



**AN ANALYSIS OF CYBER-SECURITY POLICY COMPLIANCE
IN ORGANISATIONS**

by

HUGUES HERMANN OKIGUI

210051124

Thesis submitted in fulfilment of the requirement for the degree

MASTER OF TECHNOLOGY: INFORMATION TECHNOLOGY

IN THE FACULTY OF INFORMATICS AND DESIGN

AT THE CAPE PENINSULA UNIVERSITY OF TECHNOLOGY

Supervisor: Prof. Johannes Cronje

Co-supervisor: Dr. Errol Francke


Date Submitted December 2023

CPUT copyright information

The thesis may not be published either in part or as a whole unless permission has been obtained from the University

DECLARATION

I, **Hugues Hermann Okigui**, declare that the contents of this dissertation/thesis represent my own unaided work, and that the dissertation/thesis has not been previously submitted for academic examination towards any qualification. Furthermore, it represents my own opinions and not necessarily those of the Cape Peninsula University of Technology.

Signed: 

Date: 29 December 2023

ABSTRACT

In the contemporary digital landscape, cyber-attacks and incidents have placed cyber-security at the forefront of priorities in organizations. As organizations face cyber risks, it becomes imperative to implement and comply with various cyber-security policies. However, due to factors such as policy complexity and resistance from employees, compliance can be a challenging task. The study investigated the variables that affect an organization's adherence to cyber-security policies. A case study design was chosen as part of a qualitative approach to answer the research question. For data gathering, semi-structured interviews were performed, and existing documents were also considered when available to supplement interviews. The gathered data was meticulously organized, coded, and analyzed using the Actor-Network Theory perspective, with a focus on its four moments of translation: problematization, interessement, enrolment, and mobilization. The analysis revealed that insider threats and phishing attempts are the two cyber threats that affect organizations, behavioral challenges and enforcement limitations are factors influence and contribute to the non-compliance of cyber-security policy, phishing exercises and policy development process are used to enforce cyber-security policies. The study concludes that both insider Threats, involving staff or internal end-users, and Phishing Attempts perpetrated by external individuals, pose significant risks to organizations. Despite awareness initiatives, behavioral challenges persist among internal end-users, which complicate adherence to available security measures. A one-size-fit cyber-security policies are sometimes inadequate due to the diversity in business sectors, necessitating a tailored solution. Periodic phishing exercises serve to evaluate the readiness of internal end-users or staff, and identify areas for improvements. Ultimately, for effectiveness, cyber-security policies development process should follow a collaborative and inclusive approach where organization stakeholders will be participating.

ACKNOWLEDGEMENTS

I would like to express my gratitude to:

- God for the gift of health and strength, never giving up.
- My late mother for her unconditional love and unwavering support. Her encouragement and believe in my abilities have profoundly influenced my journey.
- My supervisors Prof. Johannes Cronje and Dr. Errol Francke. Your guidance, patience, kindness and commitment to assist your students has made this achievement possible.
- All my colleagues at the research forum for their valuable contributions through advice, critiques, knowledge sharing.
- Last but not least, my partner for her steadfast encouragement and emotional support. From day one, you have been by my side; this achievement is as much yours as it is mine.

TABLE OF CONTENTS

DECLARATION	ii
ABSTRACT	iii
ACKNOWLEDGEMENTS.....	iv
LIST OF TABLES	x
LIST OF FIGURES.....	xi
ACRONYMS AND ABBREVIATIONS.....	xii
CHAPTER ONE: INTRODUCTION	1
1.1 INTRODUCTION AND BACKGROUND.....	1
1.2 STATEMENT OF THE RESEARCH PROBLEM	2
1.3 AIM AND OBJECTIVES OF THE RESEACH.....	3
1.3.1 Aim of the research.....	3
1.3.2 Objectives of the research	3
1.4 RESEARCH QUESTION AND SUB-QUESTIONS.....	3
1.4.1 Main research question.....	3
1.4.2 Research sub-questions	3
1.5 DEFINITION OF TERMS	4
1.5.1 Information and communication technologies	4

1.5.2	Cyberspace	4
1.5.3	Cyber-security.....	5
1.5.4	Cyber-incident.....	5
1.5.5	Cyber-attack	5
1.5.6	Cyber-security policy.....	5
1.5.7	Actor-network theory.....	6
1.6	RESEARCH DESIGN AND METHODOLOGY	6
1.6.1	Research paradigm.....	6
1.6.2	Research approach.....	7
1.6.3	Research methodology	7
1.6.4	Research design.....	7
1.6.5	Data collection	7
1.6.6	Data analysis	7
1.7	DELINEATION OF THE RESEARCH	8
1.8	SIGNIFICANCE OF THE RESEARCH.....	8
1.9	ETHICAL CONSIDERATION	8
1.10	THE STRUCTURE OF THE STUDY.....	9
	CHAPTER TWO: LITERATURE REVIEW	11
2.1	INTRODUCTION	11

2.2	INFORMATION AND COMMUNICATION TECHNOLOGIES.....	11
2.3	CYBERSPACE AND ORGANISATIONS	13
2.4	CYBER-ATTACK AND CYBER-INCIDENT.....	14
2.5	CYBER-SECURITY IN ORGANISATIONS	15
2.6	THE GOALS OF CYBER-SECURITY	16
2.7	END-USERS.....	17
2.8	POLICY AND COMPLIANCE.....	18
2.9	ACTOR-NETWORK THEORY	19
2.10	ACTOR NETWORK THEORY AND INFORMATION SYSTEMS RESEARCH.....	22
2.11	SUMMARY	24
CHAPTER THREE: RESEARCH DESIGN AND METHODOLOGY.....		25
3.1	INTRODUCTION	25
3.2	RESEARCH PARADIGM.....	25
3.3	RESEARCH APPROACH	26
3.4	RESEARCH METHOD	27
3.5	RESEARCH DESIGN	28
3.5.1	Case overview	29
3.6	DATA COLLECTION	31
3.6.1	Participant selection criteria	31

3.6.2	Ethical considerations	31
3.6.3	Data collection technique and procedure	32
3.7	DATA ANALYSIS.....	35
3.8	SUMMARY	36
CHAPTER FOUR: DATA ANALYSIS AND FINDINGS.....		38
4.1	INTRODUCTION	38
4.2	DATA ANALYSIS OVERVIEW.....	38
4.3	CYBER-SECURITY: ANT'S VIEW	39
4.4	THE FOUR MOMENTS OF TRANSLATION.....	44
4.4.1	Problematism	44
4.4.2	Interessement.....	45
4.4.3	Enrolment	47
4.4.4	Mobilization.....	47
4.5	FINDINGS	48
4.6	SUMMARY	50
CHAPTER FIVE: CONCLUSION AND RECOMMENDATIONS.....		51
5.1	INTRODUCTION	51
5.2	SUMMARY OF FINDINGS AND ANSWERING RESEARCH QUESTIONS	52
5.2.1	Summary of Findings	52

5.2.2	Answers to research questions	52
5.3	CONTRIBUTION OF THE RESEARCH	54
5.3.1	Theoretical contributions	54
5.3.2	Practical contributions	54
5.4	LIMITATIONS OF THE STUDY	54
5.5	SUGGESTIONS FOR FUTURE RESEARCH	55
5.6	CONCLUSION	55
5.7	RECOMMENDATIONS	55
	REFERENCES	56
	APPENDICES	75
	APPENDIX A: INTERVIEW GUIDELINE	75
	APPENDIX B: ETHICAL CLEARANCE	76
	APPENDIX C: ANONYMISED EMAIL REQUEST FOR PARTICIPATION	77
	APPENDIX D: EMAILED PARTICIPANT CORRESPONDENCE	78
	APPENDIX E: EDITING CERTIFICATE	83

LIST OF TABLES

Table 3.1 Comparative approaches	27
Table 3.2 Case overview.....	30
Table 3.3 Demography.....	34
Table 3.4 Advantages of remote interview	35
Table 4.1 Findings	49

LIST OF FIGURES

Figure 2.1 The CIA Triad	17
Figure 2.2 Four moments of translation	20
Figure 4.1 Cyber-security actors	42
Figure 4.2 Cyber-security networks.....	43

ACRONYMS AND ABBREVIATIONS

ANT	Actor-Network Theory
CIA	Confidentiality Interiority Authentication
CPUT	Cape Peninsula University of Technology
DDoS	Distributed Denial of Service
ICT	Information and Communication Technologies
IDS	Intrusion Detection Systems
IPS	Intrusion Prevention Systems
OSU	Online Service Unavailable
POPI	Protection of Personal Information
SQL	Structured Query Language

CHAPTER ONE: INTRODUCTION

Chapter One comprises ten sections, organized as follows:

- Introduction and background (1.1).
- Statement of the research problem (1.2).
- Aim and objectives of the research (1.3).
- Research question and sub-questions (1.4).
- Definition of terms (1.5).
- Research design and methodology (1.6).
- Delineation of the research (1.7).
- Significance of the research (1.8).
- Ethical consideration (1.9).
- The structure of the study (1.10).

1.1 INTRODUCTION AND BACKGROUND

Cyber-security is a growing concern around the world. This includes in South Africa where public and private organizations constantly face cyber-attacks and incidents causing considerable financial losses. The phenomenon is caused by the nation's high internet access rate and rising adoption of information and communication technology (ICT) (Bridging Of Digital Divide Programme), which is a digital paradox. A digital paradox is the countless opportunities that technological advances present to the development of a country on one hand and the proliferation of cyber-incidents and cyber-attacks on the other hand (Mabunda, 2021).

In the attempt to respond to the problematic of cyber-incidents and cyber-attacks, several efforts have been deployed. The efforts include regulations (Protection of Personal Information (POPI)), legislative frameworks (National Cybersecurity Policy Framework (NCPF)), businesses spending considerable amount of money on security technologies (firewalls, IDS, IPS), awareness campaigns, and employees sent to periodical training sessions (Da Veiga, 2015)

South Africa continues to be one of the most targeted nations in the world and in Africa despite all the efforts (Kshetri, 2019; Evans *et al.* 2016; Kortjan & von Solms, 2014). The problem could

be attributed to the fact that less focus has been put on human-related vulnerabilities, which represent the main target in most modern and recent cyber-attacks and cyber-incidents (Gundu, 2019; Abawajy, 2014). Considering the Bridging Of Digital Divide Program engaged by South Africa, the fourth industrial generation (4IR), and the ineffectiveness of current approaches to cyber-security (Dunn Cavelty, 2014), it could be anticipated that South Africa will experience an increase in a likelihood of cyber-incidents and cyber-attacks if solutions are not provided (Olutoyin O. Olaitan *et al.*, 2021).

Thus, a different approach is needed to understand why and how cyber-incidents and cyber-attacks occur. This study aimed to analyze cyber-security policy compliance in organizations. The study's results can be applied to direct and enforce agents' (end-users) compliance through which cyber activities can be monitored, managed, so as to minimize cyber-incidents and cyber-attacks within organizations. This study is underpinned by Actor-Network Theory (ANT), which is recognized to be a social-technical theory. ANT is a framework increasingly used in social sciences such as information systems to examine the interactions between existing actors and how networks are built. In ANT, both human and non-human constitute information systems components (Iyamu *et al.*, 2013). ANT is special as it considers non-human and human actors equal in a specific environment (Balzacq & Cavelty, 2016).

1.2 STATEMENT OF THE RESEARCH PROBLEM

Many organizations in South Africa are facing cyber-attack and incident challenges, despite having cyber-security policies in place. The rapid increase in cyber-attacks and incidents have placed South Africa among the most targeted countries in the world (Mabunda, 2021). As a result, organizations continue to incur billions of Rand in losses annually, as seen in 2014 where the losses amounted to 5.8 billion (Jacobs *et al.*, 2016).

The problem faced by these organizations is non-compliance with cyber-security policies by actors such as end-users and technologists (Mtambeka *et al.*, 2023). If left unaddressed, this problem will continue to challenge the sustainability, existence, and competitiveness of South African organizations.

This study aims to explore the profitability of incorporating ANT's concepts (four moments of translation) into research methodologies, with a focus on understanding and addressing the issue of cyber-security policy compliance.

1.3 AIM AND OBJECTIVES OF THE RESEARCH

1.3.1 Aim of the research

The purpose of this study is to analyze the level of compliance with cyber-security policies in organizations and to understand the factors influencing this compliance.

1.3.2 Objectives of the research

The study objectives are as follow:

- I. To identify cyber-attack and incidents registered by organizations.
- II. To understand factors that contribute and influence non-compliance with cyber-security policies in organizations.
- III. To examine how cyber-security policy compliance is enforced in organizations.

1.4 RESEARCH QUESTION AND SUB-QUESTIONS

1.4.1 Main research question

The main research question is: What are the factors influencing cyber-security policy compliance in organizations?

The outcome of this question could inform organizations on how to effectively implement and enforce cyber-security policies, thereby improving their overall cyber-security posture and reducing the risk of cyber-attacks and incidents.

1.4.2 Research sub-questions

The following are the study sub-questions:

- I. What are the cyber-attacks and incidents that affect organizations?
- II. What are the contributing and influencing factors to the non-compliance with cyber-security policies in organizations?
- III. How is cyber-security policy compliance enforced in organizations?

1.5 DEFINITION OF TERMS

1.5.1 Information and communication technologies

Information and Communication Technologies refer to ranges of technologies used to collect, store, retrieve, process, analyze and transmit data and information (Luo & Bu, 2016; Nduati *et al.*, 2015). For Kuzior and Lobanova (2020), Information and Communication Technologies is a “set of various technological devices, tools and resources used to ensure the communication process based on the creation, dissemination, storage and management of information. By these technologies are meant computers, the Internet, radio and television, and telephone (mobile) communication. These definitions present what Information and Communication Technologies stands for in this study as they emphasize the multifaceted nature and their integral role in managing digital information and data across domains though the use of computers, the Internet, radio and television, and telephone (mobile) communication.

1.5.2 Cyberspace

“Cyberspace is a global, virtual, ICT-based environment, including the Internet, which directly or indirectly interconnects systems, networks and other infrastructures critical to the needs of society” (Sigholm, 2013). Li and Liu (2021) define Cyberspace as “Interconnected networks, from IT infrastructures, communication networks, computer systems, embedded processors, vital industry controllers, information virtual environment and the interaction between this environment and human beings for the purpose of production, processing, storage, exchange, retrieval and exploitation of information”. In this study, the term cyberspace stands for a dynamic platform that facilitates diverse interactions between digital environments and human activities, enabling functions such as processing, storage, exchange, retrieval, and exploitation of information.

1.5.3 Cyber-security

Cyber-security refers to the “protection of cyberspace itself, the electronic information, the ICTs that support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace” (von Solms & van Niekerk, 2013). Li and Liu (2021), define cyber security as an important subject in the infrastructure of every company and organization. This includes practical measures to organization’s assets such as information, networks and data against internal or external threats. The above perspectives of the term Cyber-security within the context of this study as they emphasize the broad scope of cyber-security, encompassing both tangible and intangible assets. They also highlight the proactive nature of cyber-security efforts aimed at ensuring the integrity, confidentiality, and availability of digital assets within organizational infrastructures.

1.5.4 Cyber-incident

A cyber-incident refers to “the act of violating or an intention to violate computer security policies, acceptable use policies, or standard security practices” (Ferreira, 2012). This includes data leakage, cyber extortion, identity theft, espionage, online service unavailable (OSU) unauthorized access, and service disruption. Throughout this study, the term cyber-incident is used as defined here.

1.5.5 Cyber-attack

A cyber-attack is an activity that takes place in a cyberspace and carried out by an attacker with the aim to undermine cyber-security objectives (confidentiality, integrity and availability) by stealing, modifying, getting illegal access, destroying data or taking over the control of some elements of cyberspace infrastructure (Hruza *et al.*, 2014). Throughout this study, the term cyber-attack is used as defined here.

1.5.6 Cyber-security policy

Typically, the term "policy" refers to laws and rules governing the dissemination of information, private sector goals for data security, computer operations techniques for managing technology,

and configuration variables in electronic devices. (Bayuk *et al.*, 2012). In an organization, the role of policy would be to provide a platform on which rules for behavior that are expected to achieve cyber-security are prescribed. Cyber-security policy can be described as all the procedures and processes which must be followed by employees in order to keep the confidentiality, integrity, and availability of organization resources.

1.5.7 Actor-network theory

Michel Callon, Bruno Latour, and John Law are the pioneers of Actor-Network Theory (ANT) in the early 80's (Czarniawska, 2016.). The theory focuses on interactions and relationships among actors within heterogeneous networks (Greenhough, 2017). In ANT, both human and non-human are considered actors. Other authors define ANT as a way of engagement that helps to create and to transform realities (Justesen, 2020). These views suggest that ANT not only help to understand existing networks but also plays a role in shaping and reshaping them through actor interactions and collaboration.

1.6 RESEARCH DESIGN AND METHODOLOGY

The methods, procedures, and methodology used in this study are highlighted and described in this section. The research design and methodology also include gathering of data and analysis processes followed to achieve stated objectives.

1.6.1 Research paradigm

A research paradigm includes the three main elements: the ontology, the epistemology and the methodology. This study was underpinned by the interpretivism research philosophy, which was based on the goal stated in Section 1.3. This was mainly because the researcher assumes that there is no single truth (ontology) and that the truth is contextually or subjectively constructed (Epistemology) through participants' perceptions and experiences as discussed by Kivunja and Kuyini (2017). The interpretivist research philosophy also influenced the choice of the methodology used in this study.

1.6.2 Research approach

The inductive approach was adopted in this study. This was mainly because the researcher sought to develop a theory rather than testing an existing one. It is also because the researcher induced sense making in the analysis from the content of collected data (Soiferman, 2010).

1.6.3 Research methodology

Qualitative research was adopted because the analysis and sense making were based on an exploration and understanding of a situation related to human actors, how they interact and how they make sense of the world around them. As stated by Creswell (2013), in qualitative research, researchers seek to explore and get thorough understanding of the situation through participant's viewpoint and experiences. Also, the researchers aim to understand how individuals apprehend and make sense of the environment they are in, themselves and other actors around them.

1.6.4 Research design

This study focused on an exploration of employee's attitude toward organization cyber-security policy. So, for being an approach that facilitates the exploration of phenomenon within its context, where a researcher focuses on specific settings, a case study design was employed in this study.

1.6.5 Data collection

Semi-structured Interview technique was used for data gathering process. This is mainly because semi-structured technique is suitable to explore the opinions and perceptions of participants regarding the complex and sensitive topic of cyber-security but also because they enable the possibility for probing when provided answers are not clear. To supplement semi-structured interviews, documentation was also used when available.

1.6.6 Data analysis

The purpose of this phase was to make sense of collected data and obtain usable and useful information (Ponelis, 2015). To achieve that, ANT was used as guide in the whole process of the analysis. More specifically, ANT from the viewpoint of its four moments of translation as discussed

in Section 1.5.5. The four moments dictated how the process of analysis was conducted. This was done from three (3) main perspectives: (1) existence of actors (human and non-human); (2) creation of networks through conscious and unconscious approach; and (3) interaction and relationship. The theory was useful to identify different actors (actants) including focal actors, and how they exist. Also, how the networks were created within the different environments was examined. Furthermore, the lens was used to understand actors' relationships and interactions within their various networks. Through this means compliance of cyber-security policy could be examined.

1.7 DELINEATION OF THE RESEARCH

This study focused on an organization's cyber-security policy. As stated in the aim, the study was about end-user behaviors toward cyber-security policy within organizational environments.

1.8 SIGNIFICANCE OF THE RESEARCH

This study is important as, we hope, the result will continuously assist organizations in their fights against the persistently growing cyber-attacks and incidents. We also hope that the result will be an effective contribution to enforce cyber-security policy compliance within organizations. Additionally, the study had the potential to add to the academic literature, particularly given the paucity of research in the field of cyber-security studies utilizing the ANT concept and the four moments of translation.

1.9 ETHICAL CONSIDERATION

Ethics can be defined as "normative and regulatory tool kits that provide guidance to constructing good research practices and to the processes related to obtaining research clearance" (Frauenberger *et al.*, 2017). Recognizing that a research project can only have value when carried out with integrity and the respect of ethics code of conduct (Walliman, 2010), this study was carried out with a commitment to these principles.

The researcher first applied for an ethical clearance certificate from the Cape Peninsula University of Technology's Ethics Committee in order to guarantee complete integrity. Then, the faculty and Research Code of Ethics was rigorously used as a guideline in the whole research process.

1.10 THE STRUCTURE OF THE STUDY

The study chapters were structured as follows:

Chapter One: Introduction

The researcher provides an overview of the study's background and research outlines in this chapter. This comprises the problem statement for the study as well as the goals and research questions.

It outlines the study significance and why it is important to analyze the cyber-security policy compliance in its stated context.

It also provides a roadmap for the study.

Chapter Two: Literature Review

This chapter comprehensively reviews existing literature and connects it to the research questions. It also discusses the relevance of Actor-Network Theory and its Four Moments of Translation.

Chapter Three: Methodology

This chapter presents the research philosophy, the methods and techniques, including the data collection procedures and data analysis approach used to achieve research objectives. It also describes the procedures followed to guarantee the accuracy and consistency of the findings.

Chapter Four: Analysis and Results

This chapter presents the data analysis and highlights the findings in line with the research questions.

Chapter Five: Conclusion

This chapter provides an overview of the work done during the investigation, along with the main conclusions and study implications. It also lists the study's shortcomings and makes suggestions for additional research.

CHAPTER TWO: LITERATURE REVIEW

Chapter Two consists of eleven sections, given as:

- Introduction (2.1).
- Information and communication technology (2.2).
- Cyberspace and organizations (2.3).
- Cyber-attack and cyber-incident (2.4).
- Cyber-security in organizations (2.5).
- The goals of cyber-security (2.6).
- End-users (2.7).
- Policy and compliance (2.8).
- Actor network theory (2.9).
- Actor network theory and information systems research (2.10).
- Summary (2.11).

2.1 INTRODUCTION

This chapter reviews existing literature related to the study focus area (Boote & Beile, 2005). According to Marczyk, DeMatteo and Festinger (2010), the literature review is indispensable as it helps to understand and be familiar with the current state of knowledge around the topic being studied. Also, it allows to identify gaps in the existing knowledge and justify the research being conducted (Machi & McEvoy, 2021; Maier, 2013). Thus, a holistic review of literature around Information and Communication Technologies, Cyberspace and organizations, Cyber-attacks and incidents, Cyber-security in organizations, End-users, Policy and compliance, Actor-Network Theory, Actor-Network Theory and Information systems research is presented in this chapter.

2.2 INFORMATION AND COMMUNICATION TECHNOLOGIES

Considered as an essential component of business growth, Information and Communication Technologies (ICT) can be described as a set of technologies used to collect, store, retrieve,

process, analyze and transmit data and information (Luo & Bu, 2016; Nduati *et al.*, 2015; Olise *et al.*, 2014). Many organizations rely on the use of ICT to sustain and remain competitive (Skopik *et al.*, 2012). According to Linton (2017), this is because the adoption and use of ICT improves several aspects of businesses such as a better decision-making, increase of productivity, improve of customer service, greater collaboration, and improve financial performance. Consequently, ICT has become indispensable and broadly used in business chains of diverse types of industry. However, the main purpose of adopting and using ICT mostly varies from one business to another. For example, some businesses make use of ICT to reach a bigger market through the deployment of websites and web applications (Pearson & Bethel, 2016; Taylor, 2015). In the banking industry, ICT is being used to provide bank services such as account balance consultation, funds transfer and to bring many more services closer and available anytime to customers (Aboelmaged & Gebba, 2013).

According to Bayo-Moriones *et al.* (2013)'s study, the impact of ICT depends on the type of ICT adopted and used but also the type of business. In that perspective, they concluded that businesses with a lot of coordination needs, and more communication flows would benefit more from ICT than other types of businesses. Furthermore, the authors believe that the adoption of ICT should not be isolated, it should be aligned with some changes related to the Job design. Taruté and Gatautis (2014) state that major impacts of ICT are mostly around external and internal communication performance. According to them, this is because the implementation and use of ICT within and across businesses has been proven to provide a faster communication using emails, internal chat via media such as skype, and video conferences which help organizations to save a lot of time and consequently maximizes their productivity. Nevertheless, they also believe that ICT could bring much more to businesses if its capability could be aligned with the capability of some internal resources such as people.

The amount of information being shared across and within organizations keeps increasing and information sharing has become a challenge for cyber-security. This is supported by Wiederhold (2001) and Amini and Bozorgasl (2023), as they asserted that information sharing is increasingly growing and plays an important role in organizations. In healthcare for instance, it contributes to the improvement of the quality of healthcare service. Some experts such as Patrick *et al.* (2016) describe information as an important asset for organization which can be shared and transformed

in order to achieve organization goals while information sharing is described as a process of exchanging data, information, and/or knowledge among entities (Kembro *et al.*, 2014).

However, the use of ICT does not only provide advantages to organizations, but it also generates some risks. As ICT platform gets more developed and complex, many researchers agree on the fact that the implementation and use of ICT creates a stage for cyber-attacks and cyber-incidents which become more organized, dangerous, and costly for organizations (Gao, 2023; Quaglia, 2016; Cavelty, 2014; Olise *et al.*, 2014; Skopik *et al.*, 2012; Czosseck *et al.*, 2011). This is mainly because most individuals and organizations make use of ICT to share and store important business assets such as data and information, sometimes confidential and crucial for them. As stated by Zhang *et al.* (2015), like electricity, water and oil, information has become one of the most essential resources in the world. Data and information are not only important for businesses; they are also important for hackers because they are used to harm organizations or customers (Johar, 2017).

2.3 CYBERSPACE AND ORGANIZATIONS

Cyberspace is defined by Sigholm (2013) as “the global, virtual, ICT-based environment, including the Internet, which directly or indirectly interconnects systems, networks and other infrastructures critical to the needs of society” but the term already existed long before that. In 1982, the term was already used by a Canadian writer in the name of William Gibson in a science fiction story called “Burning Chrome” referring to a virtual information space formed by computers. In his fiction description of cyberspace, William Gibson expressed the fact that cyberspace is not only about information, but it is also about its impact on humans using it through their thoughts and cognitions (Zhang *et al.*, 2015).

According to (van den Berg *et al.*, 2014), there are three layers in cyberspace. The first layer is the technical which refers to the technologies in place, the second layer is the socio-technical which refers to the interactions between people and technologies, and finally the governance which refers to people and organizations that govern both technical and socio-technical. On this, some other experts think that the cyberspace is constituted of four layers instead of three: physical, logical, informational and human. Where the physical refers to the physical devices connected to each other including communication cables, logical refers to computer applications

such database applications and web applications, the information transmitted, and finally the user themselves referring to people such as employees or individuals.

Unlike other types of domains naturally created such as the domain of air, land and sea, cyberspace or cyber domain is a manufactured and totally depends on human initiatives (Denning, 2015). Cyberspace has become essential in our daily activities and the number of individuals and organizations active in cyberspace keeps increasing. Ramírez and García-Segura (2017) are experts and they think that it mainly because from human nature perspective, no one wants to be left behind or being considered as ignorant, but also because the huge potential of cyberspace has been understood by organizations. This potential of cyberspace has a double face as if cyberspace is not properly protected, it becomes vulnerable and exploitable for malicious cyber activities such as cyber-attacks. Thus, Sigholm (2013) stated that cyber-attacks and cyber-incidents are subsets of cyberspace. In this study, it was also about the understanding of cyberspace and its different actors that play a role in cyber-security.

2.4 CYBER-ATTACK AND CYBER-INCIDENT

Millions of cyber-attacks and cyber-incidents take place every year causing financial losses, disruptions and annoying all sorts of organizations (Nye Jr, 2016). (Hruza *et al.*, 2014) describe cyber-attack as an activity that takes place in a cyberspace and carried out by an attacker with the aim to undermine cyber-security objectives (confidentiality, integrity and availability) by stealing, modifying, getting illegal access, destroying data or taking over the control of some elements of cyberspace infrastructure. Next to cyber-attack, there is “cyber-incident which is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices” (Ferreira, 2012).

Organizations face different types of cyber-attacks and incidents. This is because technologies change, and malicious people or hackers develop new and various methods to break the confidentiality, integrity, and authentication of organization assets (Safa *et al.*, 2015) impacting organizations, consumers and stakeholders. Many studies were conducted to have an idea about how cyber-attacks and incidents have overwhelmed the globe, and the results revealed that organizations and their consumers are nowadays more concerned about cybercrimes than traditional physical crimes (Kshetri, 2013).

Current cyber-security literature tries to summarize cyber-security threats in four categories which are (I) Cyber terrorism which refers to terrorism activities executed through the use of computer technology, (II) Hacktivism which refers to the use of hackers for political purposes, (III) Cyber-crime which refers to an offense committed through computer technology, and (IV) Cyber-warfare, the use of computer technology in a war or conflict activities (Quigley *et al.*, 2015).

Cyber-crimes have grown throughout the years and become a major concern for government, private organizations and individuals (Marsh, 2017). According to (Quigley *et al.*, 2015), Cyber-crimes are among the common cyber threat registered by organizations, but it receives less attention. According to a Norton cybercrime report from 2011, South Africa and China had the two economies most affected by cybercrimes, with 84% of South Africans and 85% of Chinese citizens respectively falling victim to cybercrimes (Dlamini & Modise, 2013; Kshetri, 2013). Another report from Global Economic Crime and Fraud Survey for 2018 claimed that South Africa was the world's second-most-targeted nation due to poor policing and immature laws, and naive end-users (Citizen Reporter, 2018). Hence, identifying the cyber-attacks and indents faced by organizations was one of the objectives of this study.

2.5 CYBER-SECURITY IN ORGANIZATIONS

The phenomenon of cyber-security came into the spotlight in 2007 with the cyber-attack addressed to the republic of Estonia which shown how modern countries and modern organizations could be destabilized through ICT (Jansen Van Vuuren *et al.*, 2015; Kozlowski, 2013). Since then, cyber-security has become a major concern for individuals and organizations. This is also because over the years, cyber-attacks and cyber-incidents have been increasing causing huge economical and safety damages to institutions that do not have proper cyber-security measures. Hence, in many countries around the globe, cyber-security is considered as a national priority (Gcaza & von Solms, 2017). Kesan and Hayes (2014) think that this is because a failure in cyber-security can lead to expensive losses for organizations but can also be critical to human lives as hackers have ability today to manipulate information systems and prevent organizations and governments to spread out an evacuation alert in a case of incidents and emergency. According to Kesan and Hayes (2014), the annual cost of cybercrime and economic espionage to the global economy ranges from \$375 billion to \$575 billion. According to Kshetri (2015), cybercrimes cause South African organizations to lose about 20 billion annually.

Although many countries are now conscious about the importance of cyber-security and have decided to join forces and be part the fight to eradicate or minimize cyber threats, some details still need to be addressed for concerned and involved countries to easily stand as one for the same cause. One of the issues identified by Luijff *et al.* (2013) is the understanding of cyber-security which can differ from nations. According to the authors, not having a common understanding and perspective of what cyber-security is can cause confusion and be a barrier to the current fight against the threats of cyberspace. For the purpose of having harmony in the definitions of terminologies, some nations including South Africa develop and publish a national cyber-security strategy (NCSS), in which they provide their understanding of cyber-security. In some South African publications, cyber-security is described as *“the collection of tools, policies, security concepts, safeguards, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, and organization and user assets”* (Luijff *et al.*, 2013). Consequently, the vision of South Africa about cyber-security is to create a trusted and secure environment where ICT can be used with confidence by individual and organizations. von Solms and van Niekerk (2013) also define cyber-security as *“protection of cyberspace itself, the electronic information, the ICTs that support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace”*. The latter definition is unique because it emphasizes the significance of the roles played by both human and non-human actors in the problem that organizations face. This join Bada and Sasse (2014) cyber-security view. They indicated that the purpose of cyber-security is not limited to secure non-human organization assets but also to secure humans that make use of ICT systems. Mosca (2015) went further to say that through the attempt to protect individuals, organizations and other cyberspace entities from threats, cyber-security would contribute to the sustainability and competitiveness of organizations because organizations without proper security plans provide business to those with effective security plans.

2.6 THE GOALS OF CYBER-SECURITY

Maintaining the confidentiality, integrity (Which in some instances may include authenticity and non-repudiation), and availability of organizational assets like data and information is the primary objective of cyber-security, as illustrated in figure 1. The CIA triad—confidentiality, integrity, and

availability—was created to direct the creation of security measures like cyber-security policies inside enterprises (Rouse, 2014).

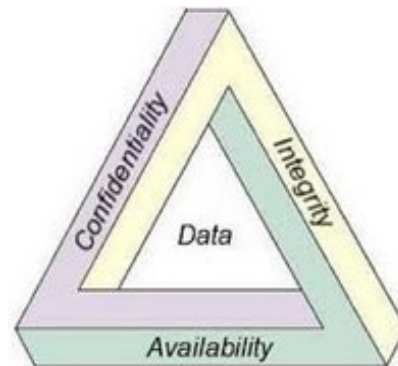


Figure 2.1 The CIA Triad (Farooq *et al.*, 2015)

Data and information confidentiality implies that the system must prevent unauthorised people to access sensitive data and information. This is from an external and an internal aspects. The integrity implies that the data and information must not be altered, lost or compromised. The availability implies that the data and information must be available and accessible when required (Kumar *et al.*, 2015).

2.7 END-USERS

An end-user as defined by the Oxford dictionary is simply a person who makes use of a product. End-users are also referred to as technical or a non-technical person (Poon *et al.*, 2014). Employees remain frequently held responsible for security incidents and breaches in many organizations (Flores *et al.*, 2014). In fact, computers have been replaced by end-users as hackers first target choice (Safa *et al.*, 2016). This has been proven by the techniques mostly used nowadays by attackers to harm or access individuals and organizations assets and systems. These techniques include social engineering and fishing and make use of human weaknesses as they usually start with a human disclosing personal information or clicking on an unknown link sent intentionally by an attacker (Junger *et al.*, 2017). Moyo (2015) feels that because end-users are the weakest link in an organization's security chain, they are typically the target of hackers. Some experts go further and say that if end-user variable is removed for the security equation, it

would be easier for organizations to secure their systems (Safa *et al.*, 2016; Arachchilage & Love, 2014)

Although technologies and other tools used to manipulate data and transmit information from one entity to another one exists, those technologies or systems receive instructions from end-users (Tang *et al.*, 2016). End-user attitudes toward security measures play a crucial part in the process of preventing security risks (Cong Pham *et al.*, 2017). Arachchilage and Love (2014) emphasized by asserting that end-user's role is the most important one. According to them, educated end-users with a good attitude with regards to security policy can contribute to reduce security risks and make cyberspace a more secure environment. Thus, this study also attempted to understand human actor 'attitudes toward deployed cyber-security measures such as policies.

2.8 POLICY AND COMPLIANCE

To mitigate cyber-crimes, organizations have adopted technical methods and approaches, such as firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and other technical measures (Said *et al.*, 2015). Safa *et al.* (2015) believe that technology alone cannot stand against hackers and their constantly changing offensive methods. The authors further suggested that technology measures should be associated to security policy to expect effectiveness. This is because the security policy plays a major role in the fight against cyber-attacks and incidents as it regulates and controls organization user's behavior which becomes a challenge for organizations (Sannicolas-Rocca *et al.*, 2014).

According to Bayuk *et al.* (2012), the term policy refers to every regulation and law. The law and regulations that have a purpose to maintain organization cyber-security. Organization security policy can be described as all the procedures and processes which must be followed by employees in order to keep confidentiality, integrity, and availability of organization resources. Although having a cyber-security policy is important for organizations, experts highlight that it is ineffective to have policy without compliance (Da Veiga, 2015). Bulgurcu *et al.* (2010) think that every organization with the desire to strengthen their security aspect should put more efforts to understand how employees comply with organization existing policy.

Cavelty (2014) stated that cyber-security policy is a solution to cyber-security challenges globally faced. According to him, most security stakeholders are more concerned about common security

issues such as vulnerability and privacy which can be addressed through regulations. A study revealed that having policy does not necessarily solve the security issues because there is a gap between having policy available to employees and their practices. The current dilemma with cyber-security policy is that employees do not comply with organization security policy but most of them are using social media and internet for communication purpose (Streeter, 2013). Blythe (2013) also noted that half of data breaches are due to compliance failure to organizations' security policy. As a result, some organizations embark on awareness campaigns, such as messages (via emails), informative posters, newsletters, and computerized training modules (Albrechtsen & Hovden, 2010).

According to Da Veiga (2015) this approach can only give a sensation of having end users aware of security policy but not an effective method for compliance. Sannicolas-Rocca *et al.*(2014) stated that methods to improve and enforce employee behavior toward organization security policy are needed. This study objective was also to unpack how cyber-security policy is developed, communicated and enforced in organizations.

2.9 ACTOR-NETWORK THEORY

Michel Callon, Bruno Latour, and John Law were the pioneers of actor-network theory (ANT) in the early 1980s (Czarniawska, 2016). ANT is a socio-technical theory putting emphasis on interactions and relationships among actors within heterogeneous networks (Greenhough, 2016). ANT focuses on how networks are constructed rather than why they exist (Shim & Shin, 2016)(Shim & Shin, 2016). Actors and networks are the main tenets of the theory. In ANT, human and non-human entities are both actors, and they are both equal in a network. Non-human actors include technologies supported by organizations, tools used by humans (Hanseth *et al.*, 2004), cultural meanings or environmental conditions (Scott, 2017).

From ANT perspective, heterogeneity refers to network composed of diverse materials or elements (Shim & Shin, 2016; Law, 1992). According to (Law, 1992), the interaction between actors or actants of heterogeneous networks such as people, technologies, machines, texts, architectures, animals, money and any other elements which can contribute or mediate in social interactions constitutes the base of the society.

A network is an established connection between actors. For a connection to be formed, actors must be moved and translated (Dankert, 2011). According to Iyamu and Sekgweleo (2013), the objective of having networks is the fact that actors can collaborate and propose solutions to identified problems or to generate a new entity. The creation of networks is based on a four steps process called translation or moments of translation (Williams, 2014). Translation is presented by Costa and Cunha (2015) as “a set of methods by which actors within a network will try to enroll the other actors into positions that can serve their own purposes.” According to Jessen & Jessen (2014), it can also be described as a process of delegating and persuading actors to accept roles and responsibilities through inter-related four phases which also describe how the actor-network relationships come to be. As shown in Figure 2.2, the translation includes problematisation, interessement, enrolment, and mobilisation.

MOMENTS OF TRANSLATION

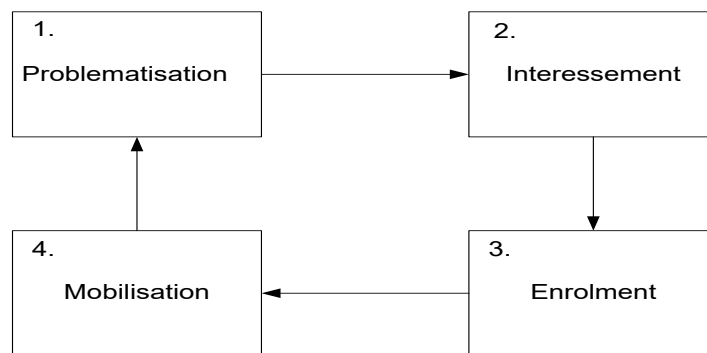


Figure 2.2 Four moments of translation (Callon, 1984)

PROBLEMATISATION

The problematisation is the first moment of translation and it refers to the step where the main actor, also called focal actor makes himself indispensable to the rest of actors, identifies and describes the problem. It is also the moment where actor interests are identified and negotiations to attempt to merge them into a common interest take place (Costa & Cunha, 2015; Heeks & Stanforth, 2015). Jessen and Jessen (2014) stated that an obligatory passage point (OPP) is known as a proposed solution in the problematisation phase.

INTERESSEMENT

After different aligning interests and human and non-human roles identified, the next moment is the interessement. In this moment, focal actor or actors initiate the recruitment process according to the role and responsibilities defined in the problematisation phase and convinced them on the viability of the problem faced and the proposed solution to the problem (Costa & Cunha, 2015; Jessen & Jessen, 2014).

ENROLMENT

Once the interessement moment is successful, then enrolment moment can take place. The enrollment is where role and responsibilities are assigned to recruited actors (both human and non-human). This moment is very important as it is in this phase where the actor allies, supports and relationships are also defined (Jessen & Jessen, 2014). According to Costa and Cunha (2015), the enrolment is successful when recruited actors accept the role and responsibilities assigned to them and solid network of allies are formed.

MOBILISATION

After the problematisation, interessement, and enrolment phases are completed, the mobilisation phase occurs (Costa & Cunha, 2015). In order to establish a network, a designated spokesperson or actor mobilizes allies in a way that they act in line with their assigned roles and responsibilities (Jessen & Jessen, 2014).

Apart from translation, ANT has other concepts such as Alliances, Black box, and Inscription. Alliances are the outcome of a successful translation. Stockbruegger and Bueger (2017) described a black box as *“a combination of actants, such as a device, system, or technology whose internal workings are hidden and do not matter anymore for those who use it and the way it is used”*. According to Alexander and Silvis (2014), an actor is as strong as the alliances it has with other actors. A black box is an uncheckable network formed by allied strong actors. In a black box, the alliances are so strong that it is one single actor. Inscription is described by Shim and Shin (2016) as the development of a technical artifact in order to protect the interests of actors. According to Stockbruegger and Bueger (2017), the concept of inscription also describes a stable relationship between two actors or heterogeneous actors. In that relationship, the role of different actors is clearly defined, and their interactions are well established. A successful inscription can also result in a black box. The concept of inscription is a special and useful concept as it has been

used to understand how technologies become part of our daily life and how they are involved in how things are done. ANT concepts should be considered as flexible research tools that facilitate empirical studies. ANT concepts are not used to explain the world but to facilitate its exploration and description (Stockbruegger & Bueger, 2017).

2.10 ACTOR NETWORK THEORY AND INFORMATION SYSTEMS RESEARCH

ANT is a framework mostly adopted in research to guide analysis and understand how existing heterogeneous networks are formed within a specific environment (Shim & Shin, 2016). The theory is interesting as it proposes a new approach of thinking based on agency concept and the effect of an entity (actant) on another one (Felski, 2016). The theory is also said to be a useful tool to empirically examine and understand organization processes where organization can be considered as networks, or an assemblage of networks within which heterogeneous actors can be found (Whittle & Spicer, 2008). According to (Alexander & Silvis, 2014), one of the main strengths of the theory would be its ability to include and consider heterogeneous actors in an analysis process.

Although the theory was initially developed for sociology and sciences studies, the theory is increasingly used in many other research studies (Dedeke, 2017; Walsham, 1997). This includes information systems (IS) studies where the theory has been widely used to examine the complexity and huge number of existing interactions between human and non-human actors (Fornazin & Joia, 2016; Alexander & Silvis, 2014; Tatnall, 2005; Walsham, 1997). IS research being mostly focused on interaction between humans, technologies and information systems which in ANT concept is referred to as human and non-human collaboration. The aspect of ANT which consists of denying any differences between human and non-human actors makes the theory particularly interesting for IS studies (Alexander & Silvis, 2014). According to Iyamu *et al.* (2013), the theory is also used to explain and interpret the developments and changes managed by non-human and human actors in social and technological domains. Other researchers such as Mahama *et al.*, (2016), used ANT to examine relationship between actors (actor-actor) for a better understanding of how IS are organized more specifically the collaboration between human and technologies in a network (Greenhalgh & Stones, 2010).

In the domain of healthcare, ANT is recommended and used to address the complexity in the process of IT systems implementation (Troshani & Wickramasinghe, 2014; Cresswell *et al.*, 2010). In other domain such as the finance, the application of ANT has assisted to understand the convergence between the finance and technology what Chinese called the “fintech” and more importantly to explore the interaction between “fintech” and social (Shim & Shin, 2016). In the concept of home, ANT was interpreted as a dynamic and relationship process where human and non-human actors are also valued. In that context, Wang *et al.* (2023) argued that in the development of ideal home networks, collaborations and translations would take place between urban-rural migrants and rural heterogeneous actors (local people, means of subsistence farmland, landscapes, and ICT facilities). This facilitates the building of new entities (networks and actor-networks structures) through three steps: The presentation of the problem by main actor(s), enrollment and benefit granting, and negotiation based on actors’ common goals. This approach shows that with ANT, irrespective of the domain in which it is being used, the process developing network and actor-network structures, the interactive relationship, and the of translation have to take place in order for a new entity to be constructed based on actors’ common goals. In another study conducted by Gutiérrez (2023) examined the intersection between ANT and algorithms in the context of Artificial Intelligence (AI). The study highlights that ANT is sociological theory where human and non-human are both important and have equal power, while an AI receives and executes instructions. The study concluded by proposing a framework to address the existing power dynamic in AI.

The above discussions show that there is still so much that need to be done through the use of ANT. Although the theory has numerous strengths, some weaknesses have been identified. Alexander and Silvis (2014) argued that its lack of explicit boundaries is one of them; but could be addressed by staying focused on the research main objective. For some researchers, ANT cannot be considered as a theory because unlike traditional concepts of theories where there are a priori assumptions about the world and existing entities in it, ANT does not limit empirical investigations by providing a system of generalization which could be adopted or test in studies. It is helpful to understand and interpret the world (Stockbruegger & Bueger, 2017).

2.11 SUMMARY

This chapter was about reviewing existing studies on the following key concepts: Information and Communication Technologies, Cyberspace and organizations, Cyber-attack and incident, Cyber-security in organization, End-users, Policy and compliance, Actor-Network Theory, and Actor-network theory and IS research. The review supported a holistic understanding of the concepts, how they relate to the study and most importantly the challenges and implications about the current cyber-security phenomenon. The review started by providing an understanding of what ICT is and what are the implications of its implementation and use by businesses. This allowed the researcher to notice that although the implementation and use of ICT is advantageous for organizations, it also provides a new domain called cyberspace or cyber domain where cyber activities such as cyber-attacks and incidents take place. To prevent and fight cyber-attacks and incidents, in many countries including South Africa, organizations have deployed a cyber-security. The review also revealed that in some countries such as South Africa, although there is a cyber-security in place, the number of cyber-attacks and incidents keeps increasing because the cyber-security systems are mostly technology oriented while end-users (humans) have been the new targets of attackers. Organizations urged to develop cyber-security policy which was later on revealed to be ineffective due to a lack of cyber-security policy compliance as cyber-security policy without compliance is useless.

CHAPTER THREE: RESEARCH DESIGN AND METHODOLOGY

3.1 INTRODUCTION

The various methods, procedures, and techniques employed for this study are highlighted and explained in this chapter. It also discloses the procedures used for data collection and analysis to answer the research questions and accomplish the objectives (Stage & Manning, 2015; Degu & Yigzaw, 2006). The chapter is organized in eight sections as follows: In the next section, the research paradigm is presented (3.2); then the research approach followed in the study is discussed in the Section 3.3; the method adopted is presented in the Section 3.4; the Section 3.5 is about the research design employed; in the Section 3.6, the data collection technique used in the study was presented; the Section 3.7 is about data analysis. Finally, Section 3.8 presents a summary of the entire chapter.

3.2 RESEARCH PARADIGM

The paradigm in the context of research is the fundamental set of ideas that direct the activities. It is also a way of thinking assumptions about the reality under study (Punch, 2013) and guides the choice of the methodology used in the study (Khun, 1962). Being philosophical by nature, the research paradigm is directly associated with the concept of ontology, epistemology, and methodology. Ontology and epistemology are important as they are the starting points of research. In the context of this study, the ontology indicates how the researcher defined the truth and the reality, what was known, and the reality about cyber-security policy compliance; the epistemology indicates how the researcher got to discover the truth and reality, what could be known, and how the researcher went about it; the methodology is the methods used to conduct the research (Antwi & Hamza, 2015; Johnston, 2014).

Interpretivism

As opposed to the positivism which refers to an empirical research philosophy in which causes determine effects and mostly adopted for theories and hypotheses testing and experiences studied through objective and quantifiable variables (Mackenzie & Knipe, 2006), Interpretivism research philosophy underpinned this study. This is mainly because it is consistent with the

research aim and objectives supporting an understanding of the world from an individual point of view. Also, because the researcher believes in a subjective approach to reality. The researcher thinks that reality depends on its context so an interaction with the phenomenon under study and its settings is necessary for in-depth understanding. Furthermore, interpretivist researchers do not only examine causal relationships of facts, but they also try to understand the context in which facts came about as it was the case for the objectives of this study. Interpretivism was also suitable because it is more focused on the “how it happened” (Chowdhury, 2014). Thus, knowledge about cyber-security policy compliance used to address the aim of this study was not found but subjectively constructed.

3.3 RESEARCH APPROACH

The research approach is about deciding if the research should begin with a theory or should the theory itself be resulted from the research (Goswami, 2010).

Based on the study aim and objectives as stated in chapter one and provided advantages as shown in Table 3.1, an inductive approach was followed in this study. This was mainly due to the fact that researchers sought to develop a theory rather than testing an existing one. It is also because the researcher induced sense making in the analysis and interpretation from the content of collected data (Goswami, 2010; Soiferman, 2010).

Table 3.1 presents brief descriptions and comparison of the three research approaches that exist. This includes deductive, abductive and inductive research approaches. The comparison is based on components such as the logic followed by the approaches, what each of them is used for, their use data, and their relationship with theories.

Table 3.1 Comparative approaches (Niiniluoto, 2018)

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

3.4 RESEARCH METHOD

The research method was the “How” in the context of developing knowledge and its choice depended on the research questions and the philosophical assumptions that underpinned this study.

The objectives of this study and the researcher philosophical assumptions (ontology and epistemology) dictated the choice of the research method used (Lewis, 2015). The study made use of qualitative research methods to achieve the stated aim and objectives as the development of the model was based on the exploration and understanding of a situation related to humans, how they make sense of the world around them.

This was also due to the fact that research work was conducted in natural settings, where the researcher sought to explore and get in-depth understanding of phenomenon through the interpretation of actors’ experiences. It is a rigorous approach to provide answers to research questions. In a qualitative research, researchers aim to understand how people learn about and make sense of themselves and people around (Creswell, 2013; Hox & Boeije, 2005). Qualitative research is sometimes referred to as a real-world enquiry because it takes in consideration the researcher’ active engagement with the phenomenon under study to providing knowledge

(Henwood, 2014) and it is more inductive. Another important point that led to applying a qualitative method is that it does not credit any assumption about perspectives of people considered with more power being more important than perspectives of those considered with less power. The qualitative method was also suitable as it helped the researcher to examine how things look from different perspectives because every perspective was important and had to be taken in consideration (Taylor *et al.*, 2015).

3.5 RESEARCH DESIGN

Research design has sometimes been presented as a plan to conduct research. In this study, the research design was more than that because a work plan derived from a research design. The research design also helped to insure that resulting evidence enabled researchers to address research questions without any ambiguity. This includes being specific about the nature of evidence required to describe the phenomenon under study and address research questions (de Vaus, 2001).

This study exclusively focused on an exploration of organization employee's attitude toward organization cyber-security policy. The case study design was employed because it makes the examination of phenomenon within its usual settings much easier (Baxter & Jack, 2008).

Case study design was also chosen for other advantages such as its flexibility and adaptability to multiple research techniques especially for data gathering. This gives it the potential to address various types of situations (simple and complex). with simple and more complex situations. Case study design also enables the researchers to address various types of research questions without neglecting the context factor influencing the phenomenon under study. Case study design was suitable as it provided an understanding of the interaction between the specific context and the phenomenon being studied. As stated by Baxter and Jack (2008) *“Qualitative case study methodology provides tools for researchers to study complex phenomena within their contexts. When the approach is applied correctly, it becomes a valuable method.”* Another important strength and reason for using a case study design is its aptitude to generate results which are not out of context and provides an analysis on a specific case. Furthermore, case study design is appropriate to real life situations, and it is useful to promote an understanding of complex real-life situations such as the current cyber-security phenomenon faced by south African institutions.

Due to the sensitivity of the topic in this study, which resulted in organizations being reluctant to share cyber-security related information and participate in the study, the researcher encountered challenges in securing enough samples. Consequently, the study made use of three South African-based organizations, all operating locally. One of these organizations functions as cyber-security service providers, a crucial inclusion considering the outsourcing practice for cyber-security services in the industry. The main criteria for the case selection were the existence of a cyber-security department or cyber-security team in the organization with the core responsibility to maintain the security CIA triad (Confidentiality, Integrity, Authenticity). Despite the limited number of participating organizations, this approach ensured that the selected cases directly aligned with the main objectives of this audit.

For anonymity reasons, the names of the organizations were changed into pseudonyms. So, they were called HollanRaph for Case 1, NoahGabi for Case 2, and LenJo for Case 3.

3.5.1 Case overview

In an era dominated by digitalization and a landscape where cyber-security is no longer an option but a necessity for organization. The study purpose was to analyze the level of compliance with cyber-security policies in organizations and to understand the factors influencing this compliance. To achieve this, a case study design has been employed, focusing on the organizations presented in Table 3.2.

Table 3.2 Case overview

Case	Organization	Industry	Size	Cyber-security relevant detail
1	HollanRaph	Higher education	Large with over 5,000 staff	<p>Located in the Gauteng province, HollanRaph shows its commitment to cyber-security through the implementation of a cyber-security department and cyber-security policy.</p> <p>The institution can be seen as a dynamic network comprising not only human actors but also non-human actants.</p>
2	NoahGabi	Higher education	Large	<p>NoahGabi has over 32,000 students and 5,000+ staff. Located in the province of Western Cape, it is one of the largest highest education institutions of the province. Being big doesn't make you safe; CPUT recognizes this and actively and shows its commitment by having a dedication cyber-security team onsite.</p>
3	LenJo	IT services and consulting	Small	<p>Based in the province of Gauteng, LenJo is a key player in the realm of IT Services and IT Consulting in South Africa. LenJo specializes and focuses on offering Business-to-Business (B2B) ICT solutions. It caters to a diverse range of clients. The scope of clients goes from small businesses to cross-border enterprises. Its aspirations are to be a leader in business process digitalization, cyber-security services, and ICT skills development.</p>

Table 3.2 sets out a review of three cases. It tabulates organizational names and associated industry type and size. The final column shares relevant details concerning cyber-security. These cases constitute the empirical focus of the case study strategy of the study.

3.6 DATA COLLECTION

A qualitative data collection technique was used to gather data in accordance with the study's objectives, which were outlined in the first chapter. Using data collection techniques, a researcher can gather information about the subjects or phenomena under investigation as well as the environments in which they occur in a methodical manner (Elmusharaf, 2012). In a qualitative case study, various types of techniques for data gathering. However, this study adopted the semi-structured technique for its process of data collection. This was mainly because semi-structured perspective is suitable to explore the opinions and perceptions of participants regarding the complex and sensitive topic of cyber-security but also because they enable the possibility for probing when provided answers are not clear. To supplement semi-structured interviews, documentation was also envisaged in case documents were to be put available by participants. This is because apart from being a stable, unobtrusive, and exact source of data, documents can also provide useful information (Merriam & Tisdell, 2015).

3.6.1 Participant selection criteria

For this study, the researcher employed a purposive sampling technique to select participants and it was done based on specific criteria. The aim was to have diverse and representative samples but also to ensure its relevance and richness, participants. The key criteria included occupation, expertise and/or experience in cyber-security and policies. Another reason for using purposive sampling was to capture insights from individuals directly involved in the complex and sensitive nature of cyber-security.

3.6.2 Ethical considerations

Ethical considerations are crucial in any research study, especially when involving human participants. Therefore, the following points were rigorously considered to maintain the ethical standard: informed consent, confidentiality, privacy, transparent communication, approval from ethics committee.

Prior to the commencement of any data collection activities, participants were informed about the study's purpose and all the procedures introduced to them. procedures. They were explicitly

informed that their involvement was entirely voluntary, and they had they could withdraw from the study at any point without consequences.

The researcher tried to protect the identities of participants. Any personally identifiable information was anonymized or replaced by pseudonyms in the report to ensure confidentiality. Additionally, all collected data, including interview recordings and transcripts, were securely stored using password protected. electronic systems accessible. They were only accessible to the researcher and authorized people such as supervisors.

Participants' privacy was maintained throughout the study process. Virtual interviews were conducted in private settings to minimize the risk of exposing sensitive information. The researcher also ensured that data collection activities did not intrude into participants' personal lives more than necessary.

Throughout the recruitment and data collection processes, clear and transparent communication was maintained with participants. Any questions or concerns raised by participants were addressed promptly and comprehensively. Participants were provided with contact information, and they were encouraged to reach out for any queries or further clarification.

3.6.3 Data collection technique and procedure

The first contact with potential participants was made via email. The researcher sent out emails requesting interview opportunities from organizations. The emails were personalized for each potential participant. The emails included some important study details such as the study purpose, the length of the interview, the questions that would be asked, and any confidentiality agreements intended to reassure them, and some criteria on desired participants. After the first lot of emails were sent out, the researcher carefully tracked which organization/participants had responded and which ones still needed to be contacted. For participants who had not responded to the first email, follow-up emails were sent or phone calls when the contact number was available. In follow-up emails or phone calls, the researcher made sure to remind the research purpose, context, importance of the study, and the opportunity for the participant to share their insights and experiences. If the participant agrees to participate, then a meeting for the interview could be scheduled. A reminder email or phone call was sent to the participant a day before the scheduled interview to confirm their participation and ensure they have all the necessary information to join

the meeting. On the interview day, the researcher ensured that the participant is comfortable with the format and that the technical requirements are met. After the interviews, participants were again contacted by the researcher to thank them for their participation.

Despite the challenges caused by the reluctance of some organizations to participate, the researcher successfully managed to schedule four interviews from some significant organizations.

Table 3.3 Demography

Participants	Job Title	Experience	Case
1	Manager: IT Risk and Compliance	>10 years	HollanRaph
2	Senior Systems Engineer: Networks, Information Security	>10 years	HollanRaph
3	CEO, Security Specialist	>9 years	LenJo
4	Manager: IT Strategic Services	>10 years	NoahGabi

Table 3.3 summarizes key demographic details concerning the four participants who provided data for the study. Details include roles within respective organizations, years of professional experience and the specific case associated with each individual.

Remote interviewing

Although the initial plan was to have participants in face-to-face interviews, the researcher finally went for remote interviews using video conferencing platforms, specifically Zoom and Microsoft Teams. This was motivated by the geographical position of some participants and the financial implications such as travel expenses that the researcher had to mitigate. Conducted interviews remotely facilitated the engagement with participants regardless of their location and helped in overcoming barriers imposed by existing distances. More advantages for using remote interviewing process in this study are presented in Table 3.4.

Table 3.4 Advantages of remote interview

Benefit	Description
Accessibility	Video call meetings allowed for greater flexibility and accessibility for participants, regardless of their location or mobility restrictions.
Consistency	Video call meetings ensured consistency and standardization in the data collection process, as the same format and technology was used for all participants.
Convenience	Participants could participate in the interviews from the comfort of their own homes or workplaces, reducing the time and costs associated with travel.
Record keeping	Video call meetings allowed for easier record keeping, as the audio and video recordings could be stored and transcribed for analysis.
Reduced logistical challenges	Face-to-face interviews can be challenging to organize. Video call meetings reduced the logistical challenges associated with organizing face-to-face interviews.

Table 3.4 outlines five benefits concerning the conducting of remote interviews, namely: accessibility, convenience, consistency, reduced logical challenges and record keeping.

3.7 DATA ANALYSIS

The purpose of the analysis was to make sense of gathered data and obtain usable and useful information (Ponelis, 2015). To do so, the researcher collected was transcribed. This involved converting recorded words into written texts. Transcription was important as the data was put in a format that is easier to manage and analyze.

From the perspective of ANT, Problematization, Interessement, Enrolment, and Mobilization known as four moments of translation reviewed in the second chapter were used as lenses to guide the entire analysis of data. This was done from three main perspectives: existence of actors (human and non-human); creation of networks through conscious and unconscious approach; and interaction and relationship. As shown in Chapter 2, Figure 2.2, actors involved in cyber-

security policy were followed and their interactions with other actors and networks were interpretively analyzed and examined as to:

- **Problematisation:** Identify the problem defined and described by the main actor. This is called.
- **Interessement:** Identify actor interests and understanding negotiations that took place as the focal actor attempts to merge them into a common interest, examine how actors are recruited based on defined roles and responsibilities. This moment also involved exploring how actors were convinced of the viability of the identified problem and the proposed solution.
- **Enrollement:** Examine how the roles and responsibilities were assigned to recruited actors.
- **Mobilisation** Identify the designated spokesperson and understand how the spokesperson mobilized allies (Costa & Cunha, 2015; Jessen & Jessen, 2014).

The theory was useful to identify different actors (actants) including focal actors, and how they exist. Also, how networks were created within the environment was examined. The lens was also used to understand actors' relationships and interactions within their various networks. Furthermore, tracing existing actor connections with other actors and networks helped to understand what constitute networks.

The understanding of the phenomenon was improved by use of ANT. This is because it provides guidance through an alternative perspective which does not only give power to human actors but also gives room to non-human such as objects, rules, and processes to be examined as actors or actants (Jessen & Jessen, 2014). Cyber-security policy involves several entities including human and non-human. With an emphasis on the connections between actors (human and non-human), ANT described how connections and interactions between these entities led to the creation of networks (Dankert, 2011).

3.8 SUMMARY

This chapter holistically describes how the study was conducted as it provides sufficient and clear details allowing a reader to replicate the study. The details include philosophical assumptions,

research approach, methodology, and design employed, applied techniques and procedures for data collection, tool and process for data analysis, research delineation, significance of the research and ethical consideration. Interpretivism philosophy underpinned the study, inductive approach and qualitative research method were adopted. Case study design was followed, and interview techniques (semi-structured) and documentation (to supplement interviews when provided) were also adopted. Lastly, the entire analysis was guided by Actor-Network Theory (ANT) from the standpoint of its four moments of translations (Problematization, Interessement, Enrolment, and Mobilisation).

CHAPTER FOUR: DATA ANALYSIS AND FINDINGS

4.1 INTRODUCTION

In pursuit of examining and enhancing cyber-security in organizational, this study aimed to analyze the level of compliance with cyber-security policy compliance and to understand the factors influencing this compliance. Through compliance, cyber activities can be monitored, managed, and mitigated so as to minimize cyber-security risks within organizations. As stated in previous Chapters 1 and 3, the study is limited to South African environments. As Vosloo (2014) described it, analyzing data refers to providing order, structures and meanings. To do so, the research employed Actor-Network Theory (ANT) was used as lens to guide the entire analysis.

The chapter is divided into 6 main sections, each contributing to the comprehensive analysis of collected data. Data analysis is briefly reviewed (4.2). The data analysis is presented with respect to the ANT view (4.3) and the four moments of translation (4.4) in the third section. The results of the analysis are provided in the fifth section (4.5). Then a summary is presented in the final section (4.6).

4.2 DATA ANALYSIS OVERVIEW

As highlighted in the third chapter, the case study design was adopted, and three organizations operating within South Africa were used as cases in studying the phenomena, activities of cyber-security and associated risks. For the analysis, the four moments of translation were used to guide the entire analysis. Figure 2.2 illustrates how the building of networks through the translation of interests in the context of Actor-Network Theory (ANT). It shows that the process of translation starts with the problematisation phase. Once the problematisation is completed, the interessement phase can take place followed by the enrolment phase, finally, the mobilisation phase.

As discussed in Chapter 3, data were collected based on the objectives of the study. collected data was transcribed and coded as follows: HollanRaph for Case 1, NoahGabi for Case 2, and LenJo for Case 3.

Two explanatory transcription examples are provided:

But at the moment, apart from the awareness program, we do not regularly communicate the policy and that is something that we have identified, and something we will be working on (L139-142_P1_NoahGabi).

This means lines 139 to 142 from Participant 1 in Case 2.

Let me deal with the users first. So, if a user wants to report something, our service desk is obviously the first port of call. They log a ticket to the service desk and then if it's a security related incident, it will get routed to my unit. So, the users have always got an open line to information security. (L392-396_P1_HollanRaph).

This means lines 139 to 396 from participant 1 in Case 1.

4.3 CYBER-SECURITY: ANT'S VIEW

Using ANT as a lens, the focuses were actors, networks and the moments of translation. This means that the various actors, as they partake or show interest in the activities of cyber-security were identified. Also, the roles of the actors were examined, and the implications were assessed. The same approach was applied in the area of the networks that existed in the course of cyber-security activities in an organization in South Africa. The moments of translation entails negotiation among actors within heterogeneous networks. Such negotiation approach helps to examine and understand the activities of cyber-security, which Dlamini and Modise (2013) describe as complex and multidimensional phenomenon that engage various entities or actors.

4.3.1. Actor

In the context of ANT, both human and non-human are actors, as long as the entity can make a difference within an environment (Edwards, 2014). As depicted in Figure 4.1, both humans and non-humans are directly or indirectly involved in any cyber-security activities. In the context of this study human and non-human actors refer to individuals or entities within the organization that

play a role in cyber-security related activities. First, the human actors were identified and discussed; followed by the non-human actors:

Human actors

Human actors consist of Technical (IS/IT personnel) and non-technical (Non-IS/IT personnel). The IS/IT personnel include IT Risk and Compliance managers, IT Strategic Services Manager, Security specialists, Systems Engineers, IS/IT managers, Auditors, and Risk committee. These IS/IT personnel work for organizations that are involved in cyber-security activities. This means that in every cyber-security activity, each actor has a role. The roles were delegated or voluntarily. On the other hand, the non-technical include business personnel, end-users, business managers, clients and partners.

The statements made by participant L137-139_P1_LenJo and participant L163-167_P2_HollanRaph, referring to 'Users' and 'ICT staff,' respectively, demonstrate the involvement of human actors (technical and non-technical) in the organization's cybersecurity landscape. While some individuals are susceptible to falling victim to cyber-attacks, others with more technical skills participate in policy development. This indicates the diverse roles and implications of human actors within the organization's cyber-security.

...as you investigate, then you realize that it's an internal thing. We have had incidents where Users lack of knowledge. They would fall victim of phishing type of attacks (L137-139_P1_LenJo)

...so we have our acceptable use policy, which covers quite a few items. Then the more technical policies are for ICT, ICT staff members to implement. So we haven't had feedback that it's not reader friendly, maybe in terms of length, they might be a bit lengthy (L163-167_P2_HollanRaph)

Non-human actors

- Non-human actors that are directly or indirectly implicated in cyber-security organizations includes Cyber-security policies, Phishing exercises, Computer Systems and Networks.

- Cyber-security Policies – this includes written policies and guidelines used for compliance, control or manage the security of the organization's information systems and data.
- Phishing Exercises – this includes the Simulated phishing emails sent to employees.
- Computer Systems and Networks – this includes personal computers (PCs), security and network infrastructures (such as firewall), software, anti-virus tools.
- The security awareness programs – this includes all the initiatives designed to inform and educate the organization personnel about potential threats and best practices to maintain security.

Participant L245-250_P2_HollanRaph indicates the involvement of non-human actors in cyber-security processes through phishing exercises and generating reports. In this context non-human actors refer to technologies, policies and other programs used in develop phishing exercises and reports.

...It is through the phishing exercises. So they have been quarterly and we do get reports on it to tell us how many people clicked on the link. It would tell us specifically which department, what information they divulged. So that gives us an indication, and then we're able to target per area specific training for those individuals (L245-250_P2_HollanRaph)

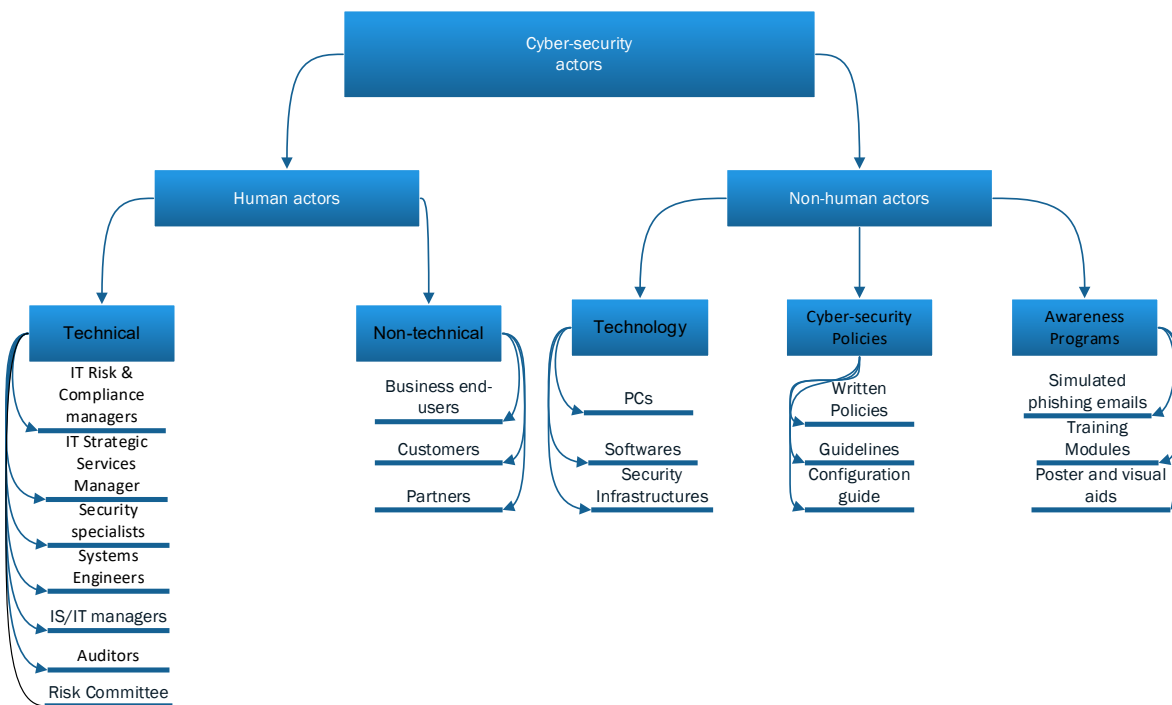


Figure 4.1 Cyber-security actors

There is no cyber-security in isolation. Actors have relationships and interact in each cyber-security activity. The relationships are either in a group (network) or groups, or individually.

4.3.2. Actor-Network

A network is an established connection between actors with the main purpose of allowing them to collaborate and have an inclusive work approach in order to solve a problem or create new entities (Iyamu & Sekgweleo, 2013). This means that a network can consist of both natures of actors (such as software and personnel). Also, from ANT perspective, networks are heterogeneous, which means they are composed of diverse types of actors and an actor can be part of one or more networks.

In the course of cyber-security policy compliance, there exist actor-networks. Some of the major networks as shown in Figure 4.2 are as follows:

- Organization – This can be private and public company in South Africa.
- Risk Committee – this consists of people with a background in information technology, risk management, cyber-security, or any other related technical fields in an organization. Their role is to review and approve proposed policies.
- IT Managers – These are IT employees with leadership and responsibilities of monitoring, coordinating, and enforcing IT systems, procedures, and policies.
- Business managers – These are employees with the responsibilities of aligning other business personnel with the goals of the company by overseeing and supervising their activities.
- Technologists – This is a group of experts in technology and consists of network administrators, software developers, IT engineers, IT researchers, and hackers.
- End-users – This includes IT personnel and non-IT personnel that make use of systems within an organization.

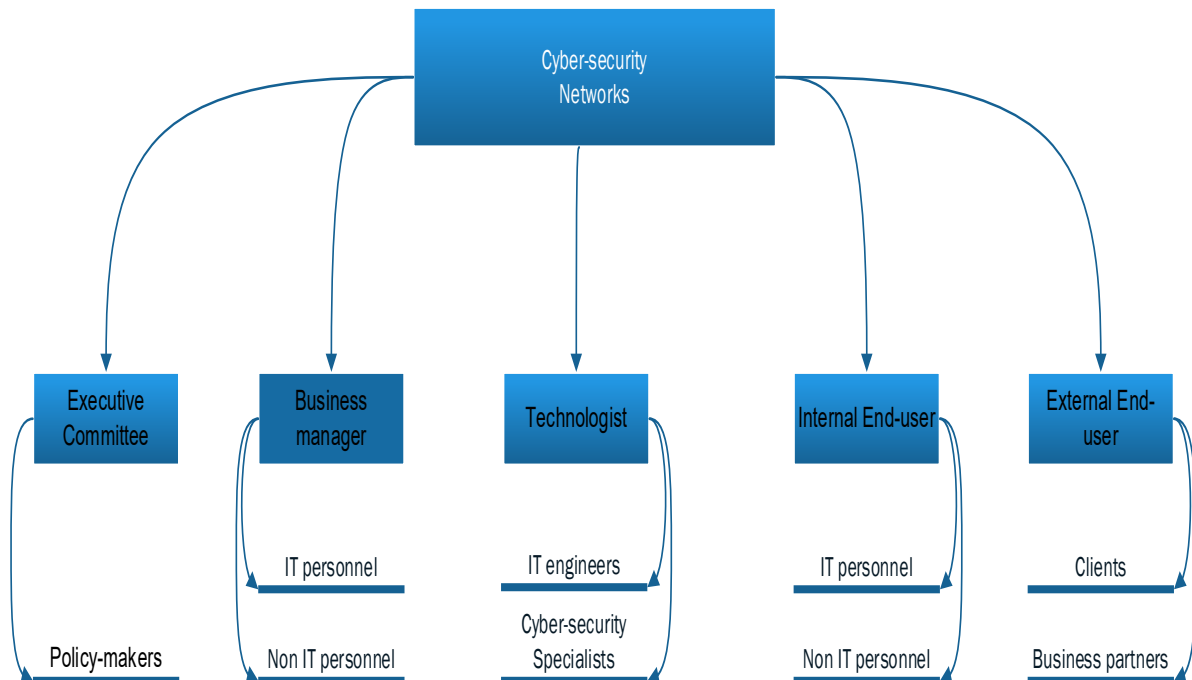


Figure 4.2 Cyber-security networks

As shown in Figure 4.2, the different actor-networks have roles and responsibilities. These are employed in the mitigation and management of cyber-security policies. The networks are briefly described as follows:

- Executive committee: Executive team are employees with leadership responsibilities. They are problem solvers and decision makers, the ones in charge of drafting the organization cyber-security policy and the rules to be communicated and complied with. They also have the responsibility to make sure that organization cyber-security policy and standards are respected.
- Managers: Business managers are the organization's employees with the responsibilities of overseeing business activities. This is primarily to ensure that other employees comply with processes and adhere to policies and standards towards achieving business objectives.
- Technologists: The technologists consist of specialists in cyber-security such as IT engineers and Security Specialists. This includes those who develop (training) from a technological perspective about cyber-security activities, and those who develop methods to impact organizations.
- Internal end-users: These are groups of users (all employees) who make use of organizational information systems and technology devices, such as PCs and terminals.
- External end-user: Business external end-users are mostly clients and partners purchasing and making use of services provided by organizations. These external end-users are also sometimes victims of cyber-attacks and incidents.

4.4 THE FOUR MOMENTS OF TRANSLATION

In ANT, translation is concerned with negotiations that occur within networks. The negotiations are shaped by the interactions that happen among actors, which are influenced by various interests. Based on the negotiations and activities transformations are observed within organizations. There are four moments in the process of translation: Problematisation, Interessement, Enrolment and Mobilisation (Wæraas & Nielsen, 2016).

4.4.1 Problematisation

As described by Jessen and Jessen (2014), this is where the focal actor(s) identify and define the problem. In the context of ANT, a problem is not necessarily a broken thing, but requires a solution, in cases an improvement (Iyamu & Mgudlwa, 2018). Organizations are challenged with cyber-attacks and incidents particularly with insider threats and phishing attempts type. Those

insider threats and phishing attempts were from different sources. Some of the sources were internal and others external. The internal sources were related to the end-users 'behaviors and were either conscious or unconscious. Irrespective of the consciousness or the unconsciousness of end-users 'behaviors, cyber-attacks and incidents such as phishing attacks and insider threats were occasioned.

Insider threats and phishing attempts represent a significant cyber-security problem for organizations. Thus, there is a need for effective measures to address the problem. The other existing problem is the behavioral challenges. As stated by a participant, despite several awareness materials put in place by organizations, it is still difficult to instigate a change of mind among end-users. According to another participant, the lack of compliance with existing cyber-security policies poses a critical problem.

So, the current attack we experience mostly is around phishing. We get a significant amount of phishing attempts. Directed to staff and directed to students. That dominate our cybersecurity awareness efficiency because if I look at the incidents we experienced over the past years, the 90% of those would be phishing related cyber incidents (L49-54_P1_NoahGabi)

... the challenges are you could say it's behavioral challenges. Just a change in mindset, because you, we do share quite a few awareness materials. So, and on quite a few platforms, but we still have end-users that would fall for a phishing attempt, you know? given the kinds of initiatives that we're trying to put in place, you would expect that there would be quite a bit of improvement in the behavior. that's one of the challenges. L220-227_P2_HollanRaph

4.4.2 Interessement

Interessement phase starts from the moment a problem is identified. At this phase, the links between the interests of different actors and allies are aligned and strengthened (Wæraas & Nielsen, 2016). The alignment of actor's interests is done through negotiations. The negotiations are based on each actor interests and the roles they may play in the network. To do so, focal actor (s) explain to others and allies how their own goals can be achieved by joining the network. As described by Iyamu and Mgudlwa (2018), this phase is important because the alignment of different interests

can contribute to addressing what was problematized. Additionally, the interests are various and can be expressed in different ways. For some people, the interests can be based on their obligations, positions or/and duties in an organization. For others, the interests can be based on their business goals, passions or the implications that cyber-security security policy or cyber-attacks and incidents could have on them.

Some organizations are facing difficulties in enforcing their cyber-security policies. As emphasized by a participant, this is due to the nature of the environment in some organizations particularly those having multiple natures of end-users in their environment. Unlike sectors such as healthcare and banking, the educational sector faces challenges to enforce its cyber-security policies. Using the one-size-fits-all method for awareness program or materials has not been working. So, there is a need for a different approach that could accommodate various nature of end-users. In this context, failing to tailor an awareness approach for all nature of end-users is a focal point of interest for cyber-security makers.

I've worked in many different organizations, and when you take a banking environment or where it's very regulated, right? Or a mining, one of the mining organizations, it's enforced in terms of compliance awareness exercises. if you don't do the training, there's repercussions for that. You don't, you're locked out of your computer. But it's a different environment and we are unable to enforce those kinds of hard and first rules to say we'll lock you out because we're working with students and lecturers. So, business needs to continue. So, it's a bit of a balancing act. (L229-237_P1_ HollanRaph).

Compliance is always a challenge. The fact that we are a higher education structure so there is that idea of openness for collaboration that we encourage: and the difficulties what that is that it creates complexity and create challenges because we are not dealing with one state of staffs. We are dealing with many different types of staff such as academics, students, and many others and think that is the challenge. The challenge is tailoring a program that suits everyone. So, you need to engage with people on a regular basis so I think there is difficulty in compliance with that because you get to deal with such a broad

circle of people. I think that is the challenge that we are looking into and actively trying to address. (L88-98_P1_ NoahGabi).

4.4.3 Enrolment

Enrolment is a critical phase in the process of translation. In this phase, actors are brought together in the same network with a common purpose of finding an effective measure to address the identified problem. It also about developing alliances and investigative how the actors align in the common objective of developing an effective cyber-security policy and awareness programs. to enforce to educate and inform end-users with the final aim to enforce. Furthermore, the existence of cyber-security policy, awareness programs such as simulated phishing emails indicate an enrolment and organizations in the objective of addressing the problem. Another point is to motivate those who do not really understand the criticality behind the whole intention of securing the systems. A participant highlighted that the reluctance of those actors is based on the approach used when communicating with them. The participant continued saying that they sometimes have to involve politics to stimulate them.

Well, I'm the risk and compliance manager in ICT. I look after the governance, so any ICT policies, frameworks, standards, processes and procedures (L51-53_P1_ HollanRaph).

I'll give you an example, you walk to a person and say, listen, I need to check that your antivirus endpoint firewall is up and running. They are not going to like it because they are busy, but when you say listen If I don't do this, when you are doing your own personal online banking, people are going to be able to see your credentials and take your money. Then suddenly change because it's no longer I think You're wasting my time, but it's about their money or their wellbeing. (L410-416_P1_ LenJo).

4.4.4 Mobilization

The mobilization is the last phase and it takes place when the problematisation, interessement and enrolment phases are completed (Costa & Cunha, 2015). This phase is important because it is where the main actor makes sure that others behave in respect of their assigned roles and

responsibilities (Jessen & Jessen, 2014). Mobilisation phase also aims to mobilize developed networks and maintained proposed solutions to effectively address identified problems. The purpose of that mobilization was to keep other end-users focused and conscious about the issues of cyber threats in particular phishing attempts and insider threats. This was done through the organization cyber-security policies and activities like phishing exercises conducted quarterly. Phishing exercises were used to evaluate the level of compliance or vigilance of actors such as end-users. This also helped to assess their capability of detecting potential cyber threats. Then collected outcomes could be an important resource as it highlighted gaps and pointed out where more attention was needed. Once those gaps are identified, improvement could be made in the following cyber-security policies and awareness materials.

It is through fishing exercises. So, they have been quarterly and we do get reports on it would tell us how many people clicked on the on the link. It would tell us who specifically which department, what information they divulged. So that gives us an indication. And then we're able to target per area specific training for those individuals. (L245-250_P2_ HollanRaph).

4.5 FINDINGS

In this section, important findings about cyber-security policy and cyber-attacks and incidents faced by some South African organizations are presented. These factors are results of the analysis presented in analysis sections and are as follows: Insider Threats; Phishing Attempts; Behavioral Challenges; Enforcement Limitations; Phishing Exercises; Policy Development Process. These findings are presented and described in Table 4.1. Both insider Threats, involving staff or internal end-users, and Phishing Attempts perpetrated by external individuals, pose significant risks to organizations. Despite awareness initiatives, behavioral challenges persist among internal end-users, which complicate adherence to available security measures. A one-size-fit cyber-security policies are sometimes inadequate due to the diversity in business sectors, necessitating a tailored solution. Periodic phishing exercises serve to evaluate the readiness of internal end-users or staff, and identify areas for improvements. Ultimately, for effectiveness, cyber-security policies development process should follow a collaborative and inclusive approach where organization stakeholders will be participating.

Table 4.1 Findings

Findings	Description
Behavioral challenges	This refers to end-users 'attitude and behavior towards cyber-security measures initiated by organizations. This includes resistance to comply with cyber-security policies and falling for phishing attempts.
Enforcement limitations	This refers to a lack of suitable cyber-security policy and awareness programs that fit the various nature of end-users existing in the organization.
Insider threats	Conscious and unconscious cyber risks generated from organization personnel or internal end-users.
Phishing attempts	Fraudulent attempts to still critical data like end-users or staff login credentials. These attempts are mostly in the form of emails or SMS.
Phishing exercises	This refers to the process of simulating real world phishing attacks. It aims to test the readiness of organization staff or end-users to identify cyber threats such as phishing emails. This also serves to evaluate the effectiveness of current awareness programs.
Policy development process	This refers to the process of developing a suitable cyber-security policy. This process should consider all phases (drafting, review, and approval), involve and collaborate with relevant stakeholders in order to deliver a cyber-security policy that meets the organization's context.

Table 4.1 concretises the findings of the study. The listed outcomes resulted from analysis of feedback from four participating representatives representing three associated organizations.

4.6 SUMMARY

In this chapter, a comprehensive analysis was presented. The analysis was based on qualitative data collected from participants with enough experience and working around cyber-security concepts. Throughout the analysis process, Actor-Network Theory from the perspective of its four moments of translation (Problematisation, Interessement, Enrolment, and Mobilisation) was used as lens to guide the analysis. As recommended by ANT, actors (human and non-human) involved in cyber-security policy were identified and categorized. Then existing networks were traced with a focus on actor-network relationships and negotiations that occur within networks. The results of this analysis allowed to identify cyber-attack and incidents registered by organizations, to understand factors that influence and cause lack of compliance with cyber-security policies in organizations, and to examine how cyber-security policy compliance is enforced in organizations as per this study objective. As presented in Table 4.1, the analysis revealed the following findings: Insider Threats; Phishing Attempts; Behavioral Challenges; Enforcement Limitations; Phishing Exercises; Policy Development Process.

CHAPTER FIVE: CONCLUSION AND RECOMMENDATIONS

Chapter Five concludes the study. It addresses closure in seven sections, namely:

- Introduction (5.1).
- Summary of findings and answering the research questions (5.2).
- Contribution of the research (5.3).
- Limitations of the study (5.4).
- Suggestions for future research (5.5).
- Conclusion (5.6)
- Recommendations (5.7).

5.1 INTRODUCTION

This section presents the study conclusion by reminding what was its objective, overviewing the findings and proving answers to the research questions. Additionally, this conclusion also highlights the limitations of the study and suggests recommendations for future studies.

This study aimed to analyze the level of compliance with cyber-security policies in organizations and to understand the factors influencing this compliance. In order to address the aim of this study, the following research questions were formulated as follows:

- I. What are the cyber-attacks and incidents that affect organizations?
- II. What are the contributing and influencing factors to the non-compliance with cyber-security policies in organizations?
- III. How is cyber-security policy compliance enforced in organizations?

The study was underpinned by the Interpretivism research philosophy, inductive research approach and qualitative research method were adopted. Case study research design was used, and data were collected through interviews (semi-structured). Additionally, documentation to supplement interviews was considered when provided. Finally, Actor-Network Theory (ANT) from the perspective of its four moments of translations (Problematization, Interessement, Enrolment, Mobilisation) was used as a lens to guide the entire process of data analysis.

5.2 SUMMARY OF FINDINGS AND ANSWERING RESEARCH QUESTIONS

5.2.1 Summary of Findings

The following is a summary of the findings obtained from the processed qualitative analysis:

- **Behavioral Challenges:** This refers to end-users 'attitude and behavior towards cyber-security measures initiated by organizations. This includes resistance to complying with cyber-security policies and falling for phishing attempts.
- **Enforcement Limitations:** This refers to a lack of suitable cyber-security policy and awareness programs that fit the various nature of end-users existing in the organization.
- **Insider Threats:** Conscious and unconscious cyber risks generated from organization personnel or internal end-users.
- **Phishing Attempts:** Fraudulent attempts to steal sensitive information such as end-users or staff login credentials. These attempts are mostly in the form of emails or SMS.
- **Phishing Exercises:** This refers to the process of simulating real world phishing attacks. It aims to test the readiness of organization staff or end-users to identify cyber threats such as phishing emails. This also serves to evaluate the effectiveness of current awareness programs.
- **Policy Development Process:** This refers to the process of developing a suitable cyber-security policy. This process should consider all phases (drafting, review, and approval), involve and collaborate with relevant stakeholders in order to deliver a cyber-security policy that meets the organization's context.

5.2.2 Answers to research questions

Research sub-question 1

I. What are the cyber-attacks and incidents that affect organizations?

The analysis conducted in Section 4.3 showed that organizations are particularly challenged with:

- **Insider Threats:** The analysis also revealed that Insider Threats involved staff or internal end-users with authorized access, and their occurrence was either conscious or unconscious.
- **Phishing Attempts:** On the other hand, usually in the form of email or SMS, Phishing Attempts were fraudulent attempts perpetrated by external individuals with the intention to steal sensitive information such as end-users or staff login credentials.

Research sub-question 2

II. What are the factors that influence and contribute to the non-compliance with cyber-security policies in organizations?

The analysis showed that the factors influencing and contributing to the non-compliance with the organization cyber-security policies are:

- **Behavioral Challenged:** The Behavioral Challenges is about internal end-user's mindsets, their attitude towards proposed cyber-security policies. Despite awareness initiatives taken by organizations, internal end-users were not adhering to the security measures available to them.
- **Enforcement Limitations:** The enforcement of Limitations is the fact that some organizations are failing to develop adequate and balanced cyber-security policies to meet their heterogeneous environment contexts. Proposed policies are sometimes not suitable for the business sector they are in. Consequently, all internal end-users cannot be targeted. For example, higher educational and banking type environments cannot consider similar aspects when developing cyber-security policies and awareness programs. Some organizations cannot have a one-size-fit cyber-security policy.

Research sub-question 3

III. How is cyber-security policy compliance enforced in organizations?

According to analysis provided in Section 4.3, organization enforce their cyber-security policy compliance using:

- **Phishing exercises:** The analysis revealed that periodically, phishing exercises such as simulated phishing emails were initiated. The main purpose of this approach was to evaluate the readiness of internal end-users or staff, to see if they are well equipped and capable of identifying and avoiding falling into some types of cyber threats. Furthermore, phishing exercise reports could indicate where improvement is needed in current proposed solutions.
- **Policy Development Process:** The analysis showed that cyber-security policies development process should follow a collaborative and inclusive approach where organization stakeholders will be participating. In such a process, potential policies should be drafted first, reviewed, and then submitted for approval.

5.3 CONTRIBUTION OF THE RESEARCH

5.3.1 Theoretical contributions

The study also contributes to the academic literature, especially the fact that very little has been done in the area of cyber-security studies through ANT concept especially using the four moments of translation.

5.3.2 Practical contributions

This study is important as, we hope, the result will continuously assist organizations with their cyber-security policy challenges and the persistently growing cyber-attacks and incidents. The findings could be used to better understand these challenges and develop more contextualized cyber-security policies to fit organization environments.

5.4 LIMITATIONS OF THE STUDY

Due to the sensitivity of the topic, some organizations were reluctant to participate in the study. Thus, this study was limited in terms of participants. The researcher emphasizes the concept of caution transferability of findings. The researcher suggests that the results of this study should be applicable to organizations with similar settings.

5.5 SUGGESTIONS FOR FUTURE RESEARCH

The analysis presented in this study reveals that one of the challenges faced by organizations is the enforcement limitations. Meaning some organizations do not have the capacity or are failing to develop cyber-security policies suitable for their environment. Based on this, it would be interesting to select two different sectors and then conduct a comparative analysis.

5.6 CONCLUSION

The benefit of this study is two-fold comprising both theoretical and practical facets. From a theoretical point of view, the study added to the body of knowledge because little literatures exist in the domain of cyber-security using Actor-Network Theory (ANT) especially from the perspective of its four moments of translation (Problematization, Interessement, Enrolment, and Mobilisation). This study reveals how the four moments of translation can be used to 1) identify cyber-attack and incidents registered by organizations; 2) to understand factors that influence and contribute to the non-compliance with cyber-security policies in organizations; and 3) To examine how cyber-security policy compliance is enforced in organizations. From a practical point of view, through its findings, this study contributes to the persistent cyber-security challenges faced by organizations.

5.7 RECOMMENDATIONS

Another study could be conducted using a bigger sample of participants to see if the perspective provided by the findings of this study will remain the same or not. Another research could be conducted in the same study but using a different tenant of ANT such as Black Box to unpack the concept of cyber-security policy to provide more insights for policymakers and cyber-security specialists.

REFERENCES

- Abawajy, J. 2014. User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, 33(3):237-248.
- Aboelmaged, M. & Gebba, T.R. 2013. Mobile banking adoption: an examination of technology acceptance model and theory of planned behavior. *International Journal of Business Research and Development*, 2(1): 35-50.
- Albrechtsen, E. & Hovden, J. 2010. Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security*, 29(4): 432-445.
- Alexander, P.M. and Silvis, E., 2014. Actor-network theory in information systems research. *Information Research*, 19(2).
- Amini, M. & Bozorgasl, Z. 2023. A Game Theory Method to Cyber-Threat Information Sharing in Cloud Computing Technology. *International Journal of Computer Science and Engineering Research*, 11: 4-2023.
- Antwi, S.K. & Hamza, K. 2015. Qualitative and quantitative research paradigms in business research: A philosophical reflection. *European Journal of Business and Management*, 7(3): 217-225.
- Arachchilage, N.A.G. & Love, S. 2014. Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, 38: 304-312.
- Bachlechner, D., Maier, R., Innerhofer-Oberperfler, F. and Demetz, L. 2011. UNDERSTANDING THE MANAGEMENT OF INFORMATION SECURITY CONTROLS IN PRACTICE. In 9th Australian Information Security Management Conference: 40.
- Bada, M. & Sasse, A. 2014. Cyber Security Awareness Campaigns: Why do they fail to change behaviour?. Global Cyber Security Capacity Centre, University of Oxford.

- Balzacq, T. & Cavelt, M.D. 2016. A theory of actor-network for cyber-security. *European Journal of International Security*, 1(02):176-198.
- Baxter, P. & Jack, S. 2008. Qualitative case study methodology: Study design and implementation for novice researchers. *The qualitative report*, 13(4): 544-559.
- Bayo-Moriones, A., Billón, M. & Lera-López, F. 2013. Perceived performance effects of ICT in manufacturing SMEs. *Industrial Management & Data Systems*, 113(1): 117-135.
- Bayuk, J.L., Healey, J., Rohmeyer, P., Sachs, M.H., Schmidt, J. & Weiss, J. 2012. *Cyber security policy guidebook*. John Wiley & Sons.
- Ben-Asher, N. & Gonzalez, C. 2015. Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, 48:51-61.
- Blythe, J. 2013. Cyber security in the workplace: Understanding and promoting behaviour change. *Proceedings of CHIItaly 2013 Doctoral Consortium*, 1065: 92-101.
- Boote, D. N. & Beile, P. 2005. Scholars before researchers: On the centrality of the Dissertation literature review in research preparation. *Educational Researcher* , 34 (6): 3-15.
- Botha, J.G., Eloff, M.M. & Swart, I. 2015, August. The effects of the PoPI Act on small and medium enterprises in South Africa. In *Information Security for South Africa (ISSA), 2015*: 1-8. IEEE.
- Bowen, G.A. 2009. Document analysis as a qualitative research method. *Qualitative research journal*, 9(2): 27-40.
- Brannen, J. 2017. *Mixing methods: Qualitative and quantitative research*. Routledge
- Brinkmann, S. 2014. Interview. In *Encyclopedia of critical psychology*; 1008-1010. Springer New York.

- Bulgurcu, B., Cavusoglu, H. & Benbasat, I. 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 34(3): 523-548.
- Byres, E. & Lowe, J. 2004. The myths and facts behind cyber security risks for industrial control systems. In *Proceedings of the VDE Kongress*, 116: 213-218.
- Callon, M. 1986. Some elements of a sociology of translation: domestication of the scallops and the fishermen of St Briec Bay. In *Power, Action and Belief*: 196-233.
- Carlton, M. 2016. Development of a Cybersecurity Skills Index: A Scenarios-Based, Hands-On Measure of Non-IT Professionals' Cybersecurity Skills, Doctoral dissertation, Nova Southeastern University.
- Cavelty, M.D. 2014. Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and Engineering Ethics*, 20(3): 701-715.
- Chen, W. & Hirschheim, R. 2004. A paradigmatic and methodological examination of information systems research from 1991 to 2001. *Information systems journal*, 14(3): 197-235.
- Chowdhury, M.F. 2014. Interpretivism in aiding our understanding of the contemporary social world. *Open Journal of Philosophy*, 4(03).
- Citizen. 2018. Presidency website back up after hack. <https://citizen.co.za/news/south-africa/1972813/presidency-website-back-up-after-hack/> [4 April 2019].
- Cochran, T. 2013. *How to Ensure Your Technology is Secure, Stable and Scalable*. <https://www.entrepreneur.com/article/229909> [23 Jun 2018].
- Cong, H., Dang, D., Brennan, L. & Richardson, J. 2017. Information Security and People: A Conundrum for Compliance. *Australasian Journal of Information Systems*, 21: 1-16.

- Costa, C. & Cunha, P. 2015. The social dimension of business models: an Actor-Network Theory perspective. In Twenty-first Americas Conference on Information Systems, Puerto Rico, August 13-15, 2015: 1-12.
- Cresswell, K.M., Worth, A. & Sheikh, A. 2010. Actor-Network Theory and its role in understanding the implementation of information technology developments in healthcare. *BMC medical informatics and decision making*, 10(1):67.
- Creswell, J.W. 2013. *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.
- Czarniawska, B. 2016. Actor-Network Theory. In Langley, A. and Tsoukas, H. (eds). *The Sage handbook of process organization studies*. Sage: 160-173.
- Czosseck, C., Ottis, R. & Talihärm, A.M. 2011. Estonia-after-the-2007-Cyber-Attacks. *International Journal of Cyber Warfare and Terrorism*, 1(1): 24–34.
- Da Veiga, A. 2015. An Information Security Training and Awareness Approach (ISTAAP) to instil an information security-positive culture. *Proceedings of the ninth international symposium on human aspects of information security and assurance (HAISA 2015), 1-3 July 2015*. Mytilene: 95-107.
- Dankert, R. 2010. Using Actor–Network Theory (ANT) doing research (Online). www.ritskedankert.nl/publications.
- De Bruyn, M. 2014. The Protection Of Personal Information (POPI) Act-Impact On South Africa. *The International Business & Economics Research Journal (Online)*, 13(6):1315.
- De Massis, A. & Kotlar, J. 2014. The case study method in family business research: Guidelines for qualitative scholarship. *Journal of Family Business Strategy*, 5(1): 15-29.
- De Massis, A. & Kotlar, J. 2014. The case study method in family business research: Guidelines for qualitative scholarship. *Journal of Family Business Strategy*, 5(1):15-29.
- De Vaus, D.A. & De Vaus, D. 2001. *Research design in social research*. Sage.

- Dedeke, A.N. 2017. Creating sustainable tourism ventures in protected areas: An actor-network theory analysis. *Tourism management*, 61: 161-172.
- Degu G. & Yigzaw T. 2006. Lecture Notes For Health Science Students Research Methodology: University of Gondar In collaboration with the 87 Ethiopia Public Health Training Initiative, The Carter Center, the Ethiopia Ministry of Health, and the Ethiopia Ministry of Education 2006, 1-68.
- Denning, D.E. 2015. Rethinking the cyber domain and deterrence. *Joint Forces Quarterly*, 1: 8-15.
- Dlamini, Z. & Modise, M. 2013. Cyber security awareness initiatives in South Africa: A synergy approach. *Case Stud. Inf. Warf. Secur. Res. Teach. Stud*: 1.
- Doody, O. & Noonan, M. 2013. Preparing and conducting interviews to collect data. *Nurse researcher*, 20(5): 28-32.
- Dunn Caveltly, M. 2014. Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Sci Eng Ethics* , 20: 701–715.
- Edwards, S. 2014. Doing actor-network theory: integrating network analysis with empirical philosophy in the study of research into genetically modified organisms in New Zealand. Doctoral dissertation, Lincoln University.
- Efrony, D. 2017. The Cyber Domain, Cyber Security and what about the International Law? https://csrcl.huji.ac.il/sites/default/files/csrcl/files/dan_efrony.pdf [20 July 2018]
- Eisenhardt, K. M. 1989. Building theories from case study research. *Academy of Management Review*, 14(4): 532-550
- Elmusharaf, K. 2012. Qualitative Data Collection Techniques. *Training Course in Sexual and Reproductive Health Research. Geneva.*
- Evans, M., Maglaras, L.A., He, Y. & Janicke, H. 2016. Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks*, 9(17):4667-4679.

- Farooq, M.U., Waseem, M., Khairi, A. & Mazhar, S. 2015. A critical analysis on the security concerns of internet of things (IoT). *International Journal of Computer Applications*, 111(7).
- Fassinger, R. & Morrow, S.L. 2013. Toward best practices in quantitative, qualitative, and mixed-method research: A social justice perspective. *Journal for Social Action in Counseling and Psychology*, 5(2): 69-83.
- Felski, R. 2016. comparison and translation: a perspective from actor-network theory. *comparative literature studies*, 53(4): 747-765.
- Ferreira, F. W. 2012. *NIST Publishes Computer Security Incident Handling Guide*.
<https://www.hlregulation.com/2012/08/16/nist-publishes-computer-security-incident-handling-guide/> [22 Jun 2018]
- Flores, W.R. Antonsen, E. & Ekstedt, M. 2014. Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, 43: 90-110.
- Fornazin, M. & Joia, L.A. 2016, September. Techno-government networks: Actor-Network Theory in electronic government research. In *International Conference on Electronic Government and the Information Systems Perspective*. Springer International Publishing: 188-199.
- Frauenberger, C., Rauhala, M. & Fitzpatrick, G. 2016. In-action ethics. *Interacting with Computers*, 29(2): 220-236.
- Gálik, S. 2016. Being and time in online communication. *European Journal of Science and Theology*, 12(5):5-14.
- Gao, Z. 2023. Development and application of web information system in enterprise management under SSH framework. *Journal of Information Systems Engineering and Management*, 8(2): 22733.

- Gcaza, N. & Von Solms, R. 2017. A Strategy for a Cybersecurity Culture: A South African Perspective. *The Electronic Journal of Information Systems in Developing Countries*, 80(1): 1-17.
- Gcaza, N., von Solms, R. & van Vuuren, J.J. 2015. An Ontology for a National Cyber-Security Culture Environment. In *HAlSA*: 1-10.
- Gill, P., Stewart, K., Treasure, E. & Chadwick, B. 2008. Methods of data collection in qualitative research: interviews and focus groups. *British dental journal*, 204(6): 291-295.
- Goswami, U. 2010. Inductive & deductive reasoning. *The Wiley-Blackwell Handbook of Childhood Cognitive Development, Second edition*: 399-419.
- Greenhalgh, T. & Stones, R. 2010. Theorising big IT programmes in healthcare: strong structuration theory meets actor-network theory. *Social science & medicine*, 70(9): 1285-1294.
- Greenhough, B.J. 2016. Actor-Network Theory. *International Encyclopedia of Geography: People, the Earth, Environment and Technology: People, the Earth, Environment and Technology*: 1-7.
- Greenhough, B.J. 2016. Actor-Network Theory. *International Encyclopedia of Geography: People, the Earth, Environment and Technology: People, the Earth, Environment and Technology*: 1-7.
- Grobler, M. and Dlamini, Z. 2012. Global cyber trends: A South African reality. In: *IST-Africa 2012*. Dar es Salaam, Tanzania, 9-11 May 2012.
- Gundu, T. 2019, February. Acknowledging and reducing the knowing and doing gap in employee cybersecurity compliance. In *ICCWS 2019 14th International Conference on Cyber Warfare and Security*: 94-102.
- Gutiérrez, J.L.M. 2023. On actor-network theory and algorithms: ChatGPT and the new power relationships in the age of AI. *AI and Ethics*:1-14.

- Hampton N, Baig Z.A. 2015. Ransomware: emergence of the cyber-extortion menace. In: Australian Information Security Management Conference, Perth, Australia, 2015, 11: 10.
- Hancock, D.R. & Algozzine, B. 2016. *Doing case study research: A practical guide for beginning researchers*. Teachers College Press.
- Hanseth, O., Aanestad, M. & Berg, M. 2004. Guest editors' introduction: Actor-network theory and information systems. What's so special?. *Information Technology & People*, 17(2): 116-123.
- Heeks, R. & Stanforth, C. 2015. Technological change in developing countries: opening the black box of process using actor–network theory. *Development Studies Research*, 2(1): 33-50.
- Henwood, K. 2014. Qualitative research. *Encyclopedia of Critical Psychology*: 1611-1614.
- Herrera, A.V., Ron, M. & Rabadão, C. 2017. National cyber-security policies oriented to BYOD (bring your own device): Systematic review. In *Information Systems and Technologies (CISTI), 2017 12th Iberian Conference on* :1-4. IEEE.
- Hong, J., Nuqui, R., Ishchenko, D., Wang, Z., Cui, T., Kondabathini, A., Coats, D. & Kunsman, S.A. 2015. Cyber-physical security test bed: A platform for enabling collaborative cyber defense methods. In *PACWorld Americas Conference*.
- Hox, J.J. & Boeije, H.R. 2005. Data collection, primary versus secondary. *Encyclopedia of Social Measurement*, 1.: 593-599. Elsevier.
- Hruza, P., Sousek, R. and Szabo, S. 2014. Cyber-attacks and attack protection. *World Multi-Conference on Systemics*,18: 170-174.
- Hughes, B.B., Bohl, D., Irfan, M., Margolese-Malin, E. & Solórzano, J.R. 2017. ICT/Cyber benefits and costs: Reconciling competing perspectives on the current and future balance. *Technological Forecasting and Social Change*, 115:117-130.

- Hussein, A. 2015. The use of triangulation in social sciences research: Can qualitative and quantitative methods be combined?. *Journal of Comparative Social Work*, 4(1).
- Iyamu, T. & Mgudlwa, S. 2018. Transformation of healthcare big data through the lens of actor network theory. *International Journal of Healthcare Management*, 11(3):182-192.
- Iyamu, T. & Sekgweleo, T. 2013. Information systems and actor-network theory analysis. *International Journal of Actor-Network Theory and Technological Innovation (IJANTTI)*, 5(3): 1-11.
- Iyamu, T., Sekgweleo, T. & Mkhomazi, S.S. 2013, Actor Network Theory in Interpretative Research Approach. In *International Working Conference on Transfer and Diffusion of IT*: 605-610.
- Jacobs, P.C., von Solms, S.H. & Grobler, M.M. 2016. Towards a framework for the development of business cybersecurity capabilities. *The Business & Management Review*, 7(4):51.
- Jessen, J.D. & Jessen, C. 2014. Games as Actors Interaction, Play, Design, and Actor Network Theory.
- Jessen, J.D. & Jessen, C. 2014. What games do. *Proceedings of ACHI*, 978: 1-61208.
- Johar, A. 2017. *Internet security 101: Six ways hackers can attack you and how to stay safe*. <https://economictimes.indiatimes.com/tech/internet/internet-security-101-six-ways-hackers-can-attack-you-and-how-to-stay-safe/articleshow/61342742.cms> [22 August 2017]
- Johnston, A. 2014. Rigour in research: theory in the research approach. *European Business Review*, 26(3): 206-217.
- Junger, M., Montoya, L. & Overink, F.J. 2017. Priming and warnings are not effective to prevent social engineering attacks. *Computers in human behavior*, 66: 75-87.
- Justesen, L. 2020. Actor-Network Theory as an Analytical Approach. *Qualitative Analysis: Eight Approaches for the Social Sciences*. Thousand Oaks, Ca: SAGE: 327-244.

- Kaiser, R. 2015. The birth of cyberwar. *Political Geography*, 46: 11-20.
- Katz, G., Elovici, Y. & Shapira, B. 2014. CoBAn: A context based model for data leakage prevention. *Information sciences*, 262: 137-158.
- Kembro, J., Selviaridis, K. & Näslund, D. 2014. Theoretical perspectives on information sharing in supply chains: a systematic literature review and conceptual framework. *Supply Chain Management: An International Journal*, 19(5/6): 609-625.
- Kent, C., Tanner, M. & Kabanda, S. 2016, August. How South African SMEs address cyber security: The case of web server logs and intrusion detection. In *Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech)*, IEEE International Conference on.IEEE: 100-105
- Kesan, J.P. & Hayes, C.M. 2014. Creating a circle of trust to further digital privacy and cybersecurity goals. *Mich. St. L. Rev.*: 1475.
- Kigerl, A. 2012. Routine Activity Theory and the Determinants of High Cybercrime Countries. *Social Science Computer Review* : 470-486.
- Kortjan, N. & Von Solms, R. 2014. A conceptual framework for cyber-security awareness and education in SA. *South African Computer Journal*, 52(1):29-41.
- Kozlowski, A. 2014. Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan. *European Scientific Journal, ESJ*, 10(7).
- Kshetri, N. 2013. *Cybercrime and cybersecurity in the global south*. Palgrave Macmillan, UK..
- Kshetri, N. 2015. Cybercrime and Cybersecurity Issues in the BRICS Economies. *Journal of Global Information Technology Management*, 18(4): 245-249.
- Kshetri, N. 2019. Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management*, 22(2): 77-81.

- Kuhn, T. S. 1962. *The Structure of Scientific Revolutions*. Chicago, IL: University of Chicago Press.
- Kuipers, D. & Fabro, M. 2006. Control systems cyber security: Defense in depth strategies (No. INL/EXT-06-11478). Idaho National Laboratory (INL).
- Kumar, M., Meena, J., Singh, R. & Vardhan, M. 2015. Data outsourcing: A threat to confidentiality, integrity, and availability. In *Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on*: 1496-1501. IEEE.
- Kuzior, A. & Lobanova, A. 2020. Tools of information and communication technologies in ecological marketing under conditions of sustainable development in industrial regions (through examples of Poland and Ukraine). *Journal of risk and financial management*, 13(10): 238.
- Law, J. 1992. Notes on the theory of the actor-network: Ordering, strategy, and heterogeneity. *Systemic practice and action research*, 5(4): 379-393.
- Lewis, S. 2015. Qualitative inquiry and research design: Choosing among five approaches. *Health promotion practice*, 16(4).
- Li, Y. & Liu, Q. 2021. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, 7: 8176-8186.
- Linton, I. 2017. *The Benefits of Using ICTs in Business & Finance*. <https://bizfluent.com/list-6641121-benefits-using-icts-business-finance.html> [18 May 2017]
- Luijff, E., Besseling, K. & De Graaf, P. 2013. Nineteen national cyber security strategies. *International Journal of Critical Infrastructures* 6, 9(1-2): 3-31.
- Luo, Y. & Bu, J. 2016. How valuable is information and communication technology? A study of emerging economy enterprises. *Journal of World Business*, 51(2): 200-211.
- Lynch, J. 2005. Identity theft in cyberspace: Crime control methods and their effectiveness in combating phishing attacks. *Berkeley Tech. LJ*, 20: 259.

- Mabunda, S. 2021. Cybersecurity in South Africa: Towards Best Practices. *CyberBRICS*: 227-270.
- Machi, L.A. & McEvoy, B.T. 2016. *The literature review: Six steps to success*. Corwin Press.
- Mackenzie, N. & Knipe, S. 2006. Research dilemmas: Paradigms, methods and methodology. *Issues in educational research*, 16(2): 193-205.
- Mahama, H., Elbashir, M.Z., Sutton, S.G. & Arnold, V. 2016. A further interpretation of the relational agency of information systems: A research note. *International Journal of Accounting Information Systems*, 20: 16-25.
- Maier, H.R. 2013. What constitutes a good literature review and why does its quality matter?. *Environmental Modelling and Software*, 43: 3-4.
- Marczyk, G., DeMatteo, D. & Festinger, D. 2017. *Essentials of research design and methodology*. John Wiley.
- Mármol, F.G., Pérez, M.G. & Pérez, G.M. 2016. I don't trust ICT: Research challenges in cyber security. In *IFIP International Conference on Trust Management*. Springer International Publishing: 129-136.
- Marsh, D. 2017. Are Ethical Hackers the Best Solution for Combating the Growing World of Cyber-Crime? Unpublished Doctoral dissertation, University Honors College, Middle Tennessee State University.
- Merriam, S.B. & Tisdell, E.J. 2015. *Qualitative research: A guide to design and implementation*. John Wiley & Sons.
- Moghaddasi, H., Sajjadi, S. & Kamkarhaghighi, M. 2016. Reasons in Support of Data Security and Data Security Management as Two Independent Concepts: A New Model. *The open medical informatics journal*, 10: 4.
- Mosca, M. 2015. Cybersecurity in an era with quantum computers: will we be ready?. *IACR Cryptology ePrint Archive*: 1075.

- Mouton, F., Malan, M.M., Leenen, L. & Venter, H.S. 2014, August. Social engineering attack framework. In *Information Security for South Africa (ISSA), 2014*. IEEE: 1-9.
- Moyo, A. 2015. *End-users are juicy targets for hackers*.
<https://www.itweb.co.za/content/nG98YdqLRoj7X2PD> [28 April 2017]
- Mtambeka, P., Mtegha, C.Q., Chigona, W. & Tuyeni, T.T. 2023, May. Factors Affecting how University Students Comply with Cybersecurity Measures: A Case of South Africa. In *Proceedings of NEMISA Digital Skills Conference*, (5): 1-16.
- Naidoo, V. & Van Niekerk, B. 2014. Strategic information security management as a key tool in enhancing competitive advantage in South Africa. *Journal of Contemporary Management*, 11(1):33-46.
- Nduati, N.L., Ombui, K. & Kagiri, A. 2015. Factors affecting ICT adoption in small and medium enterprises in Thika town, Kenya. *European Journal of Business Management*, 2(3): 395-414.
- Ngulube, P. 2015. Qualitative data analysis and interpretation: systematic search for meaning. *Addressing research challenges: making headway for developing researchers*: 131-156.
- Niiniluoto, I. 2018. Peirce on Abduction. *Truth-Seeking by Abduction*: 1-18. Springer, Cham.
- Nye Jr, J.S. 2017. Deterrence and dissuasion in cyberspace. *International Security*, 41(3): 44-71.
- Olise, M.C., Anigbogu, T.U., Edoko, T.D. & Okoli, M.I. 2014. Determinants of ICT adoption for improved SME's performance in Anambra State, Nigeria. *American International Journal of Contemporary Research*, 4(7): 163-176.
- Patrick, H., van Niekerk, B. & Fields, Z. 2016. Security-Information Flow in the South African Public Sector. *Journal of Information Warfare*, 15(4): 68-V.

- Patten, M.L. & Newhart, M. 2017. *Understanding research methods: An overview of the essentials*. Taylor & Francis.
- Pearson, E. & Bethel, C.L. 2016. A design review: Concepts for mitigating SQL injection attacks. *4th International Symposium on Digital Forensic and Security (ISDFS)*.
- Pipyros, K., Mitrou, L., Gritzalis, D. & Apostolopoulos, T. 2014. A cyber attack evaluation methodology. In *Proc. of the 13th European Conference on Cyber Warfare and Security*: 264-270.
- Ponelis, S.R. 2015. Using interpretive qualitative case studies for exploratory research in doctoral studies: A case of Information Systems research in small and medium enterprises. *International Journal of Doctoral Studies*, 10(1): 535-550.
- Poon, P.L., Kuo, F.C., Liu, H. & Yueh Chen, T. 2014. How can non-technical end users effectively test their spreadsheets?. *Information Technology & People*, 27(4): 440-462.
- Punch, K.F. 2013. *Introduction to social research: Quantitative and qualitative approaches*. Sage.
- Qu, S.Q. & Dumay, J. 2011. The qualitative research interview. *Qualitative research in accounting & management*, 8(3): 238-264.
- Quaglia, F. 2016. Information and Communication Technology (ICT) and cyber threats: the main fields of analysis, Bachelor's thesis, UniversitàCa'FoscariVenezia.
- Quigley, K., Burns, C. & Stallard, K. 2015. 'Cyber Gurus': a rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection. *Government Information Quarterly*, 32(2): 108-117.
- Raiyn, J. 2014. A survey of cyber attack detection strategies. *International Journal of Security and Its Applications*, 8(1): 247-256.
- Ramírez, J.M. & García-Segura, L.A. 2017. *Cyberspace: Risks and Benefits for Society, Security and Development*. Springer.

- Rhodes, J. 2009. Using actor-network theory to trace an ICT (telecenter) implementation trajectory in an African women's micro-enterprise development organization. *Information Technologies & International Development*, 5(3):1-20.
- Rice, E.B. & AlMajali, A. 2014. Mitigating the risk of cyber attack on smart grid systems. *Procedia Computer Science*, 28: 575-582.
- Rouse, M. 2014. *Confidentiality, Integrity, and Availability (CIA triad)*.
<https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA> [25 August 2018].
- Sachdeva, M., Singh, G., Kumar, K. & Singh, K. 2010. DDOS Incidents and Their Impact: A Review. *The International Arab Journal of Information Technology*. 7(1).
- Safa, N.S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N.A. & Herawan, T. 2015. Information security conscious carebehaviour formation in organizations. *Computers & Security*, 53: 65-78.
- Safa, N.S., Von Solms, R. & Fitcher, L. 2016. Human aspects of information security in organisations. *Computer Fraud & Security*, 2016(2): 15-18.
- Said, H.M., Hamdy, M., El Gohary, R. & Salem, A.B.M. 2015. An integrated approach towards a penetration testing for cyberspaces. *European Journal of Computer Science and Information Technology*, 3(1): 108-128.
- Salvi, M.H.U. & Kerkar, M.R.V. 2016. Ransomware: A cyber extortion. *ASIAN JOURNAL FOR CONVERGENCE IN TECHNOLOGY (AJCT)-UGC LISTED*, 2.
- Sannicolas-Rocca, T., Schooley, B. & Spears, J.L. 2014, January. Designing effective knowledge transfer practices to improve IS security awareness and compliance. In *System Sciences (HICSS), 2014 47th Hawaii International Conference on*. IEEE: 3432-3441.
- Scarfone, K., Benigni, D. & Grance, T. 2009. Cyber Security Standards. *Wiley Handbook of Science and Technology for Homeland Security*.

- Scott, J. 2017. *Social Network Analysis*. London: Sage.
- Sheridan, K. 2017. *Financial Services Sector the #1 Target of Cybercriminals*.
<https://www.darkreading.com/endpoint/financial-services-sector-the--1-target-of-cybercriminals/d/d-id/1328775> [9 March 2017]
- Shim, Y. & Shin, D.H. 2016. Analyzing China's fintech industry from the perspective of actor-network theory. *Telecommunications Policy*, 40(2): 168-181.
- Sigholm, J. 2013. Non-state actors in cyberspace operations. *Journal of Military Studies*, 4(1):1-37.
- Skopik, F., Ma, Z., Smith, P. & Bleier, T. 2012. Designing a Cyber Attack Information System for National Situational Awareness. *Future Security*, 318: 277-288.
- Snedaker, S. 2013. *Business continuity and disaster recovery planning for IT professionals*. Newnes (2nd ed.). Syngress Publishing.
- Soiferman, L.K. 2010. Compare and Contrast Inductive and Deductive Research Approaches. University of Manitoba.
- Stage, F.K. & Manning, K. 2015. What is your research approach?. In *Research in the college context* : 29-54.
- Stockbruegger, J. & Bueger, C. 2017. Actor-Network Theory: Objects and actants, networks and narratives. In *Technology and World Politics*: 54-71. Routledge.
- Streeter, D.C. 2013. The effect of human error on modern security breaches. *Strategic Informer: Student Publication of the Strategic Intelligence Society*, 1(3): 2.
- Susanto, H., Kang, C.C. & Leu, F.Y. 2016. Revealing the Role of ICT for Business Core Redesign.
- Swart, I., Irwin, B. & Grobler, M. 2014. On the viability of pro-active automated PII breach detection: A South African case study. In *Proceedings of the Southern African Institute for*

*Computer Scientist and Information Technologists Annual Conference 2014 on SAICSIT
2014 Empowered by Technology: 251*

- Tang, J., Liu, J., Zhang, M. & Mei, Q. 2016, April. Visualizing large-scale and high-dimensional data. In *Proceedings of the 25th International Conference on World Wide Web*: 287-297.
- Tarutè, A. & Gatautis, R. 2014. ICT impact on SMEs performance. *Procedia-Social and Behavioral Sciences*, 110: 1218-1225.
- Tatnall, A. 2005. Actor-network theory in information systems research. In *Encyclopedia of Information Science and Technology, First Edition*: 42-46. IGI Global.
- Taylor, P. 2015. The importance of information and communication technologies (ICTs): An integration of the extant literature on ICT adoption in small and medium enterprises. *International Journal of Economics, Commerce and Management*, 3(5): 274-295.
- Taylor, S.J., Bogdan, R. & DeVault, M. 2015. *Introduction to qualitative research methods: A guidebook and resource*. John Wiley & Sons.
- Trautman, L.J. 2015. Cybersecurity: What About US Policy. *U. Ill. JL Tech. & Pol'y*: 341.
- Troshani, I. & Wickramasinghe, N. 2014, January. Tackling complexity in e-health with actor-network theory. In *System Sciences (HICSS), 2014 47th Hawaii International Conference on*.IEEE: 2994-3003.
- Tuli, F. 2011. The basis of distinction between qualitative and quantitative research in social science: Reflection on ontological, epistemological and methodological perspectives. *Ethiopian Journal of Education and Sciences*, 6(1).
- Uma, M. & Padmavathi, G. 2013. A Survey on Various Cyber Attacks and their Classification. *IJ Network Security*, 15(5): 390-396
- Van den Berg, J., Van Zoggel, J., Snels, M., Van Leeuwen, M., Boeke, S., van de Koppen, L., Van der Lubbe, J., Van den Berg, B. & De Bos, T. 2014. On (the Emergence of) Cyber

- Security Science and its Challenges for Cyber Security Education. In *Proceedings of the NATO IST-122 Cyber Security Science and Engineering Symposium*: 13-14.
- Van Heerden, R., Von Soms, S. & Mooi, R. 2016. Classification of cyber attacks in South Africa. In *IST-Africa Week Conference*. IEEE: 1-16.
- Van Slyke, C. & Belanger, F. 2003. *E-business technologies*. New York.
- Vicente, A. 2016. *SA is top cyber crime target in Africa*.
http://www.itweb.co.za/index.php?option=com_content&view=article&id=150566 [19 April 2017].
- von Faber, E. 2014. In-House Standardization of Security Measures: Necessity, Benefits and Realworld Obstructions. In *ISSE 2014 Securing Electronic Business Processes*: 35-48. Springer Vieweg.
- Von Solms, R. & Van Niekerk, J. 2013. From information security to cyber security. *Computers & security*, 38: 97-102.
- Vosloo, J. J. 2014. A Sport management programme for educator training in accordance with the diverse needs of South African Schools. PhD Thesis, North West University.
- Vroom, C. & Von Solms, R. 2004. Towards information security behavioural compliance. *Computers & Security*, 23(3):191-198.
- Wæraas, A. & Nielsen, J.A. 2016. Translation theory 'translated': Three perspectives on translation in organizational research. *International Journal of Management Reviews*, 18(3): 236-270.
- Wang, P., Xie, S. & Xu, H. 2023. Re-conceptualizing the ideal homes in rural China: an actor-network theory approach. *Humanities and Social Sciences Communications*, 10(1): 1-8.
- Walliman, N. 2017. *Research methods: The basics*. Routledge.

- Walsham, G. 1997. Actor-network theory and IS research: current status and future prospects. In *Information systems and qualitative research*: 466-480. Springer US.
- Wethington, E. & McDarby, M.L. 2016. Interview Methods (Structured, Semistructured, Unstructured). *The Encyclopedia of Adulthood and Aging*.
- Whittle, A. & Spicer, A. 2008. Is actor network theory critique?. *Organization studies*, 29(4): 611-629.
- Wiederhold, G. 2001. *Information sharing system and method with requester dependent sharing and security rules*. U.S. Patent 6,226,745.
- Wille, G. & Bradfield, G. 2007. *Wille's principles of South African law*: Juta and Company Ltd.
- Williams, I. 2014. The Role of Community Based Networks in the Development of Rural Broadband. The case of Djurslandsnet in Denmark and lessons for rural sub-Saharan Africa.
- Zalaghi, H. & Khazaei, M. 2016. The Role of Deductive and Inductive Reasoning in Accounting Research and Standard Setting. *Asian Journal of Finance & Accounting*, 8(1): 23-37.
- Zhang, H., Han, W., Lai, X., Lin, D., Ma, J. & Li, J. 2015. Survey on cyberspace security. *Science China Information Sciences*, 58(11): 1-43.

APPENDICES

APPENDIX A: INTERVIEW GUIDELINE

RESEARCH QUESTION

1. What are the cyber-attacks and incidents that affect organizations?
2. What are the contributing and influencing factors to the non-compliance with cyber-security policies in organizations?
3. How is cyber-security policy compliance enforced in organizations?

SEMI-STRUCTURED INTERVIEW GUIDELINE

Opening questions:

- Would you please tell me about your role in the organization?
- How many years of experience working in the domain of cyber-security do you have?
 - 1.1. Have you ever experienced any cyber-attacks or incidents?
 - 1.2. Does your organization have policies that explain cyber-security requirements?
 - 1.2.1. How have these policies been developed?
 - 1.2.2. How are users made aware of the existence and the importance of these policies?
 - 1.2.3. How easy to follow are these policies for end-users?
 - 1.2.4. How do you monitor end-user compliance?

APPENDIX B: ETHICAL CLEARANCE



P.O. Box 652 • Cape Town 8000 South Africa • Tel: +27 21 469 1012 • Fax +27 21 469 1002
80 Roeland Street, Vredehoek, Cape Town 8001

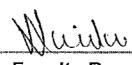
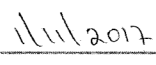
Office of the Research Ethics Committee	Faculty of Informatics and Design
--	-----------------------------------

Ethics approval was granted to MR HUGUES HERMANN KOPA OKIGUI , student number 199111243 on 1 November 2017 for research activities related to the MTech: Information Technology degree at the Faculty of Informatics and Design, Cape Peninsula University of Technology.

Title of dissertation/thesis:	Cyber-security policy compliance model
-------------------------------	--

Comments

Research activities are restricted to those detailed in the research proposal.

 Signed: Faculty Research Ethics Committee	 Date
--	--

APPENDIX C: ANONYMISED EMAIL REQUEST FOR PARTICIPATION

Dear **XYZ**

I trust this email finds you well.

My name is Hugues Hermann Okigui and I am a postgraduate student at the Department of Information and Technology, Faculty of Informatics and Design. I am working on a research study for my Master's degree. The study seeks to understand how cyber-security policy compliance works in organizations.

I am hereby requesting an opportunity to conduct interviews for the purpose of the study. If granted, the interview will be conducted with people having knowledge about Cyber-security and those involved in cyber-security policy compliance.

Kindly note that the data (from the interviews) will not be used for any other purposes other than for this research. The data will be kept confidential to me and my supervisor. The identity of the interviewees will be kept anonymous. the name of the organization will be represented with a pseudonym.

The contribution from your organization is intended to substantiate and is vital to the success of the study. Therefore, your assistance in this regard will be highly appreciated.

I have attached my ethics clearance certificate and a description of my approved research proposal.

Should you need more information, please do not hesitate to contact me or my supervisor copied into this email.

Kind regards

Hugues Okigui

Post Graduate Researcher

APPENDIX D: EMAILED PARTICIPANT CORRESPONDENCE

----- Forwarded message -----
From: [REDACTED] <sue.lose@wits.ac.za>
Date: Wed, Mar 2, 2022 at 4:57 PM
Subject: RE: Assistance with Cyber-security Research
To: [REDACTED] <Hement.Gopal@wits.ac.za> Hugues Okigui
<hugues.okigui@gmail.com>

Dear Hugues

I am happy with being included in the meeting set up with [REDACTED]. My diary is clear for Friday, 10am as well.

Kind regards,

[REDACTED]
Sue Lose

Manager: Risk and Compliance | Office of the CIO, Wits ICT

sue.lose@wits.ac.za | +27 11 717 1616 | +27 84 979 9812 | www.wits.ac.za

[REDACTED]
Solomon Mahlangu House, 1 Jan Smuts Avenue, 2nd Floor, Office 2071,

[REDACTED]
Braamfontein Campus East, Johannesburg, South Africa

From: [REDACTED] <Hement.Gopal@wits.ac.za>
Sent: Wednesday, 02 March 2022 16:23
To: Hugues Okigui <hugues.okigui@gmail.com>
Cc: [REDACTED] <sue.lose@wits.ac.za>
Subject: RE: Assistance with Cyber-security Research

Hi Hugues

It's my pleasure.

I'm happy to meet on Friday as I have a clear diary for now.

If 10 am works for you we can meet then. Please send me a Teams invite.

I'm assuming you will interview **Sue** separately.

Regards,

Hement

Hement Gopal

Senior Systems Engineer: Networks - Information Security | **Office of the CIO, Wits ICT**

E : hement.gopal@wits.ac.za

T : +27 11 717 1658

W : www.wits.ac.za

Solomon Mahlangu House, 1 Jan Smuts Avenue, 2nd Floor

Braamfontein Campus East, Johannesburg, South Africa

From: Hugues Okigui <hugues.okigui@gmail.com>
Sent: Wednesday, 02 March 2022 16:16
To: Hement.Gopal@wits.ac.za
sue.lose@wits.ac.za
Subject: Re: Assistance with Cyber-security Research

Good day [REDACTED],

Thank you so much for this great opportunity.

- If she can offer me the opportunity to interview her, I would be more than happy to do so. Her contribution would be very much appreciated.

Please suggest a day and time that works for you, and I will set the meetings.

Due to the covid-19 situation, I am suggesting that we use Microsoft Teams or Zoom depending on the one you are comfortable with for the interview process.

Thank you very much to both of you.

Regards,

Hugues

On Wed, Mar 2, 2022 at 11:35 AM [REDACTED] <Hement.Gopal@wits.ac.za> wrote:

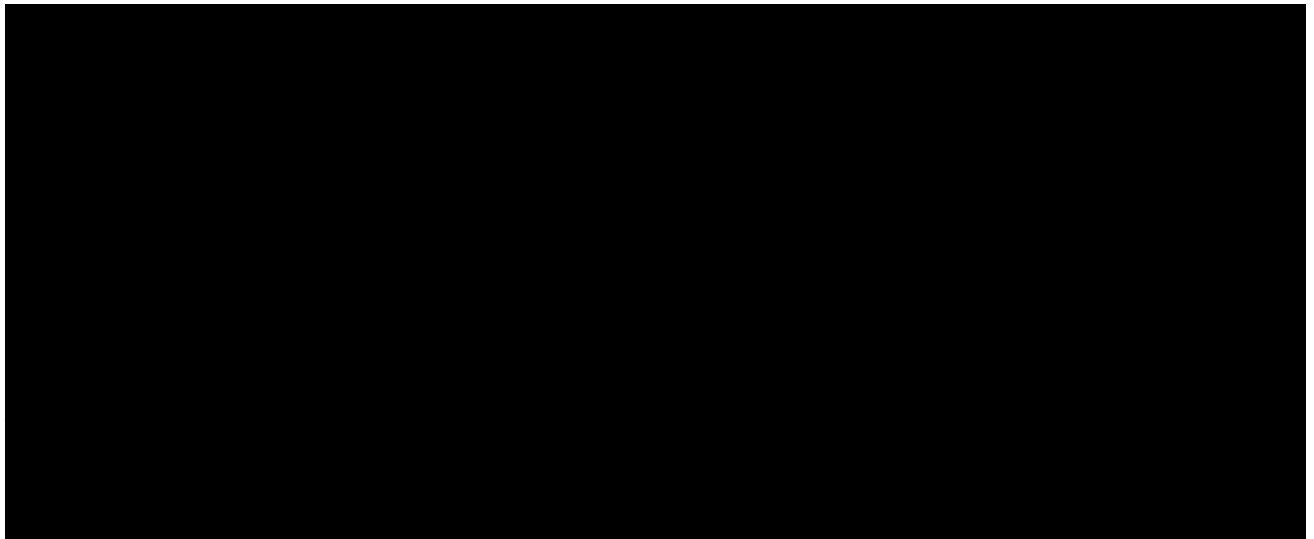
Good day Hugues

Many thanks for this. I am happy to assist.

I am cc'ing Sue as well as she heads our Risk and Compliance division and it would be beneficial to interview her as well as she would be the ideal person to talk around policy and compliance matters.

Regards,

Hement



Solomon Mahlangu House, 1 Jan Smuts Avenue, 2nd Floor,

Braamfontein Campus East, Johannesburg, South Africa

From: Hugues Okigui <hugues.okigui@gmail.com>
Sent: Thursday, 24 February 2022 10:24
To: [REDACTED] <Hement.Gopal@wits.ac.za>
[REDACTED] <CronjeJ@cput.ac.za>
Subject: Assistance with Cyber-security Research

Dear [REDACTED]

I trust this email finds you well.

My name is Hugues Hermann Okigui and I am a postgraduate student at the Department of Information and Technology, Faculty of Informatics and Design. I am working on a research study for my Master Degree. The study seeks to understand how Cyber-security policy compliance works in organizations.

I am hereby requesting an opportunity to conduct interviews for the purpose of the study. If granted, the interview will be conducted with people having knowledge about Cyber-security and those involved in Cyber-security policy compliance.

Kindly note that the data (from the interviews) will not be used for any other purposes other than for this research. The data will be kept confidential to me and my supervisor. The identity of the interviewees will be kept anonymous. The name of the organization will be represented with a pseudonym.

The contribution from your organization is intended to substantiate and is vital to the success of the study. Therefore, your assistance in this regard will be highly appreciated.

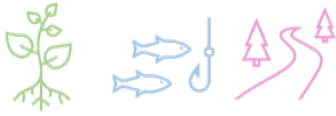
I have attached my ethics clearance certificate and a description of my approved research proposal.

Should you need more information, please do not hesitate to contact me or my supervisor copied into this email.

Kind regards

Hugues Okigui

APPENDIX E: EDITING CERTIFICATE



DR PATRICIA HARPUR

**B.Sc Information Systems Software Engineering, B.Sc Information Systems (Hons)
M.Sc Information Systems, D.Technology Information Technology**

Editing Certificate

**19 Keerweder Street
Vredelust
Bellville
7945**

**083 730 8540
doc@getthatresearchdone.com**

To Whom It May Concern

This document certifies I have copy-edited the following thesis by Hugues Hermann Okigui.:

AN ANALYSIS OF CYBER-SECURITY POLICY COMPLIANCE IN ORGANIZATIONS

Please note this does not cover any content, conceptual organisation, or textual changes made after the editing process.

Best regards

A handwritten signature in black ink, appearing to read 'P. Harpur'.

Dr Patricia Harpur

10 December 2023
