informed choice over what data is held and how it is used. Similarly, biomedical or clinical researchers must at all times respect individuals' rights to their health information, maintain ethical practices, keep sensitive information secure at all times, maintain the quality of information and comply with both legal regulation (such as the GDPR and POPIA) and best practices.

Policy Statement

Whenever collecting, processing and sharing information about biomedical data or sensitive data, biomedical researchers should agree to apply the following Data Protection Principles:

- i. The data protection strategy should start at the earliest stages of the research process.
- ii. Institution guidelines must be followed with regards to ethics and informed consent
- iii. Personal data should be processed fairly and lawfully
- iv. Personal data should be obtained only for the purpose specified and should not be retained for longer than is necessary for the purpose.
- v. Data should be adequate, relevant and not excessive for the purposes required
- vi. Accurate data must be kept up to date
- vii. Appropriate technical and organizational measures must be taken against unauthorized/unlawful processing of personal data/accidental loss/destruction/danger of personal data.
- viii. Personal data and sensitive health data should not be transferred outside biomedical premises unless an adequate level of data protection is ensured, and data transfer agreements are approved.
- ix. Sensitive data must be encrypted before it is shared.

- x. Encryption methods adopted by biomedical researchers used to protect sensitive information should be approved by ISMT or ICS.
- xi. The effectiveness of cryptographic control shall be reviewed periodically.
- xii. The encryption and decryption that the biomedical researcher should employ must be in line with international standards and techniques.
- xiii. Cryptographic algorithms, keys length and key strength that will be used for protecting sensitive data or information should be appropriately chosen depending upon the classification schema of the data and the time frame for which that sensitive information is valid.
- xiv. Biomedical researchers must cooperate in information security training programs provided by the ISMT and maintain an awareness of confidentiality and data security issues at all times.
- xv. Researchers must be able to demonstrate compliance with data regulation principles. Any policies or procedures required for compliance with data protection regulations must be documented.
- xvi. Throughout the data life cycle, the researcher must take appropriate technical and organizational measures to protect personal data against unauthorized or unlawful processing of personal data and accidental loss or destruction of, or damage to, personal data.
- xvii. A documented Measurement of Effectiveness of Control Procedure should be established, implemented and maintained.

Section C of the Proposed Information Security Policy

Information exists in many forms and can be stored in a multitude of ways. Media controls are protective measures specifically designed to safeguard electronic data. This part of the proposed policy addresses the use or handling of mobile devices that contains sensitive biomedical data and information against interference by viruses and other malware. Moreover, this part of the proposed policy also focusses on the disposal of any electronic media devices containing sensitive information. Electronic Media destruction and disposal should be accomplished in an environment-friendly manner.

1. Proposed Policy on Mobile computing Devices Handling and Electronic Media Disposal

Overview

In the current complex IT environment, portable computing and communication devices are widely, and increasingly being used by individuals, including biomedical or clinical researchers (European Commission, 2009). Organizations such as the clinical research institutes, need to ensure that confidential business information is not compromised (Jules Halpern Associates, 2010), and consider risks of networking with mobile computing devices (Best, 1984; Wlosinski, 2017). This section of the proposed policy is designed to regulate the use of mobile computing devices in the clinical or biomedical research institute setting. Moreover, the policy is intended to establish a standard for the proper and secured disposal of electronic media and computing devices containing information/data to minimize the risk of information leakage to unauthorized persons.

Policy Statement

- i. Mobile computing devices include but are not limited to;
 - a) Laptops/Desktops
 - b) Mobile phones, tablets & iPods
 - c) External storage drives
 - d) Digital copywriters such as CD writers
 - e) Mobile recording devices such as tape recorders.
- ii. Use of personally owned mobile computing devices such as mobile phones, tablets, and tape recorders which are used for collection and storage of sensitive biomedical data or information for official purposes (such as research study or project) should be prohibited unless authorized with consent documents.
- iii. Mobile computing devices must be automatically logged off a network after a period of inactivity (10 to 15 minutes)
- iv. Sensitive information stored in mobile computing devices must be protected using appropriate encryption techniques.
- v. Users of mobile computing devices should ensure that sensitive and corporate information is not compromised by unauthorized access either inside or outside of office premises.

- vi. Access to the corporate information by remote users across public networks should be facilitated via a VPN (or similar networking solution) and should only be granted after successful verification, identification, and validation.
- vii. Users of mobile computing devices must ensure that:
 - a) The devices have the latest virus definitions.
 - b) They scan for malicious codes before connecting to the biomedical institute network
 - c) They must remove detected threats or malicious code, before connecting the biomedical network
 - d) Ensure that regular backups of critical information on to the server are performed
 - e) They should not leave mobile computing devices unattended.
- viii. Hardware identified for disposal, but which contains electronic media which has to not been cleared for disposal should be backed up prior to disposal.
- ix. Information Security Management Team (ISMT) of the biomedical or clinical research institute should create a procedural document outlining the standard protocols for the disposal of electronic media and computing devices. This document must be effectively implemented and adhered to. The procedure shall ensure:
 - a) All electronic media on computing devices identified for disposal shall be erased through data destruction software (e.g. data sanitization software, disk wipe software) (Tim Fisher, 2019), so that it cannot be retrieved, degaussed, or rendered usable.
 - b) Compliance with existing environmental and other applicable regulations (e.g. The International Telecommunication Union ITU (Balde et al., 2017), E-waste Regulations (Perkins *et al.*, 2014) for disposal of electronic devices and media.

2. Proposed Policy on Antivirus and Firewall

Overview

Internet connectivity can make private systems vulnerable to misuse and attack (John, 2006; Herold and Rogers, 2010). A safeguarded such as antivirus and firewall are used to control malicious codes and access between a trusted network and a less trusted one by serving as a gatekeeper between them and centralizing access control (Management, 1999, Vacca, 2007). Malicious code includes any programs (including macros and scripts) that are

deliberately coded to cause an unwanted event on a user's workstation. This includes viruses, worms, logic bombs, Trojan horses, web bugs, and in some cases spyware.

However, antivirus and firewall are both strategies for protecting an organization's internet-reachable resources. For instance, firewalls can be used to secure segments of an organization's Intranet, while antivirus can be used to block all malicious code from running.

The objective of this policy is to protect and secure biomedical information and underlying systems from potential damages caused by malicious codes and other malware. It is expected of biomedical researchers to ensure that precautions are implemented to detect and prevent the introduction of malicious code and unauthorized mobile code into sensitive information processing facilities.

Policy Statement

Where possible, it is advantageous for a biomedical department to use a single anti-virus product for antivirus protection, and this antivirus product must be installed by the ISMT. Thereafter, the following requirements should be strictly enforced for compliance.

- i. The anti-virus product providing optimal security should be configured, operated and updated in real-time on all servers and employees' computers.
- ii. The anti-virus library definitions must be updated at least once per day. Antivirus software should be configured to install automatic updates of relevant files without requiring user intervention.
- iii. Anti-virus scans on all user computers and laptops and biomedical servers must be performed weekly.
- iv. Only domain administrators are permitted to cease an anti-virus definition update.
- v. The ISMT must configure the Anti-Virus software to:
 - a) Prevent users from disabling it or modifying configuration settings.
 - b) Control virus spreading through e-mail attachments
 - c) Scan for viruses before the use of any internal/external drive, CD and any mobile computing devices.
- vi. All activities relating to virus protection should be logged, maintained and reviewed periodically.

- vii. Data and software backups must be protected from malicious code attacks.
- viii. The number of entry points to the biomedical or clinical institute's network must be restricted and secured through a firewall.
- ix. The firewall should block unwanted traffic or direct incoming traffic to more trustworthy internal systems and it should log traffic to and from the private network.
- x. The firewall should hide vulnerable systems that cannot easily be secured from the Internet. Also, the firewall should hide information such as system names, network topology, network device types, and internal user ID's from the Internet.
- xi. Users accessing the servers from an external source must only be able to gain access to sensitive data through the firewall.

Appendix 2

Supplementary Data