ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

An Analysis of Cybersecurity Policy Compliance in Organisations

Hugues Hermann Okigui | Cape Peninsula University of Technology, South Africa | ORCID: 0009-0004-2221-5106

Johannes Christoffel Cronjé | Cape Peninsula University of Technology, South Africa | ORCID: 0000-0002-9838-4609

Errol Roland Francke | Cape Peninsula University of Technology, South Africa | ORCID 0000-0001-6029-9145

Received: 30.03.2024

Accepted: 02.08.2024

Published: 01.09.2024

Cite this article as:
H.H. Okigui, J.C. Cronjé, E.R. Francke "An analysis of cybersecurity policy compliance in organisations," ACIG, vol. 4, no. 2, 2024, doi: 10.60097/ACIG/191942

Corresponding author:
Johannes Christoffel Cronjé, Cape Peninsula University of Technology, South Africa; E-mail: johannes.cronje@gmail.com
0000-0002-9838-4609

Abstract

In the contemporary digital landscape, cyberattacks and incidents have placed cybersecurity at the forefront of priorities in organisations. As organisations face cyber risks, it becomes imperative to implement and comply with various cybersecurity policies. However, due to factors such as policy complexity and resistance from employees, compliance can be a challenging task. The study, which took a comprehensive approach, investigated the variables that affect an organisation's adherence to cybersecurity policies. The findings of this study provide insights into the challenges and factors influencing compliance with cybersecurity policies in organisations. 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 the existing documents were also considered when available to supplement interviews. The gathered data was meticulously organised, coded, and analysed using the Actor-Network Theory perspective, with a focus on its four moments of translation: problematisation, interessement, enrollment, and mobilisation. The analysis revealed that insider threats and phishing attempts are the two cyber threats

that affect organisations; behavioural challenges and enforcement limitations are the factors that influence and contribute to the non-compliance of cybersecurity policy; phishing exercises and policy development processes are used to enforce cybersecurity policies.

Keywords

cybersecurity policies, compliance challenges, insider threats, phishing attempts, Actor-Network Theory (ANT)

1. Introduction

Cybersecurity is not just a growing concern in specific regions but a global issue that affects countries around the world. This is evident in South Africa, where public and private organisations are constantly under threat from cyberattacks and incidents, leading to significant financial losses. The nation's high Internet access rate and increasing adoption of information and communication technology (ICT) have created a digital paradox situation where technological advances present countless opportunities for a country's development but also lead to a proliferation of cyber incidents and cyberattacks [1].

South Africa continues to be one of the most targeted nations in the world and Africa despite all the efforts [2–4]. 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 cyberattacks and cyber incidents [5, 6].

This study aimed to analyse cybersecurity policy compliance in organisations. The study's results can be applied to direct and enforce agents' (end-users) compliance, through which cyber activities can be monitored and managed so as to minimise cyber incidents and cyberattacks within organisations. This study is underpinned by Actor-Network Theory (ANT), which is recognised as a social-technical theory. ANT is an increasingly used framework in social sciences, such as information systems, to examine the interactions between existing actors and how networks are built.

1.1. Aims, Objectives, and Research Questions

The aim of this study was to analyse the level of compliance with cybersecurity policies in organisations and to understand

the factors influencing this compliance. The objectives were as follows:

- To identify cyberattack and incidents registered by organisations.
- To understand factors that contribute to and influence non-compliance with cybersecurity policies in organisations.
- To examine how cybersecurity policy compliance is enforced in organisations.

The main question driving the study was: What are the factors influencing cybersecurity policy compliance in organisations? The outcome of this question could inform organisations on how to implement and enforce cybersecurity policies effectively, thereby improving their overall cybersecurity posture and reducing the risk of cyberattacks and incidents. The main question was refined with three sub-questions: (1) What are the cyberattacks and incidents that affect organisations? (2) What are the contributing and influencing factors to the non-compliance with cybersecurity policies in organisations? (3) How is cybersecurity policy compliance enforced in organisations?

2. Literature Survey

In keeping with the objectives and research questions, this literature survey covered cyberattacks and incidents, cybersecurity in organisations, and cybersecurity policy before briefly introducing and defending ANT as the lens through which analysis took place.

2.1. Cyberattack and Cyber Incidents

Millions of cyberattacks and incidents occur annually, causing significant financial losses and disruptions across various organisations [7]. As described by Hruza et al. [8], a cyberattack is an act perpetrated within cyberspace aimed at compromising cybersecurity objectives, including confidentiality, integrity, and availability, through activities such as data theft, modification, unauthorised access, destruction, or control of cyberspace infrastructure elements. Additionally, Ferreira [9] defines a cyber incident as a breach or imminent threat of breaching computer security policies, acceptable use policies, or standard security practices.

Organisations encounter diverse cyber threats due to evolving technologies and the constant development of new methods by malicious actors or hackers to compromise organisational assets' confidentiality, integrity, and authentication [10]. These threats

affect organisations, consumers, and stakeholders. Research indicates a shift in concern from traditional physical crimes to cybercrimes among organisations and their consumers [11].

Contemporary cybersecurity literature categorises cyber threats into four main groups: cyber terrorism, hacktivism, cybercrime, and cyber warfare [12]. Cybercrime, in particular, has escalated over the years, emerging as a significant concern for governments, private entities, and individuals [13]. Despite being a prevalent threat, cybercrime often receives less attention [12]. Reports highlight South Africa's vulnerability to cybercrimes, with statistics from Norton's cybercrime report in 2011 indicating high victim rates in South Africa and China [11, 14]. Furthermore, the Global Economic Crime and Fraud Survey for 2018 identified South Africa as the world's second most-targeted nation due to inadequate policing, underdeveloped laws, and inexperienced end-users [15]. Therefore, this study aims to identify the cyberattacks and incidents faced by organisations.

2.2. Cybersecurity in Organisations

The 2007 cyberattack on the Republic of Estonia thrust cybersecurity into prominence, showcasing the potential destabilisation of modern countries and organisations through ICT [16, 17]. Subsequently, cybersecurity has emerged as a significant concern for individuals and organisations globally, driven by the escalating frequency of cyberattacks and incidents, leading to substantial economic and safety repercussions for inadequately protected institutions [18].

Failure in cybersecurity not only results in costly losses for organisations but also poses critical risks to human lives, as hackers possess the capability to manipulate information systems, hindering the dissemination of evacuation alerts during emergencies [19]. The annual cost of cybercrime and economic espionage to the global economy is estimated to range from $375 billion to $575 billion [19], with South African organisations losing approximately 20 billion rand annually to cybercrimes [20].

Despite growing awareness of the importance of cybersecurity, some challenges persist in fostering global cooperation and alignment in combating cyber threats. A divergence in understanding cybersecurity among nations can affect collaborative efforts [21]. Nations, such as South Africa, have developed national cybersecurity strategies (NCSS) to articulate their understanding of

cybersecurity and to establish a harmonised framework of terminology and concepts [21].

Cybersecurity is defined as 'the collection of tools, policies, security concepts, safeguards, risk management approaches, actions, training, best practices, assurance, and technologies to protect the cyber environment, organisation, and user assets' [21]. South Africa's vision regarding cybersecurity is to create a trusted and secure environment where ICT can be confidently utilised by individuals and organisations [22].

The South African perspective supports the importance of safeguarding human as well as non-human actors in cyberspace, thus aligning with Bada and Sasse's [23] view that cybersecurity extends beyond protecting organisational assets to securing human users of ICT systems. Moreover, Mosca [24] asserts that effective cybersecurity measures enhance organisational sustainability and competitiveness by reducing vulnerability to cyber threats.

2.3. Policy and Compliance

Organisations have implemented technical measures to combat cybercrimes, including firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and other technological solutions [25]. However, relying solely on technology is insufficient against hackers' evolving tactics, emphasising the necessity of integrating technical measures with robust security policies for effectiveness [10]. Security policies play a pivotal role in regulating and governing user behaviour within organisations, yet their implementation poses challenges [26].

Bayuk et al. [27] define policy as encompassing all regulations and laws aimed at maintaining organisational cybersecurity. A security policy outlines procedures and processes for employees to uphold the confidentiality, integrity, and availability of organisational resources. While having a cybersecurity policy is essential, experts stress the importance of compliance. Bulgurcu et al. [28] emphasise the need for organisations to understand and enhance employee compliance with existing policies to strengthen security measures.

Cavelty [29] asserts that cybersecurity policy is crucial for addressing global security challenges, focusing on common issues, such as vulnerability and privacy through regulatory frameworks. However, despite the presence of policies, there remains a gap between policy availability and employee practices, with non-compliance posing

significant risks [30, 31]. Consequently, organisations deploy awareness campaigns through various mediums like emails, posters, newsletters, and training modules [32].

Such approaches may only create a semblance of awareness, rather than fostering genuine compliance. Sannicolas-Rocca et al. [26] advocate for methods to improve and enforce employee adherence to security policies. Against this background, we examined the development, communication, and enforcement of cybersecurity policies within organisations.

2.4. Actor-Network Theory

Michael Callon, Bruno Latour, and John Law introduced ANT in the early 1980s where they emphasised the interactions and relationships within heterogeneous networks [33, 34]. ANT focuses on the construction, rather than the purpose of a network, with actors and networks being its core components. Both human and non-human entities are considered actors, and they are treated equally within networks. Actors can include technologies, tools, cultural meanings, and environmental conditions [35, 36].

In ANT, heterogeneity refers to networks comprising diverse elements [37, 38], where interactions among actors, such as people, technologies, texts, and others, form the basis of society [38]. Networks consist of established connections between actors, requiring movement and translation for their formation [39]. They facilitate collaboration among actors to address problems or create new entities [40].

Translation is a four-step process that involves problematisation, interessement, enrollment, and mobilisation. It is integral to network creation [41, 42] and involves persuading actors to accept roles and responsibilities that shape actor-network relationships [43].

Problematisation is the initiation phase of translation. Here, the focal actor identifies and describes the problem, aligns interests, and negotiates common goals [42, 44]. An obligatory passage point (OPP) represents a proposed solution during this phase [43]. Interessement follows problematisation and involves the recruitment of actors based on defined roles and responsibilities, persuading them of the problem's significance and proposed solution [42, 43]. Successful interessement leads to enrollment, where roles and responsibilities are assigned to recruited actors, and alliances and relationships are defined [43]. Enrollment succeeds

when actors accept their assigned roles, fostering a robust network of allies [42]. Upon completion of problematisation, interessement, and enrollment, mobilisation ensues, as designated spokespersons mobilise allies to act in alignment with their roles and responsibilities [42, 43].

3. Methods

This section discussed the case-study research approach and explain how the participating organisations and individual participants were sampled before discussing the collection of data through recorded Zoom interviews and the analysis of data through the lens of ANT. The analysis of the research was guided by ANT's four moments of translation – problematisation, interessement, enrollment, and mobilisation. These moments help in identifying the defined problem, negotiating interests, recruiting actors, assigning roles, and mobilising allies within the context of cybersecurity policy compliance.

3.1. Research Approach and Sampling

This study focused exclusively on exploring organisation employees' attitude towards organisation cybersecurity policy, employing a case study design for its ability to investigate phenomena within their natural settings [23]. The flexibility of case study design allows for the examination of various research questions while considering contextual influences [23]. The qualitative case study methodology is deemed valuable for studying complex phenomena within their contexts [23].

Despite challenges in obtaining sufficient samples due to the topic's sensitivity, three South African-based organisations were included in the study, with one functioning as a cybersecurity service provider [23]. The selection criteria focused on organisations with cybersecurity departments responsible for maintaining the Confidentiality, Integrity, Authenticity (CIA) triad [23]. The use of pseudonyms ensured anonymity for the organisations: HollanRaph for Case 1, NoahGabi for Case 2, and LenJo for Case 3.

HollanRaph, a large higher education institution with over 5000 staff located in Gauteng province, demonstrates a strong commitment to cybersecurity through the establishment of a dedicated cybersecurity department and policy. This organisation functions as a dynamic network involving both human actors and non-human actants. NoahGabi, another large higher education institution in

Western Cape province, boasts over 32,000 students and 5000+ staff, positioning itself as one of the largest institutions in the region. Despite its size, NoahGabi acknowledges the importance of cybersecurity and maintains a dedicated team onsite to address related concerns. Lastly, LenJo, a small IT services and consulting firm based in Gauteng province, plays a significant role in the South African information technology (IT) landscape. Specialising in business-to-business (B2B) ICT solutions, LenJo serves a diverse clientele ranging from small businesses to multinational enterprises. With a focus on business process digitalisation, cybersecurity services, and ICT skills development, LenJo aims to emerge as a leader in its field.

Four participants were purposively selected from these organisations and interviewed via Zoom, with the interviews being recorded. Participant 1 holds the position of manager: IT risk and compliance with over 10 years of experience, contributing to the HollanRaph case. Participant 2, a senior systems engineer specialising in networks and information security with over 10 years of experience, also pertains to the HollanRaph case. Participant 3, the chief executive officer (CEO) and security specialist at LenJo, brings over 9 years of experience to the study. Participant 4, serving as manager of IT strategic services, has over 10 years of experience and is associated with the NoahGabi case.

3.2. Data Analysis

Interview data were transcribed, cleaned, and analysed. The analysis aimed to extract meaningful information from the collected data through transcription, facilitating easier management and analysis [45]. Employing ANT's four moments of translation – problematisation, interessement, enrollment, and mobilisation – guided the analysis from three perspectives: the existence of actors (human and non-human), creation of networks, and interactions and relationships [42, 43]. These moments were utilised to identify the defined problem, negotiate interests, recruit actors, assign roles, and mobilise allies [42, 43]. ANT proved beneficial in identifying actors, including focal actors, and examining network creation and actor relationships, enhancing the understanding of the phenomenon [43]. By considering both human and non-human entities, ANT allowed us to obtain insights into how connections and interactions contributed to network formation, which was particularly relevant in understanding cybersecurity policy involving various entities [39].

4. Results and Discussion

Using ANT as a lens, our analysis focused on actors, networks, and moments of translation. We identified the actors involved in cybersecurity activities, examined their roles, and assessed the implications. Similarly, the study explored the networks existing within cybersecurity activities in South African organisations. The moments of translation, involving negotiation among actors within heterogeneous networks, helped to understand the complex and multidimensional nature of cybersecurity activities, as described by Dlamini and Modise [14].

4.1. Actors

In ANT, actors encompass both human and non-human entities capable of influencing their environment [46]. Both humans and non-humans are integral to cybersecurity activities. Human actors, including technical (IS/IT personnel) and non-technical counterparts, play roles delegated or voluntarily assumed within organisations involved in cybersecurity. Technical personnel have various roles, such as IT risk and compliance managers, IT strategic services managers, security specialists, and systems engineers. At the same time, non-technical actors include business personnel, end-users, managers, clients, and partners. Non-human actors directly or indirectly involved in cybersecurity activities include cybersecurity policies, phishing exercises, computer systems and networks, and security awareness programmes. These components encompass written policies, phishing simulations, computer systems and networks, and security awareness initiatives aimed at informing and educating organisational personnel about potential threats and best practices [46].

4.2. Networks

In cybersecurity policy compliance, actor networks facilitate collaborative problem-solving and entity creation [40]. Networks, heterogeneous in nature, comprise diverse actors, both human and non-human, with an actor potentially belonging to multiple networks. Major actor-networks in this context include the organisation, risk committee, IT managers, business managers, technologists, and end-users. Each network has distinct roles and responsibilities in managing cybersecurity policies [40]. The executive committee, comprising leadership personnel, drafts and enforces cybersecurity policies and standards. Business managers oversee compliance with policies and processes to achieve

organisational objectives. Technologists, including IT engineers and security specialists, develop training and methods for cybersecurity activities. Internal end-users utilise organisational information systems, while external end-users, such as clients and partners, also face cybersecurity risks [40].

4.3. 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. Transformations are observed within organisations based on negotiations and activities. There are four moments in the process of translation: problematisation, interessement, enrollment, and mobilisation [47].

Problematisation: As described by Jessen and Jessen [43], 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 some cases, an improvement [48]. Organisations are challenged with cyberattacks and incidents particularly with insider threats and phishing attempts type. The insider threats and phishing attempts are from different sources. Some of the sources are internal, and others are external. The internal sources are related to the end-users' behaviours and are either conscious or unconscious. Irrespective of the consciousness or the unconsciousness of end-users' behaviours, cyberattacks and incidents such as phishing attacks and insider threats are occasioned.

Insider threats and phishing attempts represent a significant cybersecurity problem for organisations. Thus, effective measures are needed to address the problem. Another existing problem is behavioural challenges. As stated by a participant, despite several awareness materials put in place by organisations, it is still difficult to instigate a change of mind among end-users. According to another participant, the lack of compliance with existing cybersecurity 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 dominates our cybersecurity awareness efficiency because if I look at the incidents we experienced over the past years, 90% of those would be phishing-related cyber incidents. (L49-54_ P1_ NoahGabi)

> The challenges are behavioural challenges. It's just a change in mindset because we share quite a few awareness materials. So, on quite a few platforms, we still have end-users who 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 behaviour. That's one of the challenges. (L220-227_P2_HollanRaph)

Interessement: The 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 [47]. The alignment of actors' interests is done through negotiations. The negotiations are based on each actor's 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 [48], this phase is important because the alignment of different interests can contribute to addressing what was problematised. Additionally, the interests are various and can be expressed in different ways. Some people's interests can be based on their obligations, positions, or/or duties in an organisation. For others, the interests can be based on their business goals, passions, or the implications that cybersecurity policy or cyberattacks and incidents could have on them.

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

> I've worked in many different organisations, and when you take a banking environment where it's very regulated, right? Or a mining, one of the mining organisations, 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 means that we encourage that idea of openness for collaboration, and the difficulty is that it creates complexity and challenges because we are not dealing with one state of staff. We are dealing with many different types of staff, such as academics, students, and many others, and I 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)

Enrollment: It is a critical phase in the process of translation. In this phase, actors are brought together in the same network with the common purpose of finding an effective measure to address the identified problem. It is also about developing alliances and investigating how the actors align in the common objective of developing an effective cybersecurity policy and awareness programmes. To enforce, educate, and inform end-users with the most important aim to enforce. Furthermore, the existence of cybersecurity policy and awareness programmes, such as simulated phishing emails, indicate enrollment and organisation with 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 get involved in politics to stimulate them:

> Well, I'm the risk and compliance manager in ICT. I look after governance, so 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 it changed because it's no longer. I think you're wasting my time, but it's about their money or their well-being. (L410-416_P1_ LenJo)

Mobilisation: It is the last phase, and it takes place when the problematisation, interessement, and enrollment phases are completed [42]. This phase is important because it is where the main actor makes sure that others behave with respect to their assigned roles and responsibilities [43]. The mobilisation phase also aims to mobilise developed networks and maintain proposed solutions to address identified problems effectively. The purpose of mobilisation 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 organisation's cybersecurity 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 they highlighted gaps and pointed out where more attention was needed. Once the gaps are identified, improvements could be made in cybersecurity policies and materials that create awareness:

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

5. Conclusions

This section provides a summary of the key findings, an answer to the research questions, a discussion of this study's limitations, and recommendations for further research.

5.1. Summary of Findings

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

- Behavioural challenges refer to end-users' attitudes and behaviours towards cybersecurity measures initiated by organisations, including resistance to complying with cybersecurity

policies and a tendency to fall for phishing attempts. Enforcement limitations involve a lack of suitable cybersecurity policies and awareness programmes that align with the specific needs of the organisation's end-users. Insider threats encompass both conscious and unconscious cyber risks generated by personnel within the organisation. Phishing attempts are fraudulent efforts to steal sensitive information, such as login credentials, often delivered via email or SMS. Phishing exercises simulate real-world phishing attacks to test the readiness of staff or end-users in identifying cyber threats and to evaluate the effectiveness of existing awareness programmes. The policy development process involves creating a cybersecurity policy that considers all phases—drafting, review, and approval—and requires collaboration with relevant stakeholders to ensure it meets the organisation's unique context.

5.2. Answers to Research Questions

Research sub-question 1: What are the cyberattacks and incidents that affect organisations?

The analysis conducted in Section 4.3 showed that organisations are particularly challenged with the following:

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

Research sub-question 2: What are the factors that influence and contribute to non-compliance with cybersecurity policies in organisations?

The analysis showed that the factors influencing and contributing to non-compliance with the organisation's cybersecurity policies are as follows:

- *Behavioural challenges*: The behavioural challenges concern internal end-user mindsets and attitudes towards proposed cybersecurity policies. Despite awareness initiatives taken by organisations, internal end-users were not adhering to the security measures available to them.

- *Enforcement limitations*: The enforcement of limitations is the fact that some organisations are failing to develop adequate and balanced cybersecurity policies to meet their heterogeneous environment contexts. Proposed policies are sometimes not suitable for the business sector they are in. Consequently, not all internal end-users can be targeted. For example, higher education and banking-type environments cannot consider similar aspects when developing cybersecurity policies and awareness programmes. Some organisations cannot have a one-size-fit cybersecurity policy.

Research sub-question 3: How is cybersecurity policy compliance enforced in organisations?

According to the analysis provided in Section 4.3, organisations enforce their cybersecurity policy compliance using the following:

- *Phishing exercises*: The analysis revealed that periodically, phishing exercises, such as simulated phishing emails, were initiated. The main purpose of this approach is 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 the current proposed solutions.
- *Policy development process*: The analysis showed that the cybersecurity policy development process should follow a collaborative and inclusive approach, with participation of organisation stakeholders. Potential policies should be drafted first, reviewed, and then submitted for approval.

5.3. Contribution of the Research

Theoretical contributions: The study contributes to the academic literature, especially the fact that very little has been done in the area of cybersecurity studies through the ANT concept, especially using the four moments of translation. ANT is employed to explore the actors and networks involved in cybersecurity activities within organisations. It helps in understanding the roles of human and non-human entities in cybersecurity, such as IT personnel, business managers, end-users, clients, partners, cybersecurity policies, phishing exercises, computer systems, networks, and security awareness programmes.

Practical contributions: This study is important, as we hope the result will continuously assist organisations with their cybersecurity policy challenges and the persistently growing number of cyberattacks

and incidents. The findings could help us better understand these challenges and develop more contextualised cybersecurity policies to fit organisational environments.

5.4. Limitations of the Study

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

5.5. Recommendations for Further Research

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

References

[1] S. Mabunda, "Cybersecurity in South Africa: Towards Best Practices," in *CyberBRICS: Cybersecurity Regulations in the BRICS Countries*. Cham: Springer International Publishing, 2021, pp. 227-270, doi: 10.1007/978-3-030-56405-6_6.

[2] N. Kshetri, "Cybercrime and cybersecurity in Africa," *Journal of Global Information Technology Management*, vol. 22, no. 2, pp. 77–81, 2019, doi: 10.1080/1097198X.2019.1603527.

[3] M. Evans, L.A. Maglaras, Y. He, H. Janicke, "Human behaviour as an aspect of cybersecurity assurance," *Security and Communication Networks*, vol. 9, no. 17, pp. 4667–4679, 2016, doi: 10.1002/sec.1657.

[4] N. Kortjan, R. Von Solms, "A conceptual framework for cybersecurity awareness and education in SA," *South African Computer Journal*, vol. 52, no. 1, pp. 29–41, 2014, doi: 10.18489/sacj.v52i0.201.

[5] Gundu, T. (2019). "Acknowledging and Reducing the Knowing and Doing gap in Employee Cybersecurity Compliance," Proceedings of the 14th International Conference on Cyber Warfare and Security, N. van der Waag-Cowling, L. Leenen, Eds. Stellenbosch University, South Africa, February 28–March 1, 2019.

[6] J. Abawajy, "User preference of cybersecurity awareness delivery methods," *Behaviour & Information Technology*, vol. 33, no. 3, pp. 237–248, 2014, doi: 10.1080/0144929X.2012.708787.

[7] J.S. Nye Jr, "Deterrence and dissuasion in cyberspace," *International Security*, vol. 41, no. 3, pp. 44–71, 2017, doi: 10.1162/ISEC_a_00266.

[8] P. Hruza, R. Sousek, S. Szabo. (2014). "Cyberattacks and attack protection," in *World multi-conference on systemics*, vol. 18, pp. 170–174 [Online]. Available: https://www.iiis.org/CDs2014/CD2014SCI/SCI_2014/PapersPdf/SA975KW.pdf [Accessed: Jul. 21, 2018].

[9] F.W. Ferreira. (2012). "*NIST publishes computer security incident handling guide"* [Online]. Available: https://www.hlregulation.com/2012/08/16/nist-publishes-computer-security-incident-handling-guide/ [Accessed: Jun. 22, 2018].

[10] N.S. Safa et al., "Information security conscious care behaviour formation in organisations," *Computers & Security*, vol. 53, pp. 65–78, 2015, doi: 10.1016/j.cose.2015.05.012.

[11] N. Kshetri, *Cybercrime and cybersecurity in the global south*. London: Palgrave Macmillan, 2013, doi: 10.1057/9781137021946.

[12] K. Quigley, C. Burns, K. Stallard, "Cyber Gurus: A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection," *Government Information Quarterly*, vol. 32, no. 2, pp. 108–117, 2015, doi: 10.1016/j.giq.2015.02.001.

[13] D. Marsh. (2017). "*Are ethical hackers the best solution for combating the growing world of cybercrime*?" Unpublished doctoral dissertation, University Honors College, Middle Tennessee State University, TN [Online]. Available: https://jewlscholar.mtsu.edu/bitstreams/2a3a0af1-5bdf-41dc-859a-8c44c92ffcfb/download [Accessed: Jul. 21, 2018].

[14] Dlamini, Z., Modise, M., 2012. Cyber security awareness initiatives in South Africa: a synergy approach. In 7th International Conference on Information Warfare and Security. pp. 1–10. [Online] Available at: http://hdl.handle.net/10204/5941 [Accessed: Jan. 21, 2020].

[15] Citizen. (2018). *Presidency website back up after hack.* [Online]. Available: https://citizen.co.za/news/south-africa/1972813/presidency-website-back-up-after-hack/ [Accessed: Apr. 4, 2019].

[16] N. Gcaza, R. von Solms, J.J. van Vuuren. (2015). "An ontology for a national cybersecurity culture environment," in: *HAISA*, pp. 1–10. [Online]. Available: https://www.researchgate.net/publication/306292545 [Accessed: Apr. 16, 2019].

[17] A. Kozlowski, "Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan," *European Scientific Journal (ESJ)*, vol. 3, pp. 237-245, 2014, https://www.researchgate.net/publication/260107032.

[18] N. Gcaza, R. Von Solms, "A strategy for a cybersecurity culture: A South African perspective," *The Electronic Journal of Information Systems in Developing Countries*, vol. 80, no. 1, pp. 1–17, 2017, doi: 10.1002/j.1681-4835.2017.tb00590.x.

[19] J.P. Kesan, C.M. Hayes, "Creating a 'Circle of Trust' to Further Digital Privacy and Cybersecurity Goals," *Forthcoming, Michigan State Law Review, Illinois Public Law Research Paper* No. 13-03, Illinois Program in Law, Behavior and Social Science Paper No. LBSS13-04, pp 1475-1559, 2014, doi: 10.2139/ssrn.2135618.

[20] N. Kshetri, "Cybercrime and cybersecurity issues in the BRICS economies," *Journal of Global Information Technology Management*, vol. 18, no. 4, pp. 245–249, 2015, doi: 10.1080/1097198X.2015.1108093.

[21] E. Luiijf, K. Besseling, P. De Graaf, "Nineteen national cybersecurity strategies," *International Journal of Critical Infrastructures 6*, vol. 9, no. 1–2, pp. 3–31, 2013, doi: 10.1504/IJCIS.2013.051608.

[22] R. Von Solms, J. Van Niekerk, "From information security to cybersecurity," *Computers & security*, vol. 38, pp. 97–102, 2013, doi: 10.1016/j.cose.2013.04.004.

[23] M. Bada, A. Sasse, "*Cybersecurity awareness campaigns: Why do they fail to change behaviour*?" Oxford: Global Cyber Security Capacity Centre, University of Oxford, 2014, arXiv:1901.02672.

[24] M. Mosca. (2015). "*Cybersecurity in an era with quantum computers: will we be ready*?" IACR Cryptology ePrint Archive, p. 1075, [Online]. Available: https://eprint.iacr.org/2015/1075.pdf [Accessed: Apr 19, 2019].

[25] H.M. Said et al., "An integrated approach towards a penetration testing for cyberspaces," *European Journal of Computer Science and Information Technology*, vol. 3, no. 1, pp. 108–128, 2015, doi: 10.1186/s12913-018-3161-3.

[26] T. Sannicolas-Rocca, B. Schooley, J.L. Spears, "Designing effective knowledge transfer practices to improve IS security awareness and compliance," in Proceedings of the 2014 47th Hawaii International Conference on System Sciences, pp. 3432-3441, IEEE, doi: 10.1109/HICSS.2014.427.

[27] J.L. Bayuk et al., *Cybersecurity policy guidebook*. Hoboken, NJ: John Wiley, 2012, doi: 10.1002/9781118241530.

[28] B. Bulgurcu, H. Cavusoglu, I. Benbasat, "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," *MIS Quarterly*, vol. 34, no. 3, pp. 523–548, 2010, doi: 10.2307/25750690.

[29] M.D. Cavelty, "Breaking the cybersecurity dilemma: Aligning security needs and removing vulnerabilities," *Science and Engineering Ethics*, vol. 20, no. 3, pp. 701–715, 2014, doi: 10.1007/s11948-014-9551-y.

[30] D.C. Streeter, "The effect of human error on modern security breaches," *Strategic Informer: Student Publication of the Strategic Intelligence Society*, vol. 1, no. 3, p. 2, 2013, https://www.researchgate.net/publication/260107032.

[31] J. Blythe. (2013). "Cybersecurity in the workplace: Understanding and promoting behaviour change," in: *Proceedings of CHItaly 2013 doctoral consortium*, pp. 92–101 [Online]. Available: https://nrl.northumbria.ac.uk/id/eprint/14720 [Accessed: Apr. 16, 2019].

[32] E. Albrechtsen, J. Hovden, "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study," *Computers & Security*, vol. 29, no. 4, pp. 432–445, 2010, doi: 10.1016/j.cose.2009.12.005.

[33] B. Czarniawska, "Actor-network theory," in: *The Sage handbook of process organisation studies*, A. Langley, H. Tsoukas, Eds. Los Angeles, CA: Sage, 2016, pp. 160–173, doi: 10.4135/9781473957954.n10.

[34] B.J. Greenhough, "Actor-network theory," in *International encyclopedia of geography: People, the earth, environment and technology*, Wiley Online Library, 2016, pp. 1–7, doi: 10.1002/9781118786352.wbieg0532.

[35] O. Hanseth, M. Aanestad, M. Berg, "Guest editors' introduction: Actor-network theory and information systems. What's so special?," *Information Technology & People*, vol. 17, no. 2, pp. 116–123, 2004, doi: 10.1108/09593840410542466.

[36] J. Scott, *Social network analysis*. London: Sage, 2017, doi: 10.4135/9781529716597.

[37] Y. Shim, D.H. Shin, "Analysing China's fintech industry from the perspective of actor–network theory," *Telecommunications Policy*, vol. 40, no. 2, pp. 168–181, 2016, doi: 10.1016/j.telpol.2015.11.005.

[38] B. Latour, *Reassembling the social: An introduction to actor-network-theory*. Oxford: Oxford University Press, 2007.

[39] R. Dankert. (2010). *Using actor–network theory (ANT) doing research*. [Online]. Available: www.ritskedankert.nl/publications [Accessed: Apr. 14, 2019].

[40] T. Iyamu, T. Sekgweleo, "Information systems and actor-network theory analysis," *International Journal of Actor-Network Theory and Technological Innovation (IJANTTI)*, vol. 5, no. 3, pp. 1–11, 2013, doi: 10.4018/jantti.2013070101.

[41] I. Williams, *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.* Munich: Grin Publishing, 2014.

[42] C. Costa, P. Cunha, "The social dimension of business models: An actor-network theory perspective," in 21st Americas Conference on Information Systems, AMCIS 2015, Puerto Rico, August 13-15, 2015. Association for Information Systems, 2015. [Online]. Available: https://aisel.aisnet.org/amcis2015/e-Biz/GeneralPresentations/25 [Accessed: Nov. 14, 2023].

[43] Jessen, J. D., Jessen, C. "Games as Actors - Interaction, Play, Design, and Actor Network Theory," *International Journal on Advances in Intelligent Systems*, vol. 7, no. 3–4, pp. 412–422, 2014.

[44] R. Heeks, C. Stanforth, "Technological change in developing countries: Opening the black box of process using actor–network theory," *Development Studies Research*, vol. 2, no. 1, pp. 33–50, 2015, doi: 10.1080/21665095.2015.1026610.

[45] S.R. Ponelis, "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*, vol. 10, no. 1, pp. 535–550, 2015, doi: 10.28945/2339.

[46] S. Edwards, *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, Lincoln, UK, 2014. [Online]. Available: https://hdl.handle.net/10182/6744 [Accessed: Apr. 14, 2019].

[47] A. Wæraas, J.A. Nielsen, "Translation theory 'translated': Three perspectives on translation in organisational research," *International Journal of Management Reviews*, vol. 18, no. 3, pp. 236–270, 2016, doi: 10.1111/ijmr.12092.

[48] T. Iyamu, S. Mgudlwa, "Transformation of healthcare big data through the lens of actor network theory," *International Journal of Healthcare Management*, vol. 11, no. 3, pp. 182–192, 2018, doi: 10.1080/20479700.2017.1397340.