UNIVERSITY OF KWAZULU-NATAL

EXPLORING THE ROLE OF ETHEKWINI ELECTRICITY UNIT LEADERSHIP IN ESTABLISHING AN EFFECTIVE ORGANISATIONAL CYBERSECURITY CULTURE

By

Naren Ramchunder

205500531

A dissertation submitted in partial fulfilment of the requirements for the degree of

Master of Business Administration

Graduate School of Business & Leadership
College of Law and Management Studies

Supervisor: Dr Xoliswa Majola

2021

DECLARATION

I, Naren Ramchunder, declare that:

(i) The research reported in this dissertation/thesis, except where otherwise indicated, is my original research.

(ii) This dissertation/thesis has not been submitted for any degree or examination at any other university.

(iii) This dissertation/thesis does not contain other persons' data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.

(iv) This dissertation/thesis does not contain other persons' writing, unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted, then:

a) their words have been re-written but the general information attributed to them has been referenced;

b) where their exact words have been used, their writing has been placed inside quotation marks, and referenced.

(v) Where I have reproduced a publication of which I am author, co-author or editor, I have indicated in detail which part of the publication was actually written by myself alone and have fully referenced such publications.

(vi) This dissertation/thesis does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the source being detailed in the dissertation/thesis and in the References sections.

Signed: ……..

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude and appreciation to all who have assisted me throughout my MBA studies. Your support has provided me with the inspiration to persevere through the challenges of this journey. I would like to thank the following individuals for their support:

- I would like to thank the Almighty God for providing me with the opportunity, strength, and discipline to persevere through the MBA program.

- I would like to thank my wife, Carminee Ramchunder, for her unwavering support throughout my MBA studies. You have provided me with sound advice, encouragement, strength, opportunity, and the time to pursue this degree. I truly appreciate all the sacrifices you have made, and I cannot thank you enough for all that you have done. I love you.

- I would like to thank my son, Bhavay Ramchunder, for always brightening up my day. Even though you are only two and a half, you have provided me with all the support and love I could ever wish for. Thank you so much my boy. I love you.

- I would like to thank my supervisor, Dr Xoliswa Majola, for the assistance and guidance she has provided throughout my dissertation. Thank you for your professionalism and dedication to providing advice and feedback timeously.

- I would like to thank the participants of this study for taking the time out of their busy schedules to share their knowledge with me. Thank you for making the interviews thought-provoking and rewarding. I appreciate your views and insight, without which this study would not be possible.

- I would like to thank my MBA team, Maria Ngcaweni, Salisha Govender, Nomkhosi Dzanibe and Nqobile Ndimande, for all the hard work, dedication, late nights and fantastic experiences we shared along this MBA journey.

- Finally, I would like to thank my family and friends for all the support, encouragement, and advice you have given me throughout this journey.

ABSTRACT

The eThekwini Electricity Unit is an electric utility responsible for distributing electricity throughout the eThekwini municipal region. The organisation is continuously modernising its electrical infrastructure by adding monitoring and control functions to improve operations. To ensure the reliability and availability of the power system, eThekwini Electricity has undertaken various initiatives to address the cybersecurity risks introduced by digitalisation. However, a limited focus has been placed on securing the cybersecurity vulnerabilities posed by employees. This study explored the role of eThekwini Electricity Unit leadership in creating an effective organisational cybersecurity culture to address cybersecurity threats that aim to exploit human vulnerabilities. The research employed an interpretivist philosophy, an inductive research approach and a qualitative design using semi-structured interview techniques. This approach allowed the participants to express their views freely. Ten participants were purposefully sampled based on their cybersecurity knowledge and leadership positions. Thematic analysis of the interview transcripts revealed common themes that connect to the objectives of this study, providing an in-depth understanding of the leadership role and challenges of establishing an organisational cybersecurity culture. Key findings of this research indicate that the immaturity of the organisational cybersecurity culture at the Unit stems from the absence of a holistic cybersecurity strategy and a lack of top management awareness around cybersecurity. Furthermore, it was found that the leadership role in developing the cybersecurity culture at the eThekwini Electricity Unit is limited by the absence of accountability for cybersecurity. Several recommendations, such as establishing leadership accountability for cybersecurity, defining an organisational cybersecurity strategy, and creating an organisational structure to support cybersecurity, were made to improve the cybersecurity culture. Furthermore, appointing cybersecurity champions, enforcing compulsory cybersecurity training, establishing employee accountability, using performance evaluations as a motivator, and building upon the organisational experience in developing a safety culture to drive the formation of an organisational cybersecurity culture, were recommended. Leaders can undertake these recommendations to shape the organisation’s cybersecurity culture such that all employees actively participate in reducing risks from the cyber domain.

Table of Contents

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1: OVERVIEW OF THE STUDY

1.1 Introduction

This chapter provides an overview and background to the study. It describes the purpose and methodology used to explore the role of leadership in creating an organisational cybersecurity culture at eThekwini Electricity. Furthermore, the reasons for why it is necessary to research the development of this culture at eThekwini Electricity is presented. Finally, the research objectives are listed, and research questions are posed, framing the study.

The proliferation of the internet has enabled widespread access to information, offering many societal and business benefits (Spremić and Šimunic, 2018). As a result, digital transformation has become the focus of many industries, and a growing number of leaders see digitalisation as a critical aspect of their strategic direction (Gole Babić, 2020). Furthermore, spurred on by the fourth industrial revolution, the growth of the Industrial Internet of Things (IIoT), which is the integration of Information and Communication Technology (ICT) and the internet with physical Operational Technology (OT) systems, has accelerated over the last decade (Jhanjhi, Humayun and Almuayqil, 2021). IIoT offers businesses increased productivity and efficiencies through ubiquitous visibility and control of cyber-physical systems. There are currently approximately 20 billion devices connected to the internet, supporting countless applications such as smart industries and smart cities. This number is projected to exceed 30 billion by 2024 (Lombardi, Pascale and Santaniello, 2021).

The increased connectedness offered by digital technologies also introduces new complex risks and vulnerabilities to organisations and users of cyberspace, as internet-enabled industries are often lucrative targets for cybercriminals (Jhanjhi et al., 2021). Therefore, organisations have focused on cybersecurity to protect themselves against increasing cyber risks such as cybercrime. Cybersecurity is concerned with the ability to protect, defend and respond to cyberattacks that can cause, amongst other things, reputational damage and financial losses, which can cripple operations (Da Veiga, 2016; NIST, 2017).

Cyber attacks on critical infrastructure have been highlighted by the discovery of malware such as Stuxnet, which malicious actors explicitly designed to target Industrial Control Systems (ICS). For example, in June 2010, Stuxnet was used to attack an Iranian nuclear power plant resulting failure of several nuclear reactors (Chen and Abu-Nimeh, 2011; Farwell and Rohozinski, 2011). Furthermore, in 2015 a cyber attack on Ukrainian electric utilities allowed hackers to remotely open substation circuit breakers, resulting in over two hundred and twenty thousand customers going without electricity for several hours (Liang, Weller, Zhao et al., 2016). Cyber attacks on critical infrastructure are becoming more frequent with implications for electrical utilities such as societal disruption, loss of revenue, reputational damage, and health and safety risks that may

result in loss of life (McLaughlin, Konstantinou, Wang et al., 2016; Miller, Staves, Maesschalck et al., 2021). Therefore, ensuring the reliability and availability of the electricity system is of utmost importance for the electrical utility.

Malatji, Von Solms and Marnewick (2019) argue that when addressing cybersecurity, many organisations focus on the technical aspects of securing systems and place little consideration on the social aspects creating a socio-technical gap. Implementing technical security controls on their own have been ineffective in securing organisations, as many successful cybersecurity attacks have exploited human vulnerabilities (Ani, He and Tiwari, 2019). Research has shown that employee behaviour is what ultimately determines the cybersecurity posture of the organisation because it is the behaviour, actions or inactions, that creates or mitigates cybersecurity vulnerabilities (Da Veiga, 2016; Huang and Pearlson, 2019; Nasir, Arshah, Ab Hamid et al., 2019; Da Veiga, Astakhova, Botha et al., 2020; Uchendu, Nurse, Bada et al., 2021). Therefore, organisations should approach cybersecurity from a human perspective, focusing on employee behaviour by creating a culture of cybersecurity. The organisational cybersecurity culture created aims to reduce cybersecurity risks by limiting undesired employee behaviours and encouraging the right behaviours (Da Veiga, 2016; Huang and Pearlson, 2019; Ertan, Crossland, Heath et al., 2020).

Creating and managing the right culture is one of the leaders most essential tasks (Daft, 2014, p. 451). Therefore, leadership serves a significant role in cultivating an organisational cybersecurity culture through their knowledge, participation, and prioritisation of cybersecurity initiatives (Huang and Pearlson, 2019). The commitment and actions of the leader influences employees to make cybersecurity a priority, creating a culture of securing the organisation against cybersecurity threats that aim to exploit human vulnerabilities (Da Veiga and Eloff, 2010; Huang and Pearlson, 2019).

1.2 Background

The eThekwini Electricity Unit is an electric utility that forms part of the Trading Services cluster of eThekwini Municipality. eThekwini Electricity purchases electricity from Eskom and distributes it to over seven hundred and forty thousand industrial, commercial and residential customers across the eThekwini metropolitan region (Electricity, 2020). Like many electric utilities around the world, eThekwini Electricity is continuously modernising its electrical infrastructure to meet the requirements of the customer of the future (de Azevedo, Pellanda and Campos, 2020; Electricity, 2020). This activity involves adding monitoring and control functions to legacy electrical distribution systems to move towards a Smart Grid (SG) that provides a two-way flow of energy and information. The SG aims to address challenges such as energy wastage, grid reliability, and security (de Azevedo et al., 2020; Electricity, 2020).

Managing a modernised electrical grid that comprises thousands of electrical substations requires sophisticated industrial control systems supported by robust communication networks. Technologies such as IIoT serve as an enabler providing smart electricity meters, sensors and control to the electrical grid (Saleem, Crespi, Rehmani et al., 2019). However, introducing online monitoring and control functions to legacy electrical distribution systems increases the complexity and bounds of the system. The resulting coupling between cyber and physical electrical grid components increases the vulnerability of the electrical grid to cyber-attacks (McLaughlin et al., 2016). Cyber attacks on critical infrastructure are becoming more frequent, and South Africa (SA) is not immune to these incidents. For example, in July 2021, a state-owned enterprise Transnet, which manages the national port infrastructure, experienced a cyber attack that completely disrupted operations at several container terminals for a week (Reva, 2021).

Cyber attacks such as these highlights the need to address cybersecurity challenges facing organisations that manage critical infrastructure. In response, eThekwini Electricity's ICT, Network Control (NC) and Communication Network (CN) branches have each formulated and applied branch level cybersecurity policies, strategies, and projects to secure the assets under their control (Electricity, 2020).

1.3 Rationale for the study

The rationale for undertaking this study at eThekwini Electricity is as follows. Firstly, cyberattacks on critical infrastructure such as electric grids are becoming more frequent (Chen and Abu-Nimeh, 2011; Farwell and Rohozinski, 2011; Liang et al., 2016). South African organisations are not immune to these incidents, and several prominent and recent incidents have disrupted critical infrastructure operators and state-owned enterprises such as City Power and Transnet (BBC, 2019; Reva, 2021). These incidents, particularly that of a comparable organisation such as City Power, highlight the reality of cyber-attacks facing the electric utility industry and further serve as a significant motivator to consider the adequacy of cybersecurity implementations at eThekwini Electricity.

Secondly, eThekwini Electricity has undertaken numerous projects to modernise its electrical infrastructure to meet new operational and customer requirements. However, this activity couples cyber and physical electrical grid components, thereby increasing the vulnerability of the electrical grid to cyber-attacks (McLaughlin et al., 2016; Electricity, 2020).

Thirdly, implementing technical controls such as hardware and software systems to address cybersecurity challenges comes at a high cost. Lee (2021) notes that worldwide annual cybersecurity spending increased by 64% between 2015 and 2020 to $124 billion. However, municipal budget constraints due to the coronavirus (COVID-19) pandemic and declining revenue can potentially impact investments in cybersecurity. Therefore, identifying alternate

mechanisms for securing the organisation needs to be undertaken. Gole Babić (2020) argues that the capital investment in developing human factors for cybersecurity is far less than the investment required for technological solutions.

Fourthly, due to the lethal nature of electricity, eThekwini Electricity has a well-established health and safety culture that starts at top leadership and permeates throughout the organisation. Reegård, Blackett and Katta (2019) argue that the managerial levers used to shape a safety culture are similar to those required to create a cybersecurity culture. Therefore, eThekwini Electricity can build on the success of its safety culture to cultivate a cybersecurity culture.

Lastly, few studies have focused explicitly on the role of leadership in creating a cybersecurity culture (Glaspie and Karwowski, 2017; Nasir et al., 2019; Uchendu et al., 2021). Furthermore, none of the studies reviewed in the last decade has explicitly focused on critical infrastructure organisations such as electric utilities (Nasir et al., 2019; Uchendu et al., 2021). Therefore, this study provides a unique perspective, focusing on the social element to provide practical insight and expand the body of knowledge in developing an organisational cybersecurity culture to secure organisations that manage critical infrastructure.

1.4 Research problem

As evidenced by McLaughlin et al. (2016), cyberattacks on critical infrastructure are becoming more frequent with implications for electrical utilities such as the loss of revenue, reputational damage and health and safety risks that may result in loss of life. In response, eThekwini Electricity's ICT, NC and CN branches have each formulated and applied branch level cybersecurity policies, strategies, and projects to secure the assets under their control. These separate cybersecurity policies and strategies mainly focus on technology and process dimensions (Ramchunder, 2018; EMARAS, 2019). However, the CN branch cybersecurity strategy acknowledges the cybersecurity vulnerabilities posed by people. The strategy notes that "*It is widely accepted that people pose the greatest security risk to any organisations information resources. Creating security awareness and culture within the branch can help to significantly reduce the risk of attacks aimed at exploiting people. Each individual within the branch needs to recognise the importance of cyber security, understand their role in it and must be constantly vigilant."* (Ramchunder, 2018, p. 5). However, this strategy does not mention the role of leadership in creating a cybersecurity culture at the Branch or Unit level. Furthermore, internal audit reports on the OT environment have made several recommendations to increase information security responsibility by assigning accountability at the appropriate level in the organisation (EMARAS, 2019).

eThekwini Electricity does not have a formal holistic cybersecurity program in place at the Unit level. As a result, current cybersecurity project implementations are fragmented within the Unit.

Moreover, each branch has focused primarily on implementing technology solutions, with little attention to securing the human element (Electricity, 2020). Furthermore, leadership is perceived to play a limited role in cybersecurity activities, indicating that there is no holistic top-down approach to securing the organisation against vulnerabilities introduced by the cyber domain.

1.5 Aim of the study

This study explores the role of eThekwini Electricity Unit leadership in creating an effective organisational cybersecurity culture at the eThekwini Electricity Unit.

1.6 Research objectives

1. To explore the current state of organisational cybersecurity culture at the eThekwini Electricity Unit.
2. To determine the extent of the leadership role in developing the current cybersecurity culture at the eThekwini Electricity Unit.
3. To provide recommendations that outline the leadership role in improving the organisational cybersecurity culture at the eThekwini Electricity Unit.

1.7 Research questions

1. What is the current state of the organisational cybersecurity culture at eThekwini Electricity?
2. To what extent does the role of leadership influence the development of an organisational cybersecurity culture at eThekwini Electricity?
3. What recommendations can be made to improve the organisational cybersecurity culture at the eThekwini Electricity Unit?

1.8 Limitations of this study

Due to the sensitive nature of cybersecurity, some participants were cautious in their responses not to reveal sensitive or confidential information that could expose the organisation to cybersecurity risks. The researcher kept this in mind and tried not to ask probing questions that would cause the participants to divulge sensitive information unintentionally.

This study examined the status of organisational cybersecurity culture at eThekwini Electricity at a single point in time. Therefore, further studies are required to assess whether the implementation of the recommendations improves the organisational cybersecurity culture.

1.9 Research methodology

The research philosophy employed in this study is that of interpretivism. Saunders, Lewis and Thornhill (2009, p.140) argue that interpretivist research aims to create new, richer understandings of social constructs and are well suited for complex business environments.

Moreover, interpretivism is well suited to the proposed research as it will enable a deeper insight into the research problem (Saunders et al., 2009, p.140).

An inductive research approach is used to develop a relationship between leadership and the development of an organisational cybersecurity culture at eThekwini Electricity. The research strategy employed a qualitative research design using semi-structured interviews, which allowed participants to speak freely, enabling a deeper understanding of the leadership role and challenges of establishing an organisational cybersecurity culture. Ten participants were purposefully sampled based on their cybersecurity knowledge and leadership positions. The time horizon for this study is cross-sectional, where the interviews were conducted over a short period.

The interviews were recorded and transcribed to enable a thematic analysis of the data to identify themes and subthemes that emerged. The research was undertaken using sound ethical practices. Ethical clearance was obtained from the University of KwaZulu Natal (UKZN) ethics office. The anonymity of participants and confidentiality of data is maintained according to the Protection of Personal Information (POPI) Act (The Presidency, 2013) and UKZN requirements.

1.10 Outline of dissertation

This dissertation is structured into six chapters. A brief discussion on the contents of each chapter is outlined below.

Chapter one: Overview of the study. This chapter introduces the study discussing the background, motivation and focus of the study. Then, the research problem and research questions are posed. Thereafter, the study's significance, justification, contribution, and limitations are discussed before outlining the research methodology utilised.

Chapter two: Literature review. This chapter examines how culture, leadership, and cybersecurity contribute to understanding how leaders can develop an effective organisational cybersecurity culture. The chapter reviews national cultures, organisational cultures and the related information security subculture to determine how they influence organisational cybersecurity culture. Furthermore, literature is reviewed to understand the role of leadership in developing a cybersecurity culture. The theoretical framework that underpins this study together with the organisational cybersecurity culture model is discussed. The chapter also outlines the gaps in literature relating to organisational cybersecurity culture and how this study contributes to addressing them.

Chapter three: Research methodology. This chapter details the design of the study focusing on the research philosophy and approach, study setting, sample strategy, data collection and analysis methods used to achieve the objectives of this study. This chapter also details why this approach was taken.

Chapter four: Results. This chapter presents the results obtained from the semi-structured interviews. Thematic analysis was conducted on the interview transcripts to reveal themes that emerged from the participant's views. The key themes were highlighted using direct quotations from the participants.

Chapter five: Discussion. This chapter undertakes an analysis of the results in relation to the literature, theoretical framework, and objectives of this study. The findings are examined from these perspectives to determine the study recommendations.

Chapter six: Conclusion and recommendations. This chapter concludes the research and makes several recommendations for using leadership to improve the organisational cybersecurity culture at the eThekwini Electricity Unit.

1.11 Chapter summary

This introductory chapter provides an overview and background to the study. It describes how digital technologies and the increased connectedness offered by the internet introduces new complex risks and vulnerabilities to organisations, making cybersecurity a concern. Furthermore, the reason organisations should focus on creating a cybersecurity culture and how leaders can create this desired culture is discussed. A detailed motivation and focus for this study are provided, highlighting why it is necessary to research the development of this culture at eThekwini Electricity. The research problem was detailed, objectives listed, and research questions posed, framing the study. The significance and justification of the study outlined why the study identified the challenges and made recommendations for mechanisms that leaders can use to shape the organisation's cybersecurity culture. Lastly, the contributions, limitations, and research methodology were discussed before providing an outline of the dissertation. The next chapter examines the literature on how culture, leadership, and cybersecurity contribute to understanding how leaders can develop an effective organisational cybersecurity culture. The theoretical framework and organisational cybersecurity culture model are discussed. The chapter also outlines the gaps in literature relating to organisational cybersecurity culture and how this study contributes to addressing them.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

This literature review chapter examines the relevant literature in the fields of culture, leadership, and cybersecurity. The purpose of the review is to examine how these three fields contribute to understanding how leaders can develop an effective organisational cybersecurity culture to secure against cyber attacks aimed at exploiting human vulnerabilities. First, the definition of organisational cybersecurity culture is examined by considering the influence of national cultures, organisational cultures, and the related information security subculture. Thereafter the role of leadership is examined, placing focus on how leaders can cultivate a cybersecurity culture. Several significant theories that underpin the study are discussed before examining a model of an organisational cybersecurity culture. Finally, existing gaps in the literature related to organisational cybersecurity culture are highlighted to support the focus of this study, which is to explore the role of leadership in creating an organisational cybersecurity culture.

2.2 Defining organisational cybersecurity culture

In the field of business management, Johnson, Whittington, Scholes et al. (2017, pp. 168-169) argue that an individual's cultural frame of reference is influenced by national culture, the organisational field (sector, profession) and the organisation's culture and subcultures. Therefore, when examining organisational cybersecurity culture, it is important to contextualise it in terms of the national and organisational cultures and how they influence an individual's perceptions of organisational cybersecurity (Da Veiga, 2016). The following subsections explore the concept of organisational cybersecurity from these perspectives.

2.2.1 National culture

The literature on geographically based cultural differences and their influence on management practices was popularised by Hofstede (1984), who developed a model of national culture comprising four key dimensions. Hofstede's research findings are significant because cultural differences and value systems are complex and vary widely between geographical regions and even amongst countries within the same region (Johnson et al., 2017, pp. 169-170). These differences manifest themselves in how employees, for example, perceive authority and compliance to rules and policies. Therefore to be effective, regional cultural differences need to be considered in applying management practices (Minkov and Hofstede, 2011).

Minkov and Hofstede (2011) describe the four major cultural dimensions: uncertainty avoidance, long-term orientation, individualism vs collectivism, and power distance. Power distance refers to an individual's relationship with institutions and organisations of authority and the acceptance of the distribution of power. Nations with high power distance, such as Asian countries, are more

accepting of hierarchy and authoritarian management styles. Whereas nations that display a low power distance, such as Australia, are more democratic and accept more flatter organisational structures (Johnson et al., 2017, p. 169).

Individualism vs collectivism refers to the degree of independence displayed between the individual and loyalty to social groups such as family, friends and work teams. Countries in North America display high levels of individualism, and countries in South America display high levels of collectivism (Johnson et al., 2017, p. 169). Long term orientation describes the extent to which individuals consider the past, present and future impact of their decisions (Minkov and Hofstede, 2011). Johnson et al. (2017, p. 169) note that Asian cultures display a tendency towards long term orientation while African and American cultures tend to display short term orientations.

Uncertainty avoidance describes the degree to which individuals are tolerant of uncertainty and ambiguity (Minkov and Hofstede, 2011). A culture of high uncertainty avoidance favours behaviours that encourage conformity and certainty. Conversely, low uncertainty avoidance notes that people accept unpredictable situations or unstructured environments (Daft, 2014, p. 340). Johnson et al. (2017, pp. 169-170) note that Hofstede's model of variations in geographical culture has been criticised for generalising whole countries and argues that the dimensions should be viewed as tendencies and not stereotypes because individuals also differ widely within countries.

2.2.2 National cybersecurity culture

National cultural differences and their effect on how individuals perceive authority and compliance to rules and policies influence the security and cybersecurity posture of the nation and the resulting cybersecurity culture that exists (Da Veiga et al., 2020). Onumo, Cullen and Ullah-Awan (2017) show a significant correlation between two of the cultural dimensions in Hofstede's model of national culture and the level of cybersecurity development observed in different nations.

Of the four dimensions, long term orientation and individualism have been shown to have a significant positive correlation with the development of strategic national cybersecurity initiatives as measured by the Global Cybersecurity Index (GCI). Their results for power distance and uncertainty avoidance were inclusive as they did not pass significance in the regression analysis (Onumo et al., 2017).

However, in a study on establishing an information security culture in the Saudi Arabian region, Alfawaz (2011) found that the high power distance due to the authoritarian and bureaucratic culture made it easier to implement information security practices. Their results also revealed that the high prevalence of uncertainty avoidance is consistent with taking a risk-averse approach to

information security. Therefore, managers in the region have adopted proven solutions, formulated contingency plans, and taken all possible measures to secure their organisations (Alfawaz, 2011).

Moreover, Uchendu et al. (2021) reviewed the last decade of literature in the fields of security culture, information security culture and cybersecurity culture and argued that national culture plays a fundamental role in an organisation's security culture. They further define national culture as *"the norms, values, beliefs and customs of the nation or region that an organisation or employee are based in; these can influence an organisation's security culture."* Uchendu et al. (2021, p. 32). Therefore, when cybersecurity is prioritised at a national level, it eventually becomes necessary to organisations and assists in developing an organisational cybersecurity culture (Uchendu et al., 2021).

To assist member countries in cultivating a national cybersecurity culture, the Organisation for Economic Co-operation and Development (OECD) published a guideline for creating a national cybersecurity culture as a priority activity (OECD, 2005; Da Veiga, 2016). As a member country, South Africa (SA) in 2012 approved the National Cybersecurity Policy Framework (NCPF), which was published for public information in 2015 (SA Government Gazette, 2015). The NCPF explicitly declares the intention of SA to foster a national culture of cybersecurity which would be driven primarily by state-led initiatives.

Although the NCPF outlines how a culture of cybersecurity can be developed through awareness programs and encouraging businesses to foster positive cybersecurity cultures, it does not provide a strategy for developing a cybersecurity culture in SA (Sutherland, 2017). Gcaza and Von Solms (2017) identified this shortfall in the NCPF and the subsequent lack of government-led initiatives required to foster a culture of cybersecurity. They argue that there is an absence of government accountability, skilled personnel, cybersecurity regulation, financial resources, and monitoring and evaluation. Furthermore, stakeholders were poorly managed, and no government-led research initiatives were observed (Gcaza and Von Solms, 2017). To address these deficiencies, Gcaza and Von Solms (2017) proposed a strategy for cultivating a national cybersecurity culture that consists of a set of guiding policies and coherent actions for government to achieve its objective of *"Promoting a culture of Cybersecurity"* SA Government Gazette (2015, p. 15).

2.2.3 Organisational culture

Culture is a fundamental aspect of organisations and comprises the basic assumptions, espoused values, and artefacts that influence how individuals think and behave. One of the most influential scholars on organisational culture, Schein (2010), defines organisational culture as *"as a pattern of shared basic assumptions that was learned by a group as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and,*

therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems." Schein (2010, p. 17). He further describes three levels of culture as basic assumptions, espoused values, and artefacts. At the core of organisational culture lies the basic assumptions or belief systems that have shaped a result of repeated action that has a successful outcome. Espoused values develop from leadership influence over the group through the establishment of strategies and goals which explicitly state the espoused values of the organisation. These develop into values that the group deems important. Finally, artefacts represent the external appearance of organisational culture and manifest in the look, feel, style, and behaviours that can be observed (Schein, 2010). Figure 2.1 illustrates the three levels of organisational culture as described by Schein (2010).

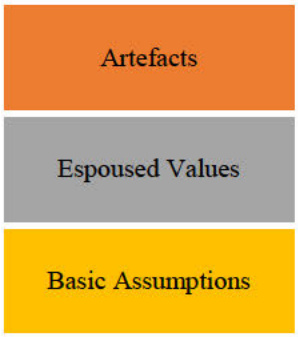


Figure 2.1: Levels of organisational culture. Source: adapted from Schein (2010, p. 26).

The competing values model is another popular model of organisational culture. Quinn, Hildebrandt, Rogers et al. (1991) developed a model that differentiates organisational culture into four types depending on the underlying values and beliefs, which vary along two dimensions, as illustrated in Figure 2.2. The first dimension characterises the organisation's point of view, either externally focused towards the environment or competitors or internally focused towards people or processes. The second dimension represents the degree of flexibility or control. The four types of resulting organisational cultures differentiated by these dimensions are *human commitment culture (support orientation)*, which embodies sharing, corporation, and mutual trust. Secondly, *expansion adaption* (*innovation orientation*) expresses creative problem solving and the willingness to accept change. Thirdly, *maximisation of output* (*rules orientation*) encompasses compliance to written rules and authority and lastly, *consolidation continuity* (*goal orientation*), which emphasises target setting, performance monitoring and reward attainment on the accomplishment of goals (Quinn et al., 1991; van Muijen and al, 1999; Huang and Pearlson, 2019).

Due to the opposing dimensions of internal-external and flexibility-control, rules orientation contrasts with innovation orientation, and goal orientation contrasts with support orientation. Vice versa, there is a correlation between cultures adjoined by a dimension, for instance, support

orientation and innovation orientation, which are adjoined by the dimension of flexibility (Quinn et al., 1991; van Muijen and al, 1999). Gole Babić (2020) argues that leaders and employees often have competing values based on individual and organisational beliefs. Their competing values foster conflict between their values, norms, and practices, and alignment in these values is necessary for the organisation to succeed (Gole Babić, 2020).

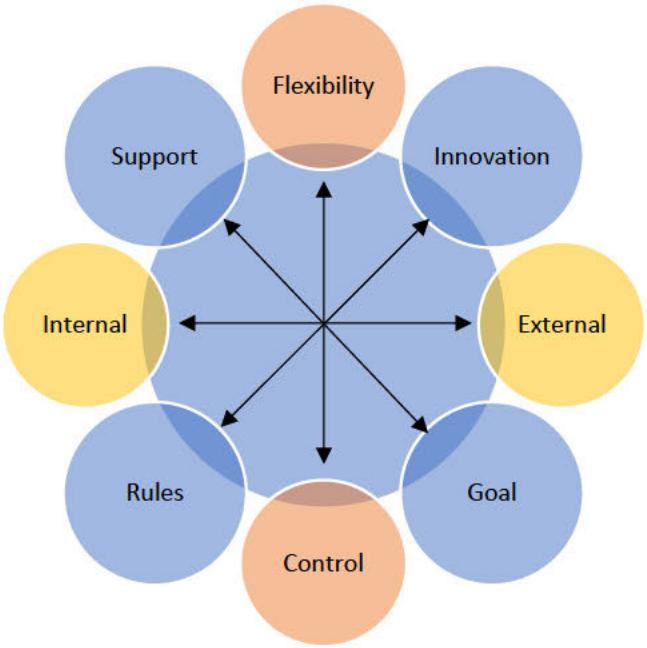


Figure 2.2: The competing values model of orientations of organisational culture. Source: adapted from van Muijen and al (1999, p. 556).

These definitions of organisational culture indicate that culture is determined by the demands of the external environment, the interpretation thereof, and the focus of leaders in setting the organisation's direction in response to those demands. Therefore, adapting the organisational culture to suit the requirements of the external environment is key to achieving organisational goals such as profitability (Daft, 2014). He further notes that organisations with strong cultures need to adapt to the environment; otherwise, they can be more harmful than weak cultures.

In addition, Gcaza, von Solms and van Vuuren (2015) argue that organisational cultures are shaped over time and become evident in the behaviours of employees. Robbins and Judge (2013) argue that employee behaviour ultimately affects the organisation's performance. Da Veiga and Eloff (2010) add that the existing organisational culture must be considered when selecting and implementing information security components. For it to be effective, it is essential to match the controls with the existing organisational culture.

In terms of cybersecurity, employee behaviour is what ultimately determines the organisation's cybersecurity posture because it is the behaviour, actions or inactions, that creates or mitigates cybersecurity vulnerabilities (Huang and Pearlson, 2019). Therefore, focusing on organisational culture and its relationship in developing a cybersecurity culture is key to shaping the desired cybersecurity behaviours (Da Veiga, 2016; Huang and Pearlson, 2019). Schein's model of organisational culture has been used as the foundation of the majority of studies examining information security culture and cybersecurity culture, with many models adding a level to Schein's model, such as knowledge, to form the basis of information security culture understanding (Nasir, Arshah, Ab Hamid et al., 2019; Uchendu et al., 2021; Da Veiga et al., 2020).

Despite the approach taken to develop a cybersecurity culture, the role and importance of leadership in instituting organisational culture change in terms of communication, involvement and training, is vital to shaping employees beliefs (Uchendu et al., 2021). The following subsections provide definitions of information security culture and organisational cybersecurity culture and survey the literature on the development of these perspectives of subcultures.

2.2.4 Information security culture

Ensuring the security of information and information systems is a vital aspect of modern organisations because of the dependence on information systems to provide critical business functions for the organisation to carry out its mission and be competitive. Furthermore, the financial losses and reputational damage resulting from a data breach can result in severe consequences such as liquidation. Therefore, organisations have made information security a priority (Diesch, Pfaff and Krcmar, 2020).

Information security is defined as *"the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability"* NIST (2006). Da Veiga and Eloff (2010) argue that organisations should address information security from a human perspective, focusing on employee behaviour and developing a culture of information security. The information security culture created aims to reduce the risks to information assets by limiting the risk of incorrect employee behaviours and encouraging the right behaviours.

Schein's organisational culture model has influenced much of the foundational research towards developing frameworks and models of information security culture (Uchendu et al., 2021). As illustrated in Figure 2.3, the three levels of culture in Schein's model, the basic assumptions, espoused values, and artefacts, form the upper layers over a foundation of information security knowledge (Da Veiga and Eloff, 2010; Van Niekerk and Von Solms, 2010; Da Veiga et al., 2020).

Figure 2.3: Information security culture layers. Source: adapted from Van Niekerk and Von Solms (2010, p. 479).

Da Veiga and Eloff (2010) state that employee behaviour and their interaction with the organisation's information systems ultimately determines the protection of those assets. They define information security culture "*as the attitudes, assumptions, beliefs, values and knowledge that employees/stakeholders use to interact with the organisation's systems and procedures at any point in time. The interaction results in acceptable or unacceptable behaviour (i.e. incidents) evident in artifacts and creations that become part of the way things are done in the organisation to protect its information assets. This information security culture changes over time."* Da Veiga and Eloff (2010, p. 198).

Information security culture is well researched in academia from the perspective of frameworks and assessment methods that can assist managers and leaders in assessing the current state of information security culture as well as providing mechanisms for its improvement (Da Veiga and Eloff, 2010; Okere, Van Niekerk and Carroll, 2012; Al Hogail, 2015; Nel and Drevin, 2019). The concept of an ideal information security culture and the factors that influence its development was investigated by Da Veiga et al. (2020). They noted that employee awareness, knowledge, compliance to policy and top management support are essential components of an information security culture. In addition, the ideal information security culture is influenced by internal organisational factors such as its structure, business activity, and technology and external environmental factors such as the political environment and state of the economy. The internal factors are categorised into management, human (employees), and mutual trust (relationships) (Da Veiga et al., 2020). Table 2.1 contains a list of factors that influence information security culture (Da Veiga et al., 2020).

Table 2.1: Factors influencing information security culture.

Focus	Scope	Factor
External	**Environment**	National culture
		Political and legal
		Economic
		Socio-cultural
		Technological advancement
Internal	**Organisational Factors**	The internal state of the organisation
		Stage of the life cycle of the organisation
		The level of the overall organisational culture
		Availability of a system for information security
		Resources
	Management Factors	Management and governance
		Information security policies and procedures
		Information security risk management
		Operational management
		Change management
		Personnel information security management
		Information security education, training awareness and communication
		Information security behaviour management
	Human	Personality and values
		Needs
		Emotional condition
		Knowledge of information security
	Factors of mutual trust	Mutual trust between employer and employees, as well as between employees of the organisation
		Customer trust in the organisation

Source: adapted from Da Veiga et al. (2020, p. 14).

Nasir et al. (2019) argue that although the development of an information security culture is well researched from the perspective of frameworks and assessment methods, there is no agreement on the factors that influence information security culture. They note that this is due to the influence of adopted theories, information security maturity level and types of organisations affecting the formulation of the models. Through their systematic review of the literature of information security culture, Nasir et al. (2019) note that the most frequently used dimensions, in order of priority, are Security Policies, Change Management, Leadership and Governance, User Security Management, Information Asset Management and Trust (Nasir et al., 2019).

Developing an information security culture is seen as an essential component in establishing employee behaviours towards minimising risks to an organisation's information assets. However, several limitations of information security culture should be noted. Gole Babić (2020) argues that information security concerns the protection of information and information systems in both the physical and cyber domains. However, information security is reactive to challenges and focuses on mitigating existing issues.

In addition, Von Solms and Van Niekerk (2013) argue that the human factor in information security culture is limited to the role of employees in information security processes and does not consider the implications of cyber attacks aimed at exploiting human vulnerabilities. Reid and Van Niekerk (2014) further argues that information security culture is confined to the bounds of the organisation, however rapid technological advancement and the adoption of cyberspace, which extends the bounds of the organisation into cyberspace, requires the development of a cybersecurity culture to mitigate against cyber threats.

2.2.5 Organisational cybersecurity culture

The proliferation of the internet, which comprises a global interconnection of independent information and communication systems, has enabled widespread access to information, offering many societal and business benefits (Spremić and Šimunic, 2018). Furthermore, the adoption of digital technologies and digital transformation, which integrates information and communication technology with physical and digital systems, has been accelerating over the last decade (Spremić and Šimunic, 2018).

The coronavirus (COVID-19) pandemic has arguably caused unprecedented digital disruption and forced the digital transformation of many industries over a short space of time for them to remain operational (Almeida, Santos and Monteiro, 2020). However, the increased connectedness offered by digital technologies also introduces new complex risks and vulnerabilities to organisations and users of cyberspace. As a result, organisations have focused on cybersecurity to protect against the increasing level of cyber risks such as cybercrime and cyber attacks that can cause, amongst other things, reputational damage and financial losses, which can cripple operations (Da Veiga, 2016). However, Malatji et al. (2019) argue that when addressing cybersecurity, many organisations focus on the technical aspects of securing systems and place little consideration on the social aspects creating a socio-technical gap. Implementing technical security controls on their own have shown to be ineffective in securing the organisation, as many successful cybersecurity attacks have exploited human vulnerabilities (Ani, He and Tiwari, 2019).

Succinctly, cybersecurity is concerned with the ability to protect, defend and respond to cyber attacks (NIST, 2017). A comprehensive definition is specified by the International Telecommunications Union (ITU) as: "*Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets. Organisation and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organisation and user's assets against relevant security risks in the cyber environment.*" ITU (2021).

It becomes apparent from this definition that there are similarities between information security and cybersecurity. However, most critically, cybersecurity extends beyond the organisation's boundaries and includes the protection of assets and individuals in cyberspace (Von Solms and Van Niekerk, 2013; Reegård et al., 2019). Nevertheless, Gcaza et al. (2015) argue that information security and cybersecurity are so closely intertwined that it is reasonable to argue that the formulation of a cybersecurity culture can be formed based on information security culture. Moreover, Da Veiga et al. (2020) argue that organisational cybersecurity culture is a subculture of information security culture.

As defined by Da Veiga (2016), the concept of cybersecurity culture is the interaction of individuals in cyberspace that either help or hinder the privacy, security, and safety of individuals, organisations, or governments. Organisational cybersecurity culture encompasses aspects of information security culture such as securing the organisation's systems, data and compliance to policy. However, Huang and Pearlson (2019) argue that organisational cybersecurity culture is distinctly different as it emphasises personal involvement in cybersecurity. They define organisational cybersecurity culture as *"the beliefs, values, and attitudes that drive employee behaviours to protect and defend the organisation from cyber attacks"* Huang and Pearlson (2019, p. 6399).

Placing a focus on personal involvement and the role of humans as both the victims as well as the potential participants (unintentional) or perpetrators (intentional) in cyber attacks makes cybersecurity culture distinctly different from information security culture (Da Veiga, 2016; Huang and Pearlson, 2019; Reegård et al., 2019). Furthermore, by extending its range from individuals, organisations to governments in cyberspace, cybersecurity culture covers a broader scope than information security culture (Uchendu et al., 2021). Moreover, cybersecurity culture drives human behaviours to be proactive, placing focus on anticipating issues and protecting against them (Huang and Pearlson, 2019; Gole Babić, 2020).

Through their systematic review of the literature on cybersecurity culture, Uchendu et al. (2021) note that both information security culture and cybersecurity culture models have been formed based on Edgar Schein's organisational culture model. However, research on organisational cybersecurity culture is still in its infancy, with only seven papers reviewed within the last decade explicitly focusing on the definition and characteristics of cybersecurity culture (Uchendu et al., 2021).

Fostering a robust cybersecurity culture requires focusing on a set of factors that are crucial for its development and maintenance. Table 2.2 lists the factors identified from the literature on building and maintaining a cybersecurity culture (Uchendu et al., 2021).

Table 2.2: Top factors for the development of cybersecurity culture.

Number	**Factors**	**Number of references out of 58 studies**
1	Top management support, leadership or involvement	34
2	Security policy	27
3	Security awareness	24
4	Security training	21
5	Change management	12
6	Compliance	12
7	Knowledge	11
8	Accountability and responsibility	9
9	Security risk	8
10	Commitment	8
11	Communication	8
12	User management	7
13	Motivation	7
14	Trust	6
15	National culture	5
16	Ethical conduct	4
17	Regulations	4
18	Establishing a network of champions	1
19	Rewards and sanctions	1

Source: adapted from Uchendu et al. (2021, p. 13).

Notably, the most cited, thirty-four out of fifty-eight studies, identified top management support, leadership or involvement as the most important factor in developing a cybersecurity culture.

This finding is consistent with the systematic literature review undertaken by Nasir et al. (2019), who found top management commitment to be a consistent dimension across articles reviewed in their study. Therefore, it is vital to focus on the role of leaders in cultivating an effective cybersecurity culture.

2.3 Organisational leadership and cybersecurity culture

2.3.1 Leadership and culture

Organisational culture and leadership are closely related. Daft (2014, p. 451) argues that leaders create the organisational culture and that creating and managing the right culture is one of the leader's most important tasks. Furthermore, leadership plays a vital role in safeguarding the organisation from external threats, allocating scarce resources and setting an example for employees, positively shaping the culture of the organisation (Huang and Pearlson, 2019).

Leaders influence the organisational culture by firstly defining and communicating values that employees can believe. Secondly, the vision for the desired culture and the values needs to be linked to the organisation's mission. Moreover, leaders need to establish daily practices that reinforce the cultural vision through establishing operating procedures and performance management systems that reinforce the values. Most importantly, leaders need to lead by example, constantly and consistently influencing employees through their actions (Daft, 2014, p. 438). Constant reinforcement and actions taken by the leader that is aligned to the vision are vital to ensuring that the espoused values of the organisation become the basic assumptions of the employees (Schein, 2010, p. 246).

2.3.2 Leadership role in cultivating cybersecurity culture

Leadership plays a vital role in cultivating cybersecurity culture through their knowledge, participation and prioritisation of cybersecurity initiatives (Huang and Pearlson, 2019). Through their systematic review of the last decade of literature related to cybersecurity culture, Uchendu et al. (2021) identified top management support and leadership as the most significant factor in developing a cybersecurity culture.

Gcaza and Von Solms (2017) further argue the importance of leadership in cultivating a cybersecurity culture at a national level. They recommend that the SA government lead the cybersecurity initiatives via establishing a dedicated body for cybersecurity culture, undertaking government-led initiatives, creating national awareness campaigns, and making cybersecurity part of the education curriculum (Gcaza and Von Solms, 2017).

Cybersecurity culture research at an organisational level has primarily focused on the dimensions, assessment instruments, and methods for developing a cybersecurity culture. Several studies have identified the importance of top management/leadership support in developing cybersecurity

culture, but few have explicitly focused on the role of leadership in creating a cybersecurity culture (Glaspie and Karwowski, 2017; Nasir et al., 2019; Uchendu et al., 2021). Da Veiga and Eloff (2010) state that strong leadership is required to influence employees to comply with organisational policies. These drive consistent behaviours that, over time, develop into the cybersecurity culture. Da Veiga and Eloff (2010) argue that, in autocratic organisations, the leadership role is vital to setting the culture. They recommend the appointment of an executive-level sponsor for cybersecurity culture. They further argue that the commitment and actions of this leader will influence employees to commit to making cybersecurity a priority (Da Veiga and Eloff, 2010).

2.3.2.1 Leadership priorities

Leaders will only make cybersecurity a priority if they believe that cybersecurity is important for the organisation. The importance will be reflected in the strategic direction leaders set as well as the allocation of resources, both human and financial, with regards to cybersecurity (Huang and Pearlson, 2019). Uchendu et al. (2021) add that without the support and attention from leadership, cybersecurity initiatives can be seen as insignificant to employees, especially compared to their daily activities. Reegård et al. (2019) further argue the importance of top management support through championing and active participation in cybersecurity as well as allocating resources to cybersecurity activities, which are essential to creating a supportive and enabling environment.

Uchendu et al. (2021) note that the commitment of resources to cybersecurity, especially in organisations with low budgets and resources, signals leaderships priority to cybersecurity and can significantly shape the cybersecurity culture of employees. Furthermore, Glaspie and Karwowski (2017) argue that leadership is seen to be prioritising cybersecurity when they establish organisational structures to support the desired cybersecurity culture, therefore aligning the organisational business strategy with the cybersecurity strategy.

2.3.2.2 Leadership knowledge

Literature on cybersecurity culture and information security culture has emphasised the importance of employee cybersecurity knowledge in shaping the cybersecurity culture of the organisation (Da Veiga and Eloff, 2010; Van Niekerk and Von Solms, 2010; Da Veiga, 2016; Nasir et al., 2019; Uchendu et al., 2021). The emphasis on employee cybersecurity knowledge is necessary to create awareness around the importance of cybersecurity and the protection of assets. Moreover, as observed in cybersecurity models, knowledge is a fundamental component of fostering information security or cybersecurity culture (Nasir et al., 2019; Da Veiga et al., 2020; Uchendu et al., 2021).

However, there has been little emphasis on the importance of leadership's cybersecurity knowledge and its impact on fostering a cybersecurity culture. Huang and Pearlson (2019) argue

that leaders who have skills and competencies relating to cybersecurity will be more knowledgeable about the organisation's cybersecurity vulnerabilities. Therefore, knowledgeable leaders are more likely to value shaping a culture of cybersecurity for the organisation through participation, prioritisation of initiatives, and allocation of resources towards cybersecurity.

In addition, Glaspie and Karwowski (2017) argue that leadership faces many challenges in cultivating a cybersecurity culture. For example, having a documented cybersecurity policy on its own has been shown to provide a minor contribution to a cybersecurity culture. They further argue that leadership must ensure that employees fully understand and appreciate cybersecurity policies. Therefore, leaders themselves need to have the requisite cybersecurity knowledge to convey effectively to employees.

Van‘t Wout (2019) highlights that the cybersecurity strategy is often disconnected from the core business in many organisations and is further relegated to the technology departments. This disconnection results in a bottom-up approach to cybersecurity, concentrating at a middle management level or lower in the organisation. They further argue that a lack of leadership awareness and knowledge about the organisation's specific cybersecurity risks and vulnerabilities is a possible cause for this disconnect. Reegård et al. (2019) further support top management knowledge about cybersecurity and their resulting beliefs. They argue that top management’s observations, perceptions, and knowledge influence their beliefs on cybersecurity and are therefore key to influencing the organisation's cybersecurity culture.

2.3.2.3 Leadership participation

Leaders reinforce the importance of cybersecurity for the organisation when they become personally involved in cybersecurity initiatives by developing and communicating policies, speaking about cybersecurity, attending training, and making cybersecurity a focus for the organisation. Employees are influenced by the participation of leadership and are more likely to become involved and participate as well (Huang and Pearlson, 2019). Glaspie and Karwowski (2017) argue that employees are positively influenced towards cybersecurity policy compliance when management is seen to be engaged in establishing and participating in cybersecurity initiatives themselves.

Reegård et al. (2019) argue that the active participation of top management is just as vital for creating observable behaviours that influence employees as it is for aspects such as allocation of resources for cybersecurity activities. They further argue that to be effective, leaders at an executive level, such as Chief Information Security Officers (CISOs), need to be more participative in their approach to cybersecurity. A more cohesive relationship between the executive and employees is created when leaders are aware of how their participation fosters a culture of organisational cybersecurity (Reegård et al., 2019).

2.4 Theoretical framework

The following subsections review the relevant theories that underpin the literature related to developing an organisational cybersecurity culture.

2.4.1 Social control theory

As part of the greater field of sociology, social control theory describes the ability of a social group to self regulate both individual and group behaviours such that they conform to the rules and expectations of that society or particular social group (Janowitz, 1975). Social control can be achieved in many ways. For organisations, two primary mechanisms denoted as formal and informal social control are commonplace. Formal social control mechanisms comprise regulations, rules and policies that describe the correct and incorrect behaviours required to shape employee values and conduct towards an ideal. Informal social control is achieved through social values, traditions, and norms that are applied by dominant groups or individuals, these influence employee behaviours through social pressure to comply with the norm (Cheng, Li, Li et al., 2013).

Cybersecurity research has primarily focused on formal social controls such as compliance to cybersecurity policies, procedures, standards and regulations, implementing operations management principles, and cybersecurity training (Da Veiga et al., 2020; Uchendu et al., 2021). However, Huang and Pearlson (2019) argue that the influence of an individual's social environment on their beliefs and attitudes can play a significant role in developing a cybersecurity culture.

Cheng et al. (2013) demonstrate that the informal social control exhibited by colleagues and workgroups contributed a significant influence towards an individual's security policy compliance. Ertan et al. (2020) recommend using informal social control such as establishing security champions throughout the organisation to promote cybersecurity at an employee level. Furthermore, Glaspie and Karwowski (2017) note that employees committed to the organisational cybersecurity goals undertake tasks with like-minded individuals, improving cybersecurity compliance. Hsu, Shih, Hung et al. (2015) argue that informal and formal social control mechanisms are crucial to improving extra-role and in-role cybersecurity behaviours, which is an essential component of developing a cybersecurity culture.

2.4.2 Technology acceptance model

Davis (1985) developed the technology acceptance model that describes how individuals perceive technology based on their beliefs. Davis (1985) argues that a user's attitude towards technology, and hence their acceptance which determines their level of use of the technology, is influenced by users perception of the benefits (Chuttur, 2009). Thus, the technology acceptance model offers a model of user intentions and behaviours based on the effect of external influences on their beliefs.

Addae, Radenkovic, Sun et al. (2016) extend the technology acceptance model to describe user acceptance of cybersecurity countermeasures which becomes evident in actual cybersecurity behaviours. Their analysis revealed that external variables such as domain knowledge, experience, environment and demographics determine a user's attitude towards personal data protection, which was found to be a significant predictor of behaviours such as the adoption of cybersecurity countermeasures. Huang and Pearlson (2019) add that the technology acceptance model highlights how one's social environment can influence an individual's beliefs and attitudes, which result in observable behaviours.

2.4.3 Shared team cognition theory

Team cognition refers to shared knowledge and understanding amongst team members through shared mental models (Rajivan and Cooke, 2017). The shared team cognition theory aims to explain the differences between effective and ineffective teams. For example, Cannon-Bowers and Salas (2001) note that team members in effective teams have similar or compatible knowledge that directs their coordinated team behaviour. They further highlight several shared cognition outcomes on organisational performance: better task performance, better team performance, and improved motivational outcomes such as trust and satisfaction.

Rajivan and Cooke (2017) argue that the complexity of the cybersecurity domain does not allow for team members to have the same level of awareness and knowledge. However, creating overlapping knowledge through cross-training of individuals can be used to create shared team cognition. Reegård et al. (2019) further argue that establishing formal cybersecurity teams and steering committees increased knowledge sharing, contributing to mitigating cybersecurity risks.

2.4.4 Interactive team cognition theory

In contrast to shared team cognition theory which emphasises team knowledge over personal knowledge, this theory states that team cognition is observed and measured at a team level through team interactions (Rajivan and Cooke, 2017). They further argue that team cognition is assessed through the observation of communications between team members. Moreover, interactive team cognition is context-based and needs to be studied in the context. Rajivan and Cooke (2017) argue that this perspective suits the ever-changing threat landscape of cybersecurity defence. Moreover, Huang and Pearlson (2019) note that interactive team cognition theory highlights how team perceptions form to increase the cybersecurity situational awareness of the organisation, as the team level outweighs the sum of individual situational awareness.

2.4.5 Social cognitive theory

This theory describes social behaviour with regard to change, adaption and self-development, by examining personal and social factors together through an agentic perspective (Bandura, 2001). Taking an agentic perspective, that is, intentionally influencing one's circumstances based on the

environment, results in behaviours such as self-reflection, self-organisation, self-regulation and being proactive (Bandura, 2001). Furthermore, intentions develop into strategies for achievement. The element of foresight brings anticipation about future events, which guide agents' motivations and current behaviours. Agents self-regulate by adopting personal standards and reflecting on their functioning and efficacy. The social system in which the agent operates influences actions through agentic transactions which aim to increase personal development (Bandura, 2005).

Lu (2018) notes that cybersecurity research utilises social cognitive theory to explain employee behaviour, arguing that if employees are able to control their actions, they will actively engage with the environment of cybersecurity expectations as outlined in the cybersecurity policy. He further argues that this theory explains how employees balance cybersecurity compliance and their self-interests through the concept of self-regulation.

Ogden (2021) notes that the prevailing organisational culture influences individual employee behaviours. He utilised social cognitive theory to show how environmental factors (subjective norms, descriptive norms, and social proximity) and cognitive factors (knowledge, attitude, and self-efficacy) positively impact employee cybersecurity behaviour towards the development of a cybersecurity culture (Ogden, 2021).

2.4.6 Expectancy theory

This theory examines employee attitudes and behaviours in an organisational setting. Expectancy theory describes the relationship between attitudes, motivation, and expectancy, which are influenced by intrinsic and extrinsic rewards. Rewards influence the motivation of employees, which is observed in increased job performance (Lawler III and Suttle, 1973).

In its application to cybersecurity culture, Huang and Pearlson (2019) argue that leaders can use expectancy theory to shape employee behaviours through performance evaluations. By observing employee behaviours and using performance reviews as motivation, leaders can highlight the importance of the desired cybersecurity behaviours in the organisation, influencing and reinforcing the cybersecurity culture (Gole Babić, 2020).

2.4.7 Rational choice theory

The rational choice theory describes how individuals make decisions balancing the perceived benefits against the cost implications. This theory assumes rationality in that a rational individual will weigh the perceived benefits and costs of their actions prior to determining how to proceed. Moreover, individuals are motivated by desires or goals that drive their actions. Therefore, decisions are taken based on the assumptions made, founded on the information at hand (Scott, 2000). Furthermore, rational choice requires individuals to anticipate alternative outcomes and choose the most appropriate outcome that gives them the most utility (Scott, 2000).

Applied to cybersecurity, Glaspie and Karwowski (2017) argue that employees weigh the benefit of compliance against the cost of non-compliance when considering cybersecurity aspects such as policy compliance. They further note that the size of the reward has a significant effect on compliance. Huang and Pearlson (2019) add that the magnitude of rewards and punishments need to match the desired or undesired behaviours for them to be effective.

2.4.8 Deterrence theory

This theory describes the psychological process that deters individuals from contravening laws based on the perceived severity of the penalty, the certainty of application, and the speed of enforcement (Williams and Hawkins, 1986). Lu (2018) argue that by applying this theory to a cybersecurity context, organisations can control employee behaviours by introducing sanctions and punishments that outline the high risk of being caught and punished for undertaking undesired cybersecurity behaviours.

Glaspie and Karwowski (2017) argue that organisations with strong consequences such as dismissal for non-compliance have been shown to achieve better compliance with cybersecurity policies and, consequently, have a stronger organisational cybersecurity culture. Therefore, having clear and consistent consequences for non-compliance is vital to fostering a positive organisational cybersecurity culture (Glaspie and Karwowski, 2017). Conversely, Thomson and Van Niekerk (2012) argue that organisations who develop a prosocial environment, where employees accept policy compliance without thinking of the consequences of non-compliance, naturally eliminate the need for punishments as a deterrent.

2.4.9 Protection motivation theory

The protection motivation theory describes the factors that influence an individual's responses when faced with a threat (Rogers, 1975). This theory builds on an individual's fear responses to threats and notes that the response is based on factors such as the perceived severity of the threat, perceived likelihood and vulnerability, and perceived efficacy of response (Lu, 2018).

Addae et al. (2016) argue that when individuals become aware of cybersecurity risk, they form beliefs about the perceived risk based on the effectiveness of the available coping mechanisms. They further argue that an individual's perceptions of cybersecurity risk significantly influence the decisions made towards cybersecurity.

Van't Wout (2019) highlights the importance of motivation in achieving cybersecurity goals which are driven by various organisational needs. They argue that the current needs, mindsets, frames of reference, perceptions, attitudes, and factors for motivation of employees need to be understood to shape an individual's cybersecurity behaviours.

2.4.10 Institutional mimicry theory

The institutional mimicry theory aims to describe why organisations in a particular organisational field are similar. Through the process of effecting organisational change, rational actors make organisations similar through coercive, mimetic, and standardising processes (DiMaggio and Powell, 1983). Jeyaraj and Zadeh (2020) note that organisational fields comprise peer institutions, regulatory agencies, standards bodies, suppliers, consumers, and competitors, who exert pressure on organisations. By complying with dominant practices and social expectations within the organisational field, organisations gain acceptance from their peers. This form of institutionalisation converges organisational practices and responses to the environment (Jeyaraj and Zadeh, 2020).

In a cybersecurity-related study, Barton, Tejay, Lane et al. (2016) argue that institutional pressures influence senior managers beliefs and participation in cybersecurity initiatives. Huang and Pearlson (2019) argue that cybersecurity presents a relatively new set of threats to organisations. The high level of uncertainty about cybersecurity risks forces leaders to turn to peer institutions for guidance on how to respond. Furthermore, the rapid adoption of cybersecurity practices by other organisations in the organisational field, and the increasing number of customers who have cybersecurity concerns, influence the organisation to adopt cybersecurity practices to maintain their competitiveness.

2.5 Organisational cybersecurity culture model

Creating an organisational cybersecurity culture that aims to align the organisation's values, attitudes, and beliefs with cybersecurity objectives is vital to effectively securing the organisation against cybersecurity threats that aim to exploit human vulnerabilities (Huang and Pearlson, 2019). Organisational cybersecurity culture models comprise several dimensions and subdimensions that aim to explain the relationship and influence between the chosen dimensions on employee behaviours (Uchendu et al., 2021).

Nasir et al. (2019) argue that despite several shared dimensions such as Security Policies, Change Management, Leadership and Governance, User Security Management, Information Asset Management and Trust, amongst cybersecurity culture models, there is a lack of consistency and standardisation of dimensions. They attribute the difference in model dimensions to factors such as the nature of the organisation, approach and objectives of the study, and the cybersecurity maturity level of the organisation. This study aims to explore the role of eThekwini Electricity Unit leadership in creating an effective organisational cybersecurity culture at the eThekwini Electricity Unit. This study utilises the conceptual cybersecurity culture model of Huang and Pearlson (2019), where the leadership dimensions of top management priority, participation, and knowledge, aid the objectives of this study.

As illustrated in Figure 2.4, the conceptual framework of organisational cybersecurity culture demonstrates the influence of external factors and organisational mechanisms on the organisation's cybersecurity culture, which manifests itself through artefacts such as employee behaviours (Huang and Pearlson, 2019).

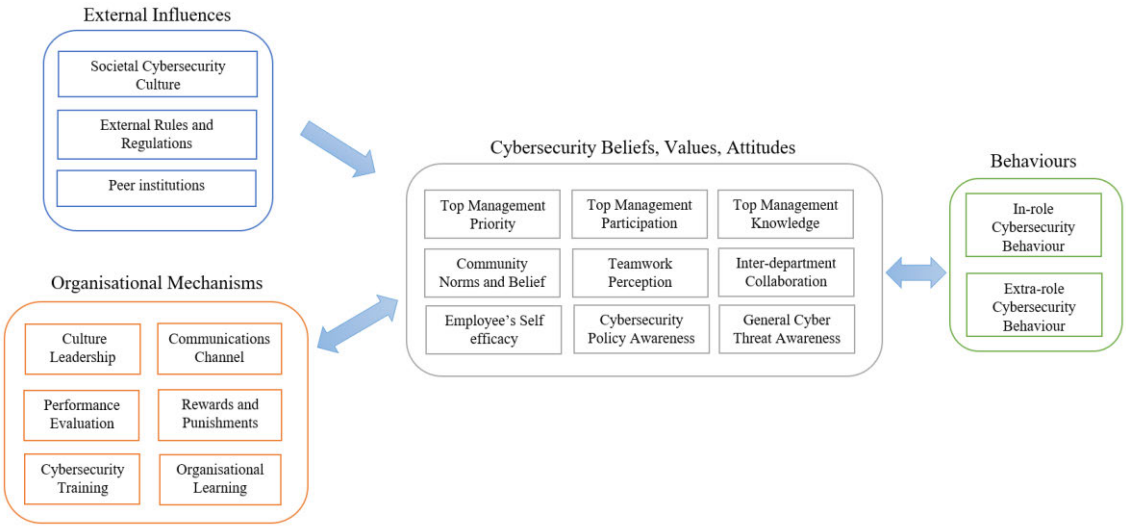


Figure 2.4: Organisational cybersecurity culture conceptual framework. Source: adapted from Huang and Pearlson (2019, p. 6404).

The external factors that shape cybersecurity culture are modelled by the external regulations, societal cybersecurity culture and peer institutions. Leaders use organisational mechanisms to influence the beliefs, values and attitudes of employees. These mechanisms include culture leadership, communications channel, performance evaluation, training, organisational learning and rewards and punishments (Huang and Pearlson, 2019). The organisational cybersecurity culture defined by the beliefs, values, and attitudes contains nine constructs that leaders, groups, and individuals influence. Huang and Pearlson (2019) distinguish two types of behaviours, in-role cybersecurity behaviour that forms part of an individual's duties and extra-role behaviours such as assisting or sharing knowledge. The following subsections discuss each dimension in more detail, examining relevant theories and perspectives from cybersecurity culture literature.

2.5.1 External influences

The cybersecurity culture of an organisation is influenced by numerous external factors ranging from news reports about cybersecurity incidents to government regulations and industry regulatory bodies that the organisation operates in (Huang and Pearlson, 2019). For example, in SA, the NCPF and the POPI Act can be viewed as external influences (The Presidency, 2013; SA Government Gazette, 2015). In addition, Huang and Pearlson (2019) note that external influences such as external regulations, societal cybersecurity culture, and peer institutions heavily influence the organisation's cybersecurity culture.

2.5.1.1 Societal cybersecurity culture

National cultural differences affect how individuals perceive authority and compliance to rules and policies and therefore influence the nation's security and cybersecurity posture and the resulting cybersecurity culture that exists (Da Veiga et al., 2020). Huang and Pearlson (2019) argue that national cybersecurity culture influences individuals' beliefs. Therefore, also influencing the organisational cybersecurity culture created by these individuals. Nations that exhibit strong cybersecurity cultures have a society that values information security and influences organisations that operate in this environment (Huang and Pearlson, 2019).

2.5.1.2 External rules and regulations

External rules and regulations imposed by the government and regulatory bodies define the legal environment in which the organisation operates. Due to the significant risks associated with cybersecurity, many governments and industry regulators have imposed cybersecurity policies and standards that organisations must comply with (Huang and Pearlson, 2019). For example, electric utilities in North America are subject to the North American Electric Reliability Corporation, Critical Infrastructure Protection (NERC CIP) standards (NERC, 2021).

2.5.1.3 Peer institutions

According to institutional mimicry theory, as discussed in Section 2.4.10, organisations are influenced by their industry peers to conform to norms established within their organisational field. Huang and Pearlson (2019) argue that cybersecurity presents a relatively new set of threats to organisations. The high level of uncertainty about cybersecurity risks forces leaders to turn to peer institutions for guidance on responding to these new threats.

2.5.2 Organisational mechanisms

Huang and Pearlson (2019) argue that leaders use organisational mechanisms to influence and shape the cybersecurity culture. They identify the following managerial levers that leaders can employ.

2.5.2.1 Culture leadership

Having a dedicated person with the accountability and responsibility for driving the formulation of organisational cybersecurity culture ensures that cybersecurity initiatives are formulated and actioned effectively. Huang and Pearlson (2019) recommend that someone at the executive level other than the CISO, who has an extensive portfolio, be appointed to this role.

2.5.2.2 Performance evaluation

This managerial lever can be used to influence employee behaviour through the performance appraisal process. Expectancy theory, discussed in Section 2.4.6, outlines how motivating factors influence employee behaviour. Using performance reviews as motivation, leaders can highlight

the importance of the desired cybersecurity behaviours in the organisation, influencing and reinforcing the cybersecurity culture (Huang and Pearlson, 2019).

2.5.2.3 Cybersecurity training

Huang and Pearlson (2019) argue that cybersecurity training is necessary to increase employee awareness around cybersecurity issues, educate employees about cybersecurity, and develop the skills and competencies required for employees to assume cybersecurity roles. They further argue that organisations often undertake cybersecurity training as part of the engagement process and hold annual refresher courses. However, they advocate for regular varied training that reinforces employee knowledge. Glaspie and Karwowski (2017) note that regular training establishes habits that support the cybersecurity policy and therefore foster a culture of cybersecurity.

2.5.2.4 Communications channel

The communications channel used to convey cybersecurity information to employees is crucial to ensuring that the information is received timeously and in the appropriate form for employees to digest (Huang and Pearlson, 2019). Therefore, varied methods of communication are needed. Huang and Pearlson (2019) suggest creating several formal and informal channels for communicating policy information, reporting vulnerabilities and cybersecurity incidents.

2.5.2.5 Rewards and punishments

According to protection motivation theory, discussed in Section 2.4.9, deterrence theory, discussed in Section 2.4.8 and rational choice theory, discussed in Section 2.4.7, rewards and punishments significantly influence employee behaviours. Uchendu et al. (2021) note that rewards and punishments should not merely be used as incentives and not applied. They argue that the enforcement of rewards and punishments determine the effectiveness of the cybersecurity culture campaign.

2.5.2.6 Organisational learning

Huang and Pearlson (2019) note that organisational learning is a mechanism through which an organisation develops, shares, and retains cybersecurity knowledge. Organisational learning is important because of the constantly evolving cybersecurity environment. Information sharing, mentorship, and new knowledge brought into the organisation via subscription to professional bodies are various examples of organisational learning (Huang and Pearlson, 2019).

2.5.3 Organisational cybersecurity culture

Huang and Pearlson (2019) define organisational cybersecurity culture as *"the beliefs, values, and attitudes that drive employee behaviours to protect and defend the organisation from cyber attacks"* Huang and Pearlson (2019, p. 6399). The cybersecurity culture model of Huang and Pearlson (2019), which is founded on the model of organisational culture by Schein (2010),

comprises three organisational levels, the leadership, group and individual level. The following subsections discuss each of the constructs within these levels.

2.5.3.1 Top management priority

Huang and Pearlson (2019) note that leaders will only make cybersecurity a priority if they believe that cybersecurity is important for the organisation. This importance will be reflected in the strategic direction leaders set as well as the allocation of resources, both human and financial, with regards to cybersecurity (Huang and Pearlson, 2019).

2.5.3.2 Top management participation

When leaders become personally involved in cybersecurity initiatives through developing and communicating policies, speaking about cybersecurity, attending training, and making cybersecurity a focus for the organisation, they reinforce the importance of cybersecurity. Employees are influenced by the participation of leadership and are more likely to become involved and participate as well (Huang and Pearlson, 2019).

2.5.3.3 Top management knowledge

Huang and Pearlson (2019) argue that leaders who have skills and competencies relating to cybersecurity will be more knowledgeable about the organisation's cybersecurity vulnerabilities. Therefore, knowledgeable leaders are more likely to value shaping a culture of cybersecurity for the organisation through their participation, prioritisation of initiatives, and allocation of resources towards cybersecurity.

2.5.3.4 Community norms and beliefs

Community norms and beliefs stem from group perceptions of cybersecurity, that is, an individual’s values are shaped by group values. The technology acceptance model, discussed in Section 2.4.2, and social control theory, discussed in Section 2.4.1, highlights the influence of an individual’s social environment on their beliefs and attitudes (Huang and Pearlson, 2019).

2.5.3.5 Teamwork perception

Teamwork perception describes the level of team cohesion regarding cybersecurity activities. The shared team cognition theory, discussed in Section 2.4.3, highlights how teams who share metal models have similar or compatible knowledge which directs their coordinated team behaviour. Interactive team cognition theory, discussed in Section 2.4.4, emphasises team knowledge over individual knowledge. Team perceptions increase the cybersecurity situational awareness of the organisation, as the team level outweighs the sum of individual situational awareness (Huang and Pearlson, 2019).

2.5.3.6 Interdepartmental collaboration

The extent of collaboration between different parts of the organisation influences the organisation's cybersecurity culture and cyber resilience. Huang and Pearlson (2019) argue that effectively securing the organisation from cybersecurity threats requires the integration of cybersecurity into all business functions. Collaboration can be achieved by establishing cybersecurity champions in every department who, through the mechanism of social control, can influence the cultivation of a cybersecurity culture (Huang and Pearlson, 2019).

2.5.3.7 Employee self-efficacy

This construct denotes an individual's level of cybersecurity knowledge and confidence in their ability to take actions to protect themselves and the organisation (Huang and Pearlson, 2019). Social cognitive theory, discussed in Section 2.4.5, highlights the agency mechanism individuals intentionally use to influence their circumstances. Huang and Pearlson (2019) argue that when individuals feel that their actions result in positive contributions towards cybersecurity, they are more likely to undertake those actions.

2.5.3.8 Cybersecurity policy awareness

Employees' awareness and understanding of cybersecurity policy ultimately determine the effectiveness of the policy in fostering the desired behaviours. Huang and Pearlson (2019) note that employees need to understand the desired cybersecurity behaviours and why they are essential for securing themselves and the organisation.

2.5.3.9 General threat awareness

Employee cybersecurity knowledge and understanding of cybersecurity threats determine their level of threat awareness, which is essential for organisational cybersecurity. In addition, individuals who are mindful of cybersecurity threats are more inclined to identify and report suspicious activity (Huang and Pearlson, 2019).

2.5.4 Behaviours

Cybersecurity research has maintained that employee behaviours ultimately determine the cybersecurity posture of the organisation because it is the behaviour, actions or inactions, that creates or mitigates cybersecurity vulnerabilities (Da Veiga and Eloff, 2010; Da Veiga, 2016; Huang and Pearlson, 2019; Nasir et al., 2019; Da Veiga et al., 2020; Uchendu et al., 2021).

2.5.4.1 In-role cybersecurity behaviour

The cybersecurity culture model defines in-role cybersecurity behaviours as those that are part of an employee's official job function. The organisation's cybersecurity policy defines the desired behaviours that apply to all employees, such as not sharing passwords (Huang and Pearlson, 2019).

2.5.4.2 Extra-role cybersecurity behaviour

Extra-role cybersecurity behaviours describe activities that employees undertake that go beyond what is required of them. These are categorised into helping and voicing behaviours. Helping behaviours refer to utilising their cybersecurity knowledge to assist colleagues in cybersecurity-related queries. Voicing behaviours refer to promptly communicating cybersecurity risks and vulnerabilities when they are identified. In addition, the voicing behaviour is instrumental in encouraging employees to speak up about cybersecurity threats or vulnerabilities that they observe (Huang and Pearlson, 2019).

2.6 Gaps in literature

Current research perspectives on organisational cybersecurity culture suggest that it is difficult to build and quantify due to the lack of consensus of the standard set of dimensions for the concept (Leidner and Kayworth, 2006; Da Veiga and Eloff, 2010; Da Veiga, 2016; Huang and Pearlson, 2019; Nasir et al., 2019; Da Veiga et al., 2020; Uchendu et al., 2021). This difficulty is due to the influence from adopted theories, information security maturity level and types of organisations, affecting the formulation of the cybersecurity models. Furthermore, the lack of consistency in dimensions limits the generalisation of the results of cybersecurity culture studies to other organisations (Nasir et al., 2019).

Moreover, cybersecurity culture research has predominantly focused on utilising quantitative research methods to develop and validate cybersecurity culture frameworks and models (Nasir et al., 2019; Uchendu et al., 2021). Uchendu et al. (2021) argue that quantitative cybersecurity culture studies that use survey methods to assess employee knowledge of cybersecurity policies lack the richness of information that can be obtained using qualitative studies. Furthermore, Fertig, Schütz and Weber (2020) argue that employee knowledge does not always indicate employee behaviour. Therefore, Uchendu et al. (2021) advocate the use of qualitative methods, which can be more beneficial in determining what factors influence the development of organisational cybersecurity culture.

A majority of studies on information security culture and cyber security culture have identified the importance of top management/leadership support in developing cybersecurity culture, but few have focused explicitly on the role of leadership in creating a cybersecurity culture (Glaspie and Karwowski, 2017; Nasir et al., 2019; Uchendu et al., 2021). However, Huang and Pearlson (2019) argue that leaders play a vital role in cultivating the cybersecurity culture. Leaders can achieve this by having the necessary cybersecurity knowledge, participating in cybersecurity activities, and making cybersecurity a priority for the organisation.

Uchendu et al. (2021) argue that many conceptual models of organisational cybersecurity have not been validated in the corporate environment. Furthermore, theoretical models of

organisational cybersecurity culture have not always provided clear guidance on the application for practitioners. The conceptual framework of an organisational cybersecurity culture proposed by Huang and Pearlson (2019) used in this study was validated using a qualitative case study in the financial sector.

Uchendu et al. (2021) note that although cybersecurity culture research has been conducted in various industries, only two studies focus on organisations that manage critical infrastructure (Ghafir, Saleem, Hammoudeh et al., 2018; Nævestad, Meyer and Honerud, 2018). Notably, none of the studies reviewed in the last decade explicitly focused on critical infrastructure organisations such as electric utilities (Nasir et al., 2019; Uchendu et al., 2021). The gaps in the literature highlighted above support the focus of this study in undertaking qualitative research to examine the role of leadership in creating an organisational cybersecurity culture to secure organisations that manage critical infrastructure.

2.7 Chapter summary

This literature review chapter examined how culture, leadership, and cybersecurity contribute to understanding how leaders can develop an effective organisational cybersecurity culture to secure against cyber attacks aimed at exploiting human vulnerabilities. In order to define and contextualise the concept of organisational cybersecurity culture, the influence of national cultures, organisational cultures and related information security subculture was discussed. Employee behaviour ultimately determines the organisation's cybersecurity posture because it is the actions or inactions that create or mitigate cybersecurity vulnerabilities. Therefore, developing a cybersecurity culture is key to shaping the desired cybersecurity behaviours. Several factors that enable organisations to analyse, build, and shape their cybersecurity culture were reviewed. The role of leadership in developing a cybersecurity culture was also examined. Although top management/leadership support is the most cited factor in recent literature on cyber security culture, few studies have explicitly focused on the role of leadership in creating a cybersecurity culture. Leaders cultivate cybersecurity culture through their knowledge, participation and prioritisation of cybersecurity initiatives. The theoretical framework that underpins this study and the organisational cybersecurity culture model was also discussed. The chapter concludes by outlining the gaps in literature relating to organisational cybersecurity culture and how this study contributes to addressing them by conducting qualitative research to explore the role of leadership in creating an organisational cybersecurity culture to secure organisations that manage critical infrastructure. The next chapter details the research methodology, focusing on the research philosophy and approach, study setting, sample strategy, data collection and analysis methods used to achieve the objectives of this study.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Introduction

This chapter details the research methodology that was used to achieve the research objectives outlined in Chapter One. The chapter begins by restating the aim of the study to contextualise the decisions taken in designing the research. Thereafter, an overview of research design methods are presented, and the justification of the chosen method is discussed. Next, the research philosophy and approach are outlined before discussing the study setting. Then, the sampling strategy, data collection, and data analysis methods used to achieve the objectives of this study are detailed. The chapter concludes by addressing data validity and reliability concerns, acknowledging researcher bias, and addressing ethical considerations.

3.2 Aim of the study

This study aimed to explore the role of eThekwini Electricity Unit leadership in creating an effective organisational cybersecurity culture at the eThekwini Electricity Unit. This study assists in addressing the cybersecurity challenges facing eThekwini Electricity by fostering a culture of organisational cybersecurity. Furthermore, this study makes recommendations that outline the leadership role in improving the organisational cybersecurity culture.

3.3 Research design

This section describes the decisions made in designing the research to answer the objectives of the study. Justification of the design choices is made based on the nature of this study's research questions and objectives (Saunders et al., 2009, p. 165). The following subsections provide an overview of quantitative and qualitative research methods and their application to cybersecurity culture research. Thereafter justification for the chosen research design is given.

3.3.1 Quantitative research method

This research method is associated with collecting, analysing, and presenting data in numerical form. Quantitative research collects data through techniques such as surveys, performs analysis using statistical methods and presents the results through charts or graphs (Saunders et al., 2009, p. 165). The positivism research philosophy is typically employed because of the highly structured nature of quantitative designs. However, Saunders et al. (2009, p. 166) note that the interpretivist and pragmatist philosophies may also be used depending on the type of data collected, especially opinion-based data. This method can be used with both the inductive, theory-building or deductive, theory-testing approach. Data collection is undertaken using standardised instruments such as questionnaires or structured interviews to standardise the responses from

participants. Standardisation of data enables relationships to be examined between the variables using statistical analysis techniques (Saunders et al., 2009, p. 166).

Cybersecurity culture research has predominately used the quantitative research method to assess the security culture within organisations. Sas, Hardyns, van Nunen et al. (2021) examined 16 studies between 2000 and 2019 found that all studies used the quantitative research method. They argue that this is due to the technique's ease of application, low cost, and statistical robustness. This finding is consistent with that of Uchendu et al. (2021), who further noted that the quantitative research approach has limitations such as undertaking analysis at a single point in time and further suffers from self-report bias.

3.3.2 Qualitative research method

Saunders et al. (2009, p. 168) argue that the interpretive philosophy is well suited to the qualitative research method because it aims to develop an understanding of subjective and socially constructed phenomena. Qualitative research is undertaken in the natural setting of the participants to establish an in-depth understanding of the problem in its natural environment. Both inductive and deductive approaches to theory development may be used. However, the inductive approach is predominantly used to build theories or develop richer perspectives of existing theories (Saunders et al., 2009, p. 168). Qualitative research can use many different strategies, data collection techniques, and methods of analysis. However, the essential characteristic of qualitative research is that data collection is non-standardised such that meanings and relationships can be established from the participant's views (Saunders et al., 2009, p. 168).

Recent survey studies on cybersecurity culture research have noted that there is a lack of qualitative research designs used to assess cybersecurity culture in organisations (Sas et al., 2021; Uchendu et al., 2021). Moreover, Sas et al. (2021) argue that further qualitative research needs to be undertaken to provide more detailed insight into a complex concept such as cybersecurity culture.

3.3.3 Justification of research design

Saunders et al. (2009, p. 174) argue that based on the nature of the research question and research objectives, the research design closely relates to either an evaluation, descriptive, explanatory, or exploratory purpose of the research. This study aims to gain a deeper understanding to explore the role of eThekwini Electricity Unit leadership in creating an effective organisational cybersecurity culture at the eThekwini Electricity Unit.

A qualitative exploratory study is most appropriate to develop this understanding based on the organisational and social concepts that need to be understood to develop a cybersecurity culture. The choice of research strategies suited for qualitative research is a case study, narrative inquiry,

grounded theory, action research, and ethnography (Saunders et al., 2009, p. 178-184). This study used the case study research strategy, as this allowed for an in-depth investigation of organisational cybersecurity culture in its native environment. Further support for this choice of research design is provided from the literature on cybersecurity culture studies. Uchendu et al. (2021) advocate the use of qualitative methods, which can be more useful in determining what factors influence the development of organisational cybersecurity culture.

3.4 Research philosophy

The research philosophy used in this study is that of interpretivism. A positivist philosophy is not suited to this research because positivism is associated with the assumption of observable and measurable facts, causal explanations, and deductive generalisations formed via hypothesis testing. Furthermore, positivism limits the exploration of the social context of organisational cybersecurity culture (Saunders et al., 2009, p. 136). They further argue that interpretivist research aims to create new, richer understandings of the social constructs and are well suited for complex business environments. Interpretivism acknowledges that the different cultural backgrounds, circumstances, and experiences of people create different social realities. Therefore, employees at different levels would experience different workplace realities in an organisational context, creating complexity in meaning and interpretations of their views (Saunders et al., 2009, p.141).

The application of interpretivism in information security and cybersecurity research allows the participants to express their views on aspects of cybersecurity based on their background and understanding (Koskosas, Kakoulidis and Siomos, 2011; Da Veiga, 2016). Similarly, this study collects data based on the participants' experiences relating to the role of leadership in cultivating a cybersecurity culture at eThekwini Electricity. Therefore, interpretivism is well suited to the research. It enables more profound insight into the leadership role and challenges of establishing an organisational cybersecurity culture from a social perspective.

3.5 Study setting

The study was undertaken at eThekwini Electricity, a Unit within eThekwini Municipality, Durban, South Africa. eThekwini Electricity purchases electricity from Eskom and distributes it to over seven hundred and forty thousand industrial, commercial and residential customers across the eThekwini metropolitan region (Electricity, 2020). This organisation was chosen for the study as cyberattacks on critical infrastructure such as electric utilities are becoming more frequent, and eThekwini Electricity faces the challenge of securing the organisation against cybersecurity threats that aim to exploit human vulnerabilities.

3.6 Sampling strategy

eThekwini Electricity has a staff complement of approximately two thousand five hundred employees. Approximately fifty-eight employees are involved in the organisation's cybersecurity initiatives, forming the research population. From this population, the target population comprises fourteen employees who are involved in cybersecurity strategies, policies, and projects at a leadership level within the organisation. These individuals comprise executive management, senior management, and senior technical experts.

This study uses non-probability purposive sampling to select individuals within the target population based on their ability to provide valuable insight that will enable suitable answers to be developed for the study objectives and research questions (Saunders et al., 2009, p. 301).

3.7 Sample size

A sample size of 10 participants was chosen from the target population based on their knowledge of cybersecurity programs and practices within the organisation. These participants possess the first-hand experience and knowledge required to provide meaningful information relating to the conceptual framework used for this study. Furthermore, similar qualitative studies have reached saturation with similar sample sizes (Robinson, 2014; Bascomb, 2020; Hussey, 2021).

3.8 Study participants

The participants of this study consist of executive management, senior management, and senior technical experts from the ICT, Network Control and Communication Network branches. These individuals have in-depth knowledge of the organisation's cybersecurity programs. As indicated in Table 3.1, two participants from executive management, four senior managers, and four senior technical experts participated in this study.

Table 3.1: Categories and number of study participants.

Designation	Number of participants
Executive management	2
Senior management	4
Senior technical experts	4
Total	10

Initial contact with participants was made via telephone. This was done to establish the purpose and nature of the research. Participants then felt more comfortable in agreeing to partake in the study. The interview appointment date and time was agreed upon, and the gatekeepers' letter and informed consent form was then emailed to participants to complete and return.

3.9 Data collection method

Primary data collection methods for exploratory qualitative research comprise unstructured or semi-structured interviews, where the questions posed to the participant are unstandardised. Semi-structured interviews consist of key questions and a set of themes that the interviewer uses to establish a conversation (Saunders et al., 2009, p. 391). Using open-ended and probing questions enables participants to express their views on a particular topic in a manner that is suitable to them (Saunders et al., 2009, p. 393-394).

This study used the researcher as the data collection instrument and undertook primary research using semi-structured interview data collection techniques to address the main research objective adequately. Using the semi-structured interview technique allowed the researcher to pose various open-ended questions from the interview schedule to participants. The interview schedule was developed based on the different dimensions of organisational cybersecurity culture identified from the literature review and organisational cybersecurity culture model discussed in Chapter Two. Where necessary, the researcher posed probing questions to delve deeper into the responses provided by the participant. Probing participants further provided richer responses that were in line with the research objectives (Saunders et al., 2009, p. 408). The semi-structured interview method also allowed the interviewer to clarify the context or meaning of the questions, therefore providing the participants with sufficient context and understanding for them to be able to respond meaningfully.

Due to the coronavirus (COVID-19) pandemic, social distancing measures necessitated the use of online videoconference platforms over which to conduct the interviews. Participants were advised that interviews would be held using online platforms. All participants had access to online videoconference applications via organisational resources and had no trouble accessing and using the applications as they are used daily in the organisation. Interviews were scheduled at a time that was most appropriate for the participants. Due to the unpredictable schedule of some of the participants, several interviews were rescheduled at a more appropriate time.

At the start of the interview, participants were reminded of the contents of the informed consent form, which detailed their anonymity and the request to record the interview. Participants were then provided with a brief background to the research and an overview of the research aim and objectives. This was necessary to provide context and highlight the importance of the study to participants. The interview commenced once the participants were comfortable to proceed (Saunders et al., 2009, p. 406).

The interviews started with general open-ended questions relating to cybersecurity challenges facing the organisation. This was done so that the participants could become comfortable and settle into the interview. Based on the responses from the participant, the interviewer could gauge

the level of knowledge relating to the dimensions of cybersecurity culture and leadership. If necessary, the participants were then asked probing questions based on their responses. Saunders et al. (2009, p. 404-411) note that this technique improves the interview quality as participants are comfortable sharing their knowledge. Furthermore, internet-mediated interviewing methods such as videoconferencing allow participants to undertake the interview from different geographic locations and in an environment comfortable and familiar (Saunders et al., 2009, p. 426). The length of the interview sessions ranged between forty minutes to three hours, depending on the depth of the participants' knowledge.

This study leveraged the additional benefits of videoconferencing applications such as recording the interview proceedings and automatic transcript generation (Salmons, 2012). Permission was sought from participants before any recordings or transcripts were taken. The automatic transcripts generated by the software often contain misinterpreted words that can change the context of the conversation. The interview recordings were used to edit and clarify all the automatically generated transcripts to remove these errors.

3.10 Data analysis

Saunders et al. (2009, p. 568-569) note that qualitative data derives its meaning from words and is therefore non-standardised. Therefore, qualitative data requires interpretation, categorisation, and conceptualisation of what has been said by the participants. Data analysis for qualitative research is founded on thematic analysis, which aims to identify and analyse patterns in qualitative data (Clarke and Braun, 2013). Thematic analysis involves the researcher searching for patterns in the data called themes, which can be based on the research objectives, and then categorising them in a process called coding (Clarke and Braun, 2013). In an inductive approach, the themes result from the data, and the researcher does not attempt to analyse the data based on predetermined theory. In a deductive approach, the themes are predetermined and are linked to existing theory and the research objectives (Saunders et al., 2009, p. 579).

Thematic analysis of transcripts was undertaken to identify themes that connect to the study objectives (Joffe, 2012). Following the process of thematic data analysis described by Clarke and Braun (2013), the content of the transcripts was read and revisited several times so that the researcher could become familiar with the content, derive meaning, and search for patterns. Thereafter patterns in the data were identified by examining keywords and phrases that participants frequently used, and for each extract, a code was assigned that summarised its meaning. Extracts with similar meanings were given the same code, and new codes were generated and assigned as new meanings emerged. Finally, reoccurring and related codes were categorised into themes and subthemes. The literature review and theoretical framework detailed in Chapter two was used to interpret and analyse the data iteratively. This process refined the

codes into the seven themes and thirty-six sub-themes that emerged. The NVivo (QSR, 2020) data analysis software was used to assist in analysis and data management.

The interpretive nature of this research necessitates the analysis and classification of the data into themes. The themes that emerged from the data aid the explanation of the challenges facing leaders in creating an effective organisational cybersecurity culture at eThekwini Electricity.

3.11 Data validity and reliability

Qualitative research using semi-structured interviews leads to data quality concerns in the form of repeatability, researcher bias, cultural differences and validity (Saunders et al., 2009, p. 396). Creswell and Creswell (2017, p. 313) describe qualitative reliability as having a consistent approach to undertaking the research. The reliability of this study is maintained by undertaking diligent documentation of the methods and procedures. Furthermore, a thorough explanation of the choices made and detailed descriptions of how the data was collected is provided in this chapter (Creswell and Creswell, 2017, p. 315).

Qualitative data validity denotes maintaining the accuracy of the research findings (Creswell and Creswell, 2017, p. 313). Data validity is maintained using open-ended interview questions, clarifying questions and probing questions (Saunders et al., 2009, p. 407). The interviews were also recorded and transcribed to minimise any misinterpretations of the participant's views. Furthermore, the empirical data gathered in this research is compared to similar studies to provide theoretical validity should there be a correlation between the findings (Johnson, 1997).

3.12 Researcher bias

Saunders et al. (2009, p. 397) note that researcher bias can be described as how the researchers verbal and nonverbal communication during an interview creates biases in how the participant responds to the questions. Bias results when the researcher imposes his or her mental models, beliefs, and frames of reference on the participant through the manner or types of questions posed during the interview (Saunders et al., 2009, p. 397). Creswell and Creswell (2017, p. 294) note that the researcher should explicitly acknowledge that their background, values, and biases influence the interpretations of the study and that precautions need to be taken to suspend the influence of their bias during the study. Therefore, the researcher was cognisant of his reflexivity and made notes of biases that could influence the research (Watt, 2007). The notes reminded the researcher not to introduce researcher bias throughout the research process, especially in the interview and data analysis phases.

3.13 Ethical considerations

The research was undertaken using sound ethical practices to ensure that the participants and the organisation under study were protected. The University of KwaZulu Natal (UKZN) ethics office approved ethical clearance to conduct this research. Ethical clearance granted the researcher permission to collect data in the form of interviews. Furthermore, the ethical conduct of this research was guided by the UKZN ethics guideline that details the ethical best practices that must be followed. Furthermore, permission to undertake this research at eThekwini Electricity and interview participants from the organisation was granted by the head of the Unit in the form of a gatekeepers letter.

All participants were provided with an informed consent form that outlined the requirements for the study and further highlighted that their decision to participate in the study was voluntary. Interviews only commenced upon the approval of ethical clearance, gatekeepers letter, and informed consent forms. Before commencing each interview, the participants were reminded of the contents of the informed consent form and that recordings and automatic transcripts of the interview would be taken. Permission for this was sought once again. At the start of the interview, participants were provided with a background to the study and enough information so that they could understand the aims of the research and how it would contribute value to the organisation.

The researcher shall maintain the participants' anonymity and data confidentiality according to the POPI Act (The Presidency, 2013) and UKZN requirements. No personal information identifying the participants was needed or collected for this research. All data collected shall be anonymised and stored on a secure online drive for a period of five years. Thereafter it will be destroyed. The link to the data shall be provided to the supervisor. Should the need arise, all data collected from the study shall be made available to UKZN upon request.

3.14 Chapter summary

This chapter details the research methodology that was used to undertake this study. The aim of the study was outlined in order to contextualise the decisions taken in designing the research. An overview of quantitative and qualitative research methods was discussed before justifying the use of a qualitative research method. A discussion of why the research philosophy of interpretivism is well suited to the research was provided. The study setting, eThekwini Electricity, was described to explain where and why the research was undertaken in this organisation. The sampling strategy, data collection and analysis methods used to achieve the objectives of this study were then detailed. The study undertook primary research using semi-structured interview data collection techniques. Thematic analysis of transcripts was undertaken to identify themes that connect to the study objectives. This provided deeper insight into the challenges facing leaders in creating an effective organisational cybersecurity culture. Thereafter techniques to

address data validity and reliability were discussed. The issue of researcher bias was discussed and acknowledged. Lastly, ethical considerations were described, and how this study addressed them were discussed in detail. The next chapter presents the results obtained from the semi-structured interviews. Thematic analysis was conducted on the interview transcripts to reveal themes that emerged from the participant's views. The key themes were highlighted using direct quotations from the participants.

CHAPTER 4: RESULTS

4.1 Introduction

This chapter presents the results obtained from the semi-structured interviews conducted at eThekwini Electricity. Chapter Three of this dissertation details the research methodology used to capture qualitative data from the research participant's views on the role of eThekwini Electricity Unit leadership in creating an effective organisational cybersecurity culture. The interviews were transcribed, and thematic analysis was conducted to reveal themes that emerged, providing deeper insight into the challenges facing leaders in creating an effective organisational cybersecurity culture.

This chapter begins by providing an overview of the study participants. Then, the thematic framework containing the key themes and subthemes are tabled before discussing the findings in greater detail. The key themes that were identified are supported using direct quotations from the participants.

4.2 Study participants

The details of each of the ten study participants are outlined in Table 4.1 below. To maintain the anonymity of the participants, the table only provides the designation and a range of years of experience of the participants in the electricity supply industry.

Table 4.1: Details of the study participants.

Participant number	Designation	Years of experience
P1	Senior technical expert	10 to 15 years
P2	Senior management	10 to 15 years
P3	Executive management	25 to 30 years
P4	Senior management	10 to 15 years
P5	Senior technical expert	5 to 10 years
P6	Executive management	25 to 30 years
P7	Senior technical expert	10 to 15 years
P8	Senior technical expert	5 to 10 years
P9	Senior management	10 to 15 years
P10	Senior management	15 to 20 years

4.3 Themes and sub-themes

This section provides an overview of the key themes and sub-themes that emerged from the thematic analysis of the interview data. The resulting thematic framework, presented in Table 4.2, details the seven themes and thirty-six sub-themes that were identified.

Table 4.2: Themes and sub-themes.

Theme	Sub-theme
4.4 Cybersecurity Challenges	4.4.1 Cybersecurity risk
	4.4.2 Internal state of the organisation
	4.4.3 Insider threats
	4.4.4 Organisational structure
	4.4.5 Cybersecurity incident experience
	4.4.6 Resource constraints
	4.4.7 Skills
	4.4.8 Sector
4.5 Cybersecurity Awareness	
4.6 Cybersecurity Culture	4.6.1 Leadership role
	4.6.2 Leadership knowledge
	4.6.3 Leadership participation
	4.6.4 Leadership priority
	4.6.5 Leadership accountability
	4.6.6 Employee general threat awareness
	4.6.7 Employee cybersecurity policy awareness
	4.6.8 Employee motivation
	4.6.9 Employee knowledge
	4.6.10 Employee accountability and responsibility
	4.6.11 Employee commitment
	4.6.12 Trust
	4.6.13 Interdepartmental collaboration
4.7 External Influences	4.7.1 Peer institutions
	4.7.2 External rules and regulations
	4.7.3 Societal cybersecurity culture
	4.7.4 Professional bodies
4.8 Organisational Mechanisms	4.8.1 Strategy, policy, procedures
	4.8.2 Cybersecurity training
	4.8.3 Communications channel
	4.8.4 Recruitment
	4.8.5 Human resources

	4.8.6 Cybersecurity systems
	4.8.7 Performance evaluation
	4.8.8 Change management
	4.8.9 Financial resources
	4.8.10 Cybersecurity champions
	4.8.11 Rewards and punishments
4.9 Safety Culture	
4.10 Behaviours	

The following subsections discuss each of the themes and sub-themes in greater detail. In addition, relevant unedited extracts from the participant's transcripts are provided to support the theme.

4.4 Cybersecurity challenges

Participants indicated that there are numerous cybersecurity challenges facing the organisation. Each of those challenges is discussed as a sub-theme in the following subsections. The word cloud in Figure 4.1 illustrates the participant's views collated under the theme cybersecurity challenges. The word cloud illustrates words that were frequently said by the participants. For example, the words risk, people, system, business and network were frequently mentioned for the theme of cybersecurity challenges.

Figure 4.1: Word cloud - cybersecurity challenges.

As a key theme, majority of the participants said that the organisation's cybersecurity challenges, particularly those that prevent the development of an organisational cybersecurity culture, stem from the lack of declared values, governance structures, and a consolidated strategy for cybersecurity.

One participant linked the lack of declared values in the organisation back to the absence of those values in the greater municipality.

"At this point we as a city have not created a set of values and the culture that we want to create in the city. If you if you say what is the value system at the eThekwini municipality, you'll find nothing. So, so the starting point is that the city does not have a set of values that they've declared or a culture that they've declared that they want to see being displayed by all employees." (P3).

Another participant highlighted that the organisation's lack of a governance structure for cybersecurity is a key challenge.

"I think the challenge is that we don't have adequate governance structures for the organisation in general, so hence why we don't have the governance structure to cover cybersecurity adequately." (P2).

This was supported by another participant who added that the absence of a consolidated strategy and governance framework for cybersecurity is the primary reason for not addressing the cybersecurity challenges adequately.

"So, I think, holistically, though, because of the lack of some sort of consolidated strategy within our business and not only within our business but within the greater municipal business, the lack of a consolidated strategy or a governance framework around cybersecurity is probably the reason why we haven't fully addressed the challenges that exists out there." (P4).

The following subsections discuss participants views on how the lack of declared values, governance structures, and a consolidated strategy for cybersecurity pose cybersecurity challenges for the organisation.

4.4.1 Cybersecurity risk

Participants felt strongly about the numerous cybersecurity risks facing the organisation. One participant highlighted that the challenges from a cybersecurity perspective, compared to the other risks facing the organisation, stem from the nature of the cyber environment.

"The challenges with cyber is that your risk could come from anywhere in the world, so I think that's one of the challenges we have is that the dynamics are different with regards to the cybersecurity environment." (P2).

Many of the participants indicated that the impact of cybersecurity attacks on organisations such as electric utilities could be significant. The economy's dependence on the electricity grid makes the electricity grid an attractive target for those who want to disrupt economies and society. One of the participants said:

"I will say from a target perspective is that utilities by nature are extremely critical to economies. So, we actually become a target, a potential target to individuals that may want to disrupt economies or obviously to access systems for economic gain, so I think that's one of our challenges that our business environment is that of a mission critical nature, so it actually makes us a target." (P2).

Another participant supported this view in saying that:

"I think nations worldwide understand that if the electricity grid is compromised, the economy is so closely tide to the grid, it could have a devastating impact on the economy as a whole." (P4).

The participant continued to provide an example of the impact, saying:

"if you access the system, there's certain functionality that can be very devastating. It can cause widespread damage. Yeah, because like I mean, even if you look at our load shedding software tool, I mean one incorrect configuration can cause the entire eThekwini region to switch off and on every second if you want." (P4).

This view is supported by another participant who additionally highlighted the value of the organisation's information and systems.

"One very simple one which is our prepaid vending system. If that system is down for two minutes, it'll cause chaos. So again, our hack value becomes quite important when you look at the impact of our stuff. So, if you look at something like prepaid vending, our call centres, our substations, our customer data. Again, hack value plays a very big role in our security and people don't understand the repercussions of it." (P8).

Electricity distribution is by nature a very dangerous environment. One participant emphasises the most significant implication of a cybersecurity attack on the organisation by saying:

"The possibility of outages or damage to critical infrastructure which could relate into either short-term outages or long-scale outages or catastrophic damage and ***loss to life****."* (P2).

Therefore, cybersecurity attacks can have severe consequences for the organisation itself, its employees, and society. Another participant highlighted that the adoption of technology to improve business functions is a primary reason for cybersecurity becoming a risk to the organisation.

"As we starting to embrace the 4th Industrial Revolution, we find that we are becoming more and more automated in a lot of our activities that would have previously been done manually. OK, so for example our distribution automation project where we are automating the controlling of our field devices remotely. So obviously going forward, that's going to become a huge challenge for

us as a utility. Because I think by embracing technology, we've actually, you know, we created an environment where cybersecurity becomes a risk." (P6).

The participant further acknowledged that the cybersecurity risks introduced by the digitalisation drive in the organisation move the cybersecurity risk from historical areas of concern to new areas of the organisation, which may not have been considered.

"We looked at it historically from our most high-risk place, which was the HV Control Centre. We never looked at it beyond this, but now that we are discussing it, I can see that the risk is probably sitting even much lower down in the organisation." (P6).

This view is supported by another participant who said:

"Remember, digitalisation is what drives security. I mean, if you're not going to digitise and you still going to remain with electro-mechanical equipment. The cybersecurity impact is far less. So, digitalisation is what really drives cybersecurity efforts." (P4).

The nature of the cybersecurity environment, the attractiveness of electric utilities as a target for cybersecurity attacks, and the digitalisation of business functions all introduce significant risks to the organisation. However, one participant cited human vulnerability as the most significant source of cybersecurity risk.

"The human vulnerability within this cybersecurity chain is probably the greatest vulnerability. Social engineering and so forth is probably the greatest threat to any environment, so it's whether it's at the electricity Unit or any other industry out there, the social aspect or the human aspect is the greatest and will always remain the greatest threat." (P4).

The view that human vulnerability poses the greatest cybersecurity risk to the organisation was a common view shared by the participants.

4.4.2 Internal state of the organisation

Participants shared several views on how the internal state of the organisation presented various cybersecurity challenges. Participants view cybersecurity incidents as low probability, high impact events. Taking this view leads to cybersecurity not being a focus for the organisation. One participant said:

"With regards to challenges, is that you'll find, this is just my view, that cybersecurity is more around resiliency because in most cases it would be a very low frequency event that could have a very high impact." (P2).

This lack of focus on cybersecurity in the organisation leads to the challenge of cybersecurity initiatives being disconnected from the core business function of electricity distribution. One participant said:

"The fact is that there's no alignment between what the core business competency is. There's no alignment between that core business function and the security function of the business." (P4).

This disconnect presents itself in projects that do not cater for cybersecurity at the onset. Departments then have to introduce measures to close the gaps to reduce the vulnerabilities in the systems they manage. One participant emphasised that:

"We didn't really look at security or cybersecurity within the initial life cycle stages and as a result what has happened now is that we see the impact of implementing stopgap solutions or specific solutions, sort of a bolt on solutions, that can come in or resolve the immediate threats." (P4).

Another participant added to the view that cybersecurity is not a priority for the organisation.

"I feel that there isn't that drive in terms of making cybersecurity a high priority. It's not considered as a key item when planning and doing any project. It's considered as an afterthought. It's not considered as a main driving force when doing any sort of projects." (P8).

The lack of priority results in taking a reactive approach to cybersecurity. One participant mentioned:

"If you look on the on the technical side of things, we at a point where we are using a reactive approach, meaning there's no visibility, so we are hoping for the best which is a very reckless approach." (P5).

Participants mentioned that the default approach to addressing the gaps in cybersecurity was to implement technology solutions.

"I think in the simple one which everyone goes to by default would have been tightening up on technologies that would allow us to monitor and filter information or call it the parameters or points of access into the network. I think that's the easy one." (P2).

"I think we, within the different branches within the municipality, have looked at those technical controls, but it's at this point, I feel within our unit specifically. That's the only thing we've been doing. We've been throwing technology at many of our challenges. We haven't really taken a risk-based approach and looked at cybersecurity holistically within the business." (P4).

Furthermore, the participants highlighted that each branch had undertaken isolated activities to secure the organisation at a branch level.

"We haven't holistically defined a top-down strategy for the OT network. We've looked at it specifically for the branch, but we haven't aligned that to the business function, and only until that's done can I really say that we have an overarching strategy towards cybersecurity." (P4).

The lack of a holistic approach to cybersecurity and the implementation of technology solutions to address cybersecurity challenges highlights the cybersecurity maturity level of the organisation. One participant felt that the organisation has a very low level of cybersecurity maturity.

"When you look at our maturity levels, we are at a very bottom level when it comes to implementation of cybersecurity services." (P9).

The participant also adds that the organisation has not matured enough to view cybersecurity as an investment. At this point, cybersecurity initiatives are reactive and are viewed as an expense to the organisation.

"You know, in most organisations. Starting from CEO to executives, the concern is revenue gain in terms of any service that brings in revenue. So, for us it's our core business of power distribution. Remember, cybersecurity services are expensive. So as soon as you talk investment around cybersecurity it's like you throwing money away because people want to react when there is a threat. They don't want to invest proactively. So, we are not matured in this regard." (P9).

4.4.3 Insider threats

Participants view the threat from employees (insiders) as more significant than external sources. One participant highlights the challenge presented by disgruntled employees.

"A lot of the threats might come from internally, from disgruntled employees. So, that's the big thing that we need to be concerned with. Not so much the external threats. It's also the internal threat." (P3).

"Nothing says they can't go into a system and try and do it covertly by trying to hack the system from inside. Our SCADA networks, be it our computer network or metering systems even. You know that's a big concern." (P3).

"What I'm then saying is that there's a greater likelihood of attacks from within." (P3).

This view was supported by another participant who said that:

"You know if an employee is disgruntled and wants to ideally cause havoc on there. It probably is a very easy thing to target, target your meters. Your vending stations that can really create havoc in that environment that has a direct customer impact." (P6).

Another participant felt that creating a cybersecurity culture can help address the challenge presented by employees that intend to disrupt the organisation.

"So, we need to have a culture in the organisation that actually then promotes people to use their knowledge as well as be part of the organisation. And I think once you have that. People are able to be more involved. Once you have that involvement, then it is less likely that you would have people trying to do intentional damage. Now, in other words, people that know about the network and how to sabotage it will obviously be less inclined to do that." (P7).

4.4.4 Organisational structure

Participants viewed that the current organisational structure presents several challenges to effectively addressing cybersecurity. The digitalisation drive within the organisation is the primary activity that introduces cybersecurity risks. One participant said:

"Currently within eThekwini Electricity, I think the issues around not having the right organisational structure to support digitalisation. We haven't really looked at redesigning the organisational structures to support that digitalisation drive" (P4).

The lack of an organisational structure to support cybersecurity, results in silos where each department takes an isolated approach to address cybersecurity vulnerabilities within their area. However, this opens other avenues of vulnerability for the organisation. The participant further adds:

"We have this spill over of tactical plans that we wish to implement between the branches. Which creates sort of grey areas which causes new vectors of attack to open up for cyber threats out there. And the lack of the correct organisational structure, I think really plays a key role" (P4).

This view is supported by another participant who highlights the importance of explicitly setting up the organisational structure to support cybersecurity over implementing technology solutions.

"We are still battling with the structure, meaning organisational structure when it comes to dealing with cybersecurity at large." (P5).

"They should raise an alarm and try to fast track the organisational structure regarding cybersecurity, as opposed to getting more tools because, we can get as big tools as you want, but if we do not have a proper procedure that will involve human resources because people at the end are hired via human resources. So, if there is not approached from that side, then we find ourselves in this position where we are putting out fires." (P5).

4.4.5 Cybersecurity incident experience

Several participants believed that because the organisation had not experienced any cybersecurity incidents that they were aware of, the risks posed by cybersecurity attacks were therefore low compared to other known risks such as health and safety. For example, in comparing health and safety risks with cybersecurity risks, one participant said:

"That's where the differences between cybersecurity and safety is, that we still at a more immature phase with regards to cybersecurity. I think, like I indicated earlier, if you picked up more incidences with regards to cybersecurity. I agree with you, we most likely would have aligned towards how we've applied it to a safety-oriented culture" (P2).

In discussing cybersecurity attacks that may originate from disgruntled customers who received incorrect electricity bills, one participant said:

"So maybe the issue is so far to date, you know there's lots of people who got lots of high bills when we moved from Coins to RMS. You know? but you're right, we give people lots of bills. It hasn't materialised. It means it's a low risk, very low risk." (P3).

In referring to cybersecurity incidents, the same participant stated that the organisation had not experienced any cybersecurity incidents as far as he is aware.

"So far I don't think it's really happened." (P3).

Another participant shared the same view and added that the lack of cybersecurity incident experience is probably why cybersecurity risk is not a focus for the organisation. Therefore, for example, cybersecurity does not influence the decisions made when developing specifications for new systems.

"I do not recall us having any attempts of outsiders trying to access our system. At least I'm not aware of it, and hence it's probably not forefront in our minds when we write our specifications." (P6).

Another participant supported this view but added that even though the business has not experienced a cybersecurity incident, it does not take away from the significance of the impact that it can have on the organisation.

"I suppose there also hasn't been any incidents that were to drive and spark anyone to take it more seriously. I don't think people understand and realise the impact that it has." (P8).

4.4.6 Resource constraints

One participant highlighted that organisational resource constraints contributed to the lack of focus on cybersecurity. The participant said that cybersecurity effectively improves the resiliency of the organisation to continue to provide services.

"Organisations such as ourselves being Electricity, are highly constrained with regards to resources, so our focus area when it comes to managing the organisation is more towards short term challenges and opportunities." (P2).

Being a resource-constrained organisation, one participant indicated that the management team needs to make decisions to optimise its resources. Unluckily cybersecurity projects are reprioritised lower than other activities.

"By minimum, I think activities that need to ensure that the business functions, are given priority. Then activities that improve some of the operational conditions are then considered. Cybersecurity effectively falls under the area of then managing risk that may or may not occur. So unluckily it does take a back seat." (P2).

4.4.7 Skills

Participants mentioned that special skills are needed to address the cybersecurity challenges facing the organisation. One participant highlighted that the complexity and the multidisciplinary nature of cybersecurity requires a special set of skills.

"The other challenge that we obviously have is that it's a very technical issue here in that it falls within the domain of information and communications technology, and I think as the electric utility covers or impacts both the IT and OT domain. So, it requires a special set of resources and capabilities to manage cybersecurity risks." (P2).

Another participant substantiated this view by saying:

"I'm saying cybersecurity is not an easy thing. It's not a simple thing, it's a complex issue. It's changing all the time. You need to recruit people that can quickly learn and adapt. So, you need people with meritocracy at that level to drive and effectively deal with these threats, cybersecurity threats." (P3).

The issue of having the requisite skills to address cybersecurity is not unique to eThekwini Electricity. One participant viewed both the skill and institutionalising a cybersecurity culture as vital aspects in addressing cybersecurity challenges.

"The issue around people I believe is probably one of the biggest challenges that not only electric utilities, but all industries or companies face holistically. The issue on people specifically is around acquiring the right type of skill to maintain an agile or a secure environment. And also,

apart from this skills gap, it's also a, not necessarily just the skills gap rather, but also as you mentioned in your first slide, is also about developing the culture and institutionalising that culture within such individuals." (P4).

4.4.8 Sector

Participants felt strongly that public sector organisations such as eThekwini Electricity faced challenges that were easily addressed in the private sector. For example, in discussing the implementation of cybersecurity policies, one participant mentioned that they were easier to implement in the private sector. The participant said:

"If you look at us, the public sector. The private sector has got an upper hand in implementing such because you know the CEO is right here, everything happens right here. Once they make a ruling, everyone must confirm. As opposed to us, we actually get to hear from the employees because of the red tape that is there and the policies that are there. So, those policies are good. But there can be a serious hindrance in doing such things." (P5).

Another participant shared a similar view as to why public sector organisations are slow to adapt to address cybersecurity challenges. The participant said that the rigidity of the organisation hindered its ability to create new roles to address the fast-changing cybersecurity environment.

"Look at something like the IT industry, there's new jobs and roles being developed every couple of years. We wouldn't have had a business scientist, data analyst, that CIO role, your security officer's role your you know your IT security people. Those rules didn't exist 20 years ago. Our hierarchy or organogram has not adapted and changed and evolved according to that. It's kept the same from the time probably the organisation has started. And the level of change and effort that's required to change that organogram is literally almost impossible. And hence, that's why in the private sector it's easy, tomorrow you can set up a new branch call it cybersecurity 4IR whatever and bang you running. In the government sector, you can never do that. You need budgets, u need changes. It needs to be approved. It's too bureaucratic to do anything." (P8).

The perspectives of these participants highlight how the bureaucracy and rigidity of public sector organisations can hinder their ability to adapt and deal with the challenges brought about by the dynamic nature of cybersecurity. The following section discusses the theme of cybersecurity awareness.

4.5 Cybersecurity awareness

During the interviews, it became clear that the participants felt strongly about the importance of cybersecurity awareness in developing a culture of cybersecurity. The word cloud in Figure 4.2 illustrates the participant's views collated under the theme cybersecurity awareness. The word cloud illustrates words that were frequently said by the participants. For example, the words

people, risk, attacks, understand, and influence were frequently mentioned for the theme of cybersecurity awareness.

Figure 4.2: Word cloud - cybersecurity awareness.

Participants expressed their views on various issues, from an awareness that electric utilities can also fall victim to a cybersecurity attack to awareness of cybersecurity attacks that have impacted other organisations. However, one of the most significant challenges around understanding cybersecurity comes from understanding the word cyber itself. One participant mentioned that:

"A gap with regards to awareness in terms of the concept of cybersecurity and the challenges that an organisation may face. Mainly I think based on the fact that the term starts off with the word cyber. Its something that's is not always highly focused on or aware in terms of organisations." (P2).

Therefore, to be aware, people need to have a basic understanding of the concept of cyber and cybersecurity. Another participant highlighted a lack of awareness that electric utilities can become victims of cybersecurity attacks.

"I think it's the awareness. Mostly I think people are not necessarily aware that an electrical utility is susceptible or could be a target for cybersecurity attacks." (P1).

Other participants also expressed similar views that awareness is a fundamental component of cybersecurity. One participant also added that developing a culture is a solution to secure the organisation against cyber attacks that exploit human vulnerabilities. The participant said:

"I think it all starts with awareness, and awareness is that building of some sort of culture and understanding of what is cybersecurity. What is the need for cybersecurity and what are the

basics in terms of how to protect organisation from the basic or the very basic cybersecurity threats that may exist." (P4).

Another participant supported this view of employees having foundational knowledge and awareness of cybersecurity and provided a basic example of how one would view security in their home compared to security at the organisation. The participant said:

"I believe it starts with just having some basic knowledge and awareness. If you understand that, let's say in an 8-port switch if you using three and the other five were left open. If we have that, just basic knowledge that hey, the same thing as having my house with eight doors and three of the doors are being used by people. But I've left 5 doors open. And if I don't see any issues with leaving 5 doors open in my own house. Then I'll see no issue with leaving five ports open on a switch." (P8).

However, another participant felt that even this basic level of awareness is deficient in the organisation. The participant said:

"For example, someone configuring a modem out on site. If they understand that, if they misconfigured this device it could shut down the economy of Durban. I don't think that level of awareness has been created at this point. So, I think that once at that level of awareness is created, it will really influence behaviour." (P4).

Therefore, it is evident that creating a fundamental awareness of cybersecurity in all employees is key to shaping the desired behaviours. Another participant highlighted a lack of awareness and focus of the concept of cybersecurity as a culture at all levels in the organisation.

"I don't think too many people in the organisation think about it, including employees at a senior level, so I'm not even putting this down to any task grade or something. I'm saying just cybersecurity as a culture, it just not fore in our mind. You know, it's not in the front of our mind in the things that we do." (P6).

Another participant mentioned that even though the organisation is aware and acknowledges the risks posed by cybersecurity. A lack of awareness and understanding of the actual risk prevents the organisation from effectively allocating adequate financial and human resources to address cybersecurity challenges.

"I feel that just my personal view is that if the risk were truly understood, the organisation itself would have had a lot more resources directed towards the mitigation of cybersecurity risks. So while we do have it on our Unit risk register, if you look at the understanding, yes, it is noted in terms of some of the high level risks. But I think it can't be further elaborated upon." (P2).

The above extracts indicate that cybersecurity awareness at all levels of the organisation is low. Therefore, it is not thought about often enough for the organisation to prioritise resources towards addressing cybersecurity risks. However, having a general awareness of the cybersecurity risks brought about by technology can influence the organisation. In discussing how the level of societal cybersecurity awareness can impact the organisation, one participant said:

"So, I think if the region of eThekwini was more aware of cybersecurity challenges or the adoption of technology and the risks, it would automatically filter into the organisation." (P2).

The theme of how societal cybersecurity awareness influences the organisation is discussed in greater detail in Section 4.7.3. The same participant highlights the view that even though eThekwini Electricity has not experienced a cybersecurity incident, having an awareness of cybersecurity attacks affecting other businesses influences the cybersecurity culture of the Unit. The theme of peer institutions is discussed in greater detail in Section 4.7.1. The participant said:

"We may have not have experienced an attack or a risk. The risks are present, and they are increasing so the fact that you have attacks or potential attacks at other companies and organisations is an external influence, but I think it's mainly about awareness of it. Because if those companies are quiet or silent. We are not aware" (P2).

Another participant mentioned that the most significant driver of cybersecurity culture is awareness and knowledge of cybersecurity incidents. However, people only take it seriously when they are personally involved. The participant said that:

"I think the big thing to improve the culture is definitely more knowledge and awareness. You know people are unaware of it and the only time people are really now reading about it is in the news externally reading about Transnet, department of justice, every two weeks you're reading about someone who's being attacked, and I think only when you hear about your personal information being jeopardised, then you're going to take it seriously." (P8).

Therefore, people need to be constantly made aware of cybersecurity and how it can affect them personally, such that it is in the front of their minds. The same participant advises that training and awareness programs are needed to increase awareness and understanding of cybersecurity. This theme is discussed in Section 4.8.2 cybersecurity training. The participant said:

"So definitely knowledge more training courses. More awareness programs. Making people understand why you need to be more. Cyber-savvy because of the repercussions of these attacks and what people can do with it." (P8).

It is evident from the above extracts that cybersecurity awareness is a fundamental aspect of developing a cybersecurity culture. Therefore, the following section discusses the theme of cybersecurity culture and the various sub-themes that underpin it.

4.6 Cybersecurity culture

The organisation's cybersecurity culture is an outcome of several constructs that each contribute to keeping the organisation secure against cybersecurity attacks aimed at exploiting weaknesses in people. This theme describes the participant's views on the current state of cybersecurity culture within the organisation. The word cloud in Figure 4.3 illustrates the participant's views collated under the theme cybersecurity culture. The word cloud illustrates words that were frequently said by the participants. For example, the words people, understand, business, managers and security were frequently mentioned for the theme of cybersecurity culture.

Figure 4.3: Word cloud - cybersecurity culture.

Participants shared a common view that there was no organisational cybersecurity culture present. However, due to different levels of awareness, certain groups of employees displayed aspects of the desired cybersecurity culture. Participants also viewed that the organisation is at the initial stages of developing an organisational cybersecurity culture, and efforts are being made to improve the level of employees awareness and knowledge.

Several participants shared the common view that the current state of organisational cybersecurity culture is varied and in the early stages of development. One participant said:

"It's varied, uhm, quite a lot, because there's different types of employees within the Unit working at different levels." (P1).

Another participant describes the cybersecurity culture as immature, and the organisation is still at the early stages of developing such a culture.

"I think it would be immature, but its the area where our stages are at the early stages of developing an organisational cybersecurity culture." (P2).

Therefore, it is evident that the organisation's cybersecurity culture is not sufficiently developed to defend against cyber threats. Another participant provides a reason for the low maturity level of the organisational cybersecurity culture. The participant said the lack of focus on developing such a culture stems from the absence of declaring such in the organisation's values.

"So, cybersecurity, culture and organisation. Uh, it's something that does not cut across the organisation. The reality is that it's left up to a few individuals. There's no emphasis on cybersecurity as a culture in the organisation. It does not even appear in our values in the organisation" (P6).

The above extract highlights the fundamental challenge in developing a cybersecurity culture. The theme of cybersecurity challenges is discussed in greater detail in Section 4.4. Another participant felt strongly that the organisational cybersecurity culture was non-existent in the Unit due to the lack of action to foster a culture of cybersecurity. The participant had not observed any concerted effort towards developing an organisational cybersecurity culture.

"I would put it at zero currently. In, my opinion there is nothing currently being done to either encourage it, to think about it or to do anything against it, to have a mitigation plan or policy. It's currently non-existent in my opinion." (P8).

Having a concerted effort towards creating awareness combined with the cybersecurity policies and management plans was viewed as the necessary mechanisms to develop the cybersecurity culture. One participant highlighted the lack of management awareness and holistic cybersecurity policy as the reason for the current low cybersecurity maturity level.

"So, I think we still far away. I think the real reason is I don't think there's an awareness around cybersecurity management or cybersecurity policy or management plan. That's definitely what's currently shaping our low maturity in terms of cybersecurity" (P4).

Therefore, the cybersecurity culture at the organisational level is viewed as inadequate. Interestingly, participants shared a view that there has been a concerted effort made within their respective branches towards increasing the level of cybersecurity awareness and knowledge of employees.

"There has been a lot done though in terms of peoples understanding. I think from where I am. Of what security is and making sure people understand this, especially those working on the critical network where we are. But yeah, I think a lot more needs to be done." (P7).

Another participant supports the view of activities being undertaken to improve the cybersecurity culture.

"There is a growth that we are forecasting, which is therefore promoted by the cybersecurity awareness trainings that we provide for the organisation, there is a lot of visibility now where it's a lot of posters and we send weekly information on security attacks." (P9).

The findings indicate that the cybersecurity culture in the organisation is varied and immature, with many participants viewing that even though a few initiatives are being undertaken, a lot more needs to be done to develop and improve the organisational cybersecurity culture. The following subsections discuss the various sub-themes that underpin the organisational cybersecurity culture.

4.6.1 Leadership role

Participants expressed strong views on the role of leadership in cultivating a cybersecurity culture within the Unit. Participants indicated that leadership plays a critical role and needs to drive the development of a cybersecurity culture through leading by example, providing and directing organisational resources towards cybersecurity, and constantly reinforcing the desired behaviours to shape the cybersecurity culture. Participants also expressed the importance of leadership to communicate the right signals to influence employees' behaviour.

In discussing the leadership role in establishing an organisational cybersecurity culture, one participant mentioned that the accountability of leadership establishes their importance in defining the culture. The participant said:

"I think the role of leadership essentially is to direct the organisation towards establishing this culture. Because in my view leadership is always accountable for activities within the organisation to a great extent" (P2).

Participants expressed that leadership is vital in establishing a cybersecurity culture through the top-down influence of leaders. Participants expressed a strong view that to create an effective cybersecurity culture, it needs to be driven using a top-down approach where the leader's actions will influence employees. One participant said:

"I think it's very important. It will bring about the change that will come through from a top-down approach. So where maybe the management would lead by example and then obviously the employees will follow suit." (P1).

Another participant supported this view and added the importance of leaders in setting the direction of the organisation. The participant said:

"Yeah, I think it's very important. Especially because well, whether it's cybersecurity or anything. When its driven top down. It gets implemented much better, quicker, faster. So, if there's no sense of direction from the top pushing this topic. It's not going to happen, so I view leadership as a very important role." (P8).

A dominant view that the participants expressed was that leaders should lead by example.

"Leading by example, and so the first thing that we got to do as leaders is to demonstrate ethics, to demonstrate professionalism, to say the right things when it comes to cybersecurity issues, to do the right things." (P3).

This statement highlights that leaders should be aware of their influence over shaping employees' behaviours. Therefore, when leaders say and do things to support cybersecurity, they influence the culture of cybersecurity. Another participant added the view that management has the ability to shape the cybersecurity culture through the direction of organisational resources to prioritise cybersecurity. The participant said:

"Management has the biggest role to play because management is in charge of defining and shaping the organisation culture, management has the budget in order to essentially create that. They have the budget to create the awareness campaigns to deliver on cybersecurity training." (P4).

Reinforcing through communication was another key area highlighted in leadership's role in cultivating a cybersecurity culture. Participants viewed reinforcing the desired behaviours by leaders as a vital process in establishing a culture. One participant mentioned that:

"Leadership needs to keep on reinforcing it. Reinforcing what needs to happen on a very frequent basis, where over time it then becomes the established norm." (P3).

The same participant stressed the importance of communication and influence of leaders by saying:

"It's the communication which is vital. But repeat communication and the right signals that we need to send out is how we can cultivate the right cybersecurity culture." (P3).

Another participant provided an example of how reinforcing and top-down drive from leadership influences employees to emulate what they see. The participant said:

"If you are not constantly remined and driven about this topic, it will fall by the wayside, it wouldn't even become something important. I think that's why it's important, especially when it's driven top down. People look up to it and say, OK, yes, it's important that this person I can see they're doing it they're following it, so I should do the same." (P8).

The above findings indicate that leadership plays a vital role in shaping the organisation's cybersecurity culture through taking the lead, directing resources, leading by example, and reinforcing the desired cybersecurity behaviours. However, one participant stressed that firstly leaders need to understand cybersecurity as a key risk to the business and how it can affect the organisation. Only then will there be a sense of urgency to cultivate a cybersecurity culture. The participant said:

"Only until it's driven from the top and that's given a level of urgency and they understand it as a key risk factor for the continuous operation of our business. Then only would the culture improve." (P4).

In order to have this understanding, leaders need to have knowledge about cybersecurity and how it can impact the organisation.

4.6.2 Leadership knowledge

Leadership knowledge of cybersecurity threats and vulnerabilities facing the organisation was highlighted as an essential aspect of shaping the organisation's cybersecurity culture. Participants viewed leaders who possess cybersecurity knowledge as more likely to undertake activities that can secure the organisation, therefore shaping the cybersecurity culture. Participants reported on their level of cybersecurity knowledge, skills, and competencies and provided insight into the impact of leaders who were knowledgeable of cybersecurity. Lastly, participants expressed their views on how the organisation can increase cybersecurity knowledge across the spectrum of leadership.

In terms of gauging the participant's level of cybersecurity knowledge, skills and competencies, it was evident that participants from the senior management and senior technical bands had undergone some level of cybersecurity training as part of their job functions. Therefore, they were, to some extent, knowledgeable about cybersecurity and the vulnerabilities of the organisation. Participants said:

"I would say that I have a general understanding of the of the architecture that the organisation utilises and the possible threat or touchpoints where we could be vulnerable." (P1).

"In terms of training. I have attended a module on information management, and I think a lot of the training with regards to communication technology covered a small cybersecurity element." (P2).

"So, I think I've got some knowledge at a high level or understanding of what cybersecurity risks are present and may impact our organisation." (P2).

"I have been on certified ethical hacking, on a certified information security professional training. I've been on the FortiGate training on those there's different levels." (P4).

The above excerpts indicate that these participants at the senior management and senior technical bands are knowledgeable about cybersecurity. However, the participants interviewed at an executive management level indicated that they do not possess cybersecurity knowledge, skills, and competencies, mainly because of their backgrounds as electrical engineers. One participant said:

"No, unfortunately, as an electrical engineer, you don't get involved in cybersecurity training or projects" (P3).

Another participant supported this view by saying:

"In terms of my own personal competence on it. I know very little about cybersecurity and maybe the error we making as an organisation is that we largely leaving it like default to the ICT staff." (P6).

However, notwithstanding their lack of cybersecurity knowledge, one participant highlighted that the most important aspect is for leaders to understand the implications of cybersecurity risks.

"You know, obviously skills wise, I don't have the skills. I don't have the competencies. I don't have even the knowledge. But I understand the overall gravity of the threats and what could be the possible impacts." (P3).

This statement is significant as all leaders do not need cybersecurity knowledge, skills or competencies, but they need to appreciate the consequences of cybersecurity risks facing the organisation. Moreover, participants expressed their views on the impact of leaders who are knowledgeable about cybersecurity as:

"The impact would be better decision making perhaps. Or maybe, a better reprioritisation or dedication of resources given the level of risk to the business." (P1).

Another participant supported this view and added that knowledgeable leaders would keep influencing aspects of the business to be more cyber-secure. The participant said:

"If they had adequate knowledge on cybersecurity, maybe when they are signing off on specifications. These people at an influential level. I'm talking chief engineer, senior manager level would then start questioning every time, is there a cybersecurity element here that we should be addressing as part of the specification." (P6).

Participants felt that only a few leaders had some cybersecurity knowledge. One participant mentioned:

"Like senior management. You know that we have in this organisation like a handful of them that actually understand, you know, like the implications or even understands cybersecurity." (P10).

Another participant added that the lack of resources focused on mitigating cybersecurity risks across the organisation shows that many leaders do not understand the risks. The participant said:

"I feel that just my personal view is that if the risk were truly understood. The organisation itself would have had a lot more resources directed towards the mitigation of cybersecurity risks." (P2).

Participants also offered their views on how the organisation should improve the level of cybersecurity knowledge of leaders. One participant said:

"As a leader, I don't even think many leaders understand what cybersecurity means. So, I think the starting point will be firstly to educate the leadership on the term. What cybersecurity is, what the risk is to the business, and then use the leaders to then influence cybersecurity down the line." (P6).

Leaders that have an understanding of cybersecurity can positively influence the culture. For example, the same participant then said:

"In terms of influencing subordinates, they can only do that if they know enough themselves." (P6).

This view was shared by other participants as well.

"They themselves need to understand what is cybersecurity before they can help others." (P8).

"If you don't have managers themselves knowing about what cybersecurity is, a definition of it, how do you instil culture to others when you yourself don't know" (P7).

Therefore, the participants highlighted the importance of leaders having fundamental knowledge about cybersecurity and its impact on the organisation. One participant discussed how the organisation prioritised and enforced mandatory coaching and mentoring training for all employees at senior positions. The participant said:

"Coaching and mentoring. If that sort of mindset were employed in terms of cybersecurity. All managers would understand and be trained in cybersecurity aggressively." (P7).

The participant suggested that the organisation should take the same approach and enforce mandatory cybersecurity training for all employees at a leadership level.

4.6.3 Leadership participation

Leadership participation in cybersecurity initiatives signals the importance of the activities to subordinates who are influenced to participate. Participants discussed how they were personally involved in cybersecurity activities such as policies, projects and training.

Participants at the senior management and senior technical level within the organisation indicated that they were involved in various cybersecurity initiatives within their respective branches. One participant said:

"I've been involved with projects that are explicit to the branch whereby we put together a branch level strategy and a few projects to be able to mitigate some of the risks that are known to us." (P2).

Other participants at this level also indicated their involvement by saying:

"I have been involved in a few projects when we delivered the digitalisation project on the MV side, we defined the VPN strategy for remote connections." (P4).

"I have been involved with a few I wouldn't call them projects, but a few initiatives." (P8).

"I have been personally involved on the safer cities strategy formulation and as well in terms of the choices of awareness, that need to go out to our users in terms of training." (P9).

These participants highlight their involvement in developing branch level strategies and initiatives to mitigate risks to assets under their control. Another participant mentioned the implementation of an E-learning program to train employees. However, due to the lack of upper management support, the project was not as successful as it could have been.

"Over the past year or so I've personally implemented an E-learning program, which I would say it wasn't as successful as I would want it to be. Mainly because it was only driven from where I am not from the whole unit. From the business there was very minimal support for that." (P5).

The above views highlight that leaders at the senior management and senior technical level actively participate in cybersecurity activities and shape the cybersecurity culture, albeit at a branch level. Participants at the executive management level mentioned that they have minimal involvement in cybersecurity activities, mainly due to cybersecurity being out of their domain as electrical engineers. One participant mentioned that:

"The only the only involvement I had in cybersecurity was undertaking periodic penetration tests into our network and I think it was because it's a legislative or an audit requirement for it to take place. Beyond that, I cannot say we done anything further." (P6).

This view indicates the limited involvement of executive leadership in cybersecurity. Moreover, this also indicates that leaders at this level participate when it is a legislative or audit requirement. This theme is discussed further in Section 4.6.5 leadership accountability and Section 4.7.2 external rules and regulations.

4.6.4 Leadership priority

Leaders make cybersecurity a priority for the organisation by setting the strategic direction and allocating resources towards the achievement of projects to secure the organisation. Participants shared ways in which they have or have not made cybersecurity a priority for the organisation. One participant mentioned that at a branch level, they felt that addressing cybersecurity was essential and, therefore, it was considered highly amongst other projects. The participant said:

"I did motivate for the cybersecurity strategy to be prioritised to be part of the priority projects that will be implemented." (P1).

However, the participant then went on to say that cybersecurity initiatives were easily reprioritised because the cybersecurity risks have yet to be quantified or realised by the business.

"Because we haven't really quantified the level of attacks that we have and the risk their off. It is always easier to reprioritise cybersecurity and it goes lower down the list because of that." (P1).

In discussing the prioritisation of cybersecurity projects over other business commitments, one participant responded to a comment from the researcher on the low priority of cybersecurity within the organisation. The researcher mentioned that a reason might be that cybersecurity risks have not been realised. A participant at the executive management level highlighted that cybersecurity had not been prioritised amongst the duties issued to employees.

"Yeah, you're right. We haven't really made it a priority. It was like, hey, you've got say 20 duties to do, and one of the things is to look at this. So, this is what you need to do amongst your branch, and we leave it. At my level, I must admit I haven't said it's a priority." (P3).

However, another participant at a senior management level demonstrated creative ways to make cybersecurity a priority within a resource-constrained municipal environment. The participant indicated that by combining smart city initiatives with safer cities initiatives, they could channel resources towards cybersecurity for the Unit. The participant mentions:

"But we have made it a priority to an extent that we, being a budget constrained municipality, we have listed it as part of the smart city initiative that a smart city needs to be a safe city, so we collaborated the two into saying every city is growing into being smart. We then need to adopt safe. So, we have prioritized in terms of budgeting in terms of project priorities. Prioritize any

project that has to do with cybersecurity because that will protect our infrastructure and protect business continuity." (P9).

This statement indicates that cybersecurity is given priority at the lower levels of management. However, more needs to be done to drive it from the top within the Unit.

4.6.5 Leadership accountability

Participants expressed strong views that management needed to accept responsibility and accountability for cybersecurity. For example, one participant highlighted that cybersecurity risks could impact service delivery; therefore, management needed to accept accountability to address such risks.

"The management team should take the lead primarily because we are accountable to ensure service delivery. So, you would need to be able to identify any risks with cybersecurity or any other risks that are preventing us from delivering electricity." (P2).

Another participant highlighted that initiatives are tracked to completion when leaders are accountable. For example, the participant mentions that audit findings were tracked on the municipal risk register, and the Unit head was accountable for addressing them.

"One good thing that came out of those audits also. Was the fact that the findings were sent to executive. It was sent to the director and the head of electricity, so he had to have sign off and to my understanding it was put on the top 100 risks on the risk register for the municipality." (P4).

Another participant advocates for making management accountable for cybersecurity. The participant said that this shows that leaders are committed to cybersecurity and are not making it someone else's problem.

"Making managers accountable or the leadership accountable. I think here they will obviously be more inclined to ensure that staff is trained and accept responsibility that cybersecurity doesn't really become somebody else's problem but there's as well." (P7).

In drawing a contrast between safety culture, discussed in Section 4.9, which has accountability at the highest levels in the organisation, and cybersecurity culture, one participant, highlighted that the lack of mandatory appointments for cybersecurity posed a challenge in using accountability to drive a cybersecurity culture. The participant said:

"There are no mandatory requirements to appoint, say a cybersecurity officer, cybersecurity specialist etc. It doesn't work, and so we can't actually use the appointments that will impact in terms of accountability in the cybersecurity space." (P3).

The lack of mandatory requirements for cybersecurity poses a challenge for taking a top-down approach to developing a cybersecurity culture. Section 4.7.2 on external rules and regulations details the participant's views on the current regulatory environment and how it may change to enforce leadership accountability.

4.6.6 Employee general threat awareness

Employees that have knowledge and understanding of cybersecurity threats are more aware of potential cybersecurity issues. Participants provided insight into developing employees cybersecurity threat awareness. Participants mentioned that employees would only understand the impact of cybersecurity attacks if they were affected personally. Participants said that this is an essential aspect of building a cybersecurity culture.

One participant said that employees should be made aware of cybersecurity threats by communicating how cybersecurity incidents can affect them personally. If people understood their connection to cybersecurity attacks, they would be more aware of the risks. The participant said:

"If maybe people understand the level of impact on a personal basis, that a cybersecurity event will have on them. Uhm, and for instance, if identity theft results in you losing money from your bank account, then you understand then why then you should pay attention to certain aspects of things." (P1).

Another participant supported this view and provided another example of how leaders can communicate how a cybersecurity attack on the organisation can affect employees personally. Creating a personal connection between cybersecurity incidents emphasises the importance of behaving in ways that will keep the organisation and themselves safe. The participant mentioned:

"If there's something that absolutely we should be saying is, it could affect the HR systems that pay your salaries, overtime whatever it might be, and if we don't address these attacks. It could block me from paying your salary. You know, and that should be something that we should be looking at. You know, and communicating that." (P3).

The view of communicating how cybersecurity incidents can affect employees was common to the participants. However, another participant highlighted that the organisation had not taken this approach to connect cybersecurity attacks against the organisation and the impact on employees. As a result, at present, employees do not view cybersecurity as their problem. The participant said:

"I think people the sooner people start realising that they're aligned organisation to pay their salaries. So that when an attack, for example on our revenue management system on smart meters, that prevents us from collecting income and that prevention in collecting income is going

to have an impact on us paying salaries. Then maybe they will draw a connection to cybersecurity. Right now, it's the organisation's problem. It's not my problem." (P6).

Creating awareness amongst employees is essential for them to understand the risks associated with the cyber domain. Several participants expressed the view that employees are assets to the organisation. Therefore, they should be made aware of cybersecurity risks to secure them in their personal lives as well. One participant said:

"I think the big thing here is awareness and education. The bulk of our users are not IT experts or, even security experts. So, you'd need to educate all of the employees a whole lot better and make them aware of how they could secure themselves and how to improve their own personal security. Obviously if people are aware of it then they would be less prone to those attacks." (P8).

Another participant added:

"We not just wanting to empower people or employees so they can protect the Units assets but they themselves they are assets." (P5).

This is an important observation because once employees understand that the organisation supports them in protecting their personal interests, they are more likely to secure the organisation from cybersecurity attacks. One participant mentioned:

"You know, the more we educate them on how to protect themselves. We start to build that culture of hey, I need to protect myself. I need to protect these systems and therefore yeah if I'm working in a company, I also need to adopt the same. It has to be flowing back into the corporate world." (P3).

At present, the organisation has embarked on a drive to create awareness of cybersecurity. One participant mentioned that the ICT branch has been communicating the concept of cybersecurity to all employees. One participant said:

"The ICT branch has started an emailing communication campaign to inform users with regards to the risks or the concept of cybersecurity. So, this initiative is whereby you'll find periodic emails forwarded across to all users within the organisation to create awareness around the concept of cybersecurity and some of the potential risks and hazards related to it." (P2).

However, another participant highlighted that the organisation had not done enough to embed cybersecurity in the minds of all employees. The participant said:

"The issue about cybersecurity residing in people's minds that they need to now protect and defend organisation against cybersecurity attacks. I don't think we've done enough." (P6).

Therefore, employees need greater awareness of cybersecurity threats to secure them in their personal lives and when they come onto the organisation.

4.6.7 Employee cybersecurity policy awareness

Employees that are aware of and understand cybersecurity policies display the required behaviours to secure the organisation. Participants mentioned that employees are currently made aware of cybersecurity policies via emails. However, one participant highlighted that this is inadequate for employees to understand the information contained in the policy and what is actually required of them. The participant said:

"The policies are being updated and cascaded by mail, cybersecurity policies and ICT policies. That is being done. But I think, coming back to earlier point. I think a lot more needs to be done. If you are sending an mail, people open the mail and delete the mail. They don't understand that." (P7).

Another participant added that the organisation needs to be more proactive in creating awareness and understanding of cybersecurity policies. The participant said:

"I think it needs to be more proactive, whereby staff need to be reminded. That level of awareness needs to be improved holistically through more than just information broadcast, but really through other methods whereby staff can really digest the information and in order to digest that information you need to see how it really effects you in your current everyday practices." (P4).

The participant highlights that the organisation needs to explore alternative methods of creating awareness and reinforcing policies, thereby creating an understanding of cybersecurity policy and the personal connection to cybersecurity required to secure the organisation.

4.6.8 Employee motivation

Participants expressed their views on various topics that would motivate employees to protect and defend the organisation against cybersecurity attacks. Participants viewed employee general cybersecurity threat awareness, discussed in Section 4.6.6, as a motivating factor. Participants said employees are motivated by incidents that disrupt their personal lives. One participant said:

"Disruption from your own life in a way that you wouldn't be able to do your work. You wouldn't be able to generate sort of value to the organisation because you are prevented by a cybersecurity incident." (P1).

Another participant viewed that employees are motivated when they feel valued in their contribution to the organisation. Therefore, they are more likely to protect and defend the organisation. One participant said:

"I think when an employee feels he's very valued it plays a significant role that whatever he does in the organisation is valued. I think he would be much more motivated to go out and defend organisation against such attacks, so he'll take on many more precautions so he would ensure that he complies with the organisational guidelines towards cybersecurity." (P4).

Another participant highlighted that cybersecurity training, discussed in Section 4.8.2, motivates and creates a culture within employees when they are aware of cybersecurity risks. The participant said:

"The way to leverage off that is firstly just train or inform people that they can be affected by cybersecurity event and how would that be severe. Which will then increase that motivation to change certain cultures or behaviours and prevent attacks." (P1).

A unique aspect of eThekwini Electricity employees is that they are also forced to be a customer of the organisation. One participant highlighted this fact by saying:

"I said the unique thing about you is that you are not just an employee, but you are forced to be the customer of this organisation. So, if you're forced to be the customer of this organisation, it means that whatever you do in your job to reduce costs or improve the service delivery. You are going to benefit yourself." (P3).

The participant further added that this fact should be communicated to all employees so that they understand that cybersecurity attacks on the organisation can impact their personal lives.

"I mean it is the fact that when you are a customer as well, you know if you do not manage cybersecurity well and you're going to have breaches and attacks that get through and shut down the network, where we can't collect our revenue, we can't control the system remotely. So, we have mel-operations, whatever. We are the ones that are going to suffer." (P3).

Creating this personal connection with cybersecurity can significantly motivate employees to protect the organisation. Performance evaluation and rewards and punishments detailed in Section 4.8.7 and Section 4.8.11, respectively, were also cited as significant motivating factors that can shape the cybersecurity culture. One participant said that:

"In short, performance evaluation is an influencer with regards to employee behaviour. In essence, if individuals are seen to be rewarded for becoming more cybersecurity aware, they're more likely to become aware. So, in short, I feel there is a role for HR performance measurement and linking it to establish cybersecurity culture for the organisation." (P2).

Another participant highlighted the role of leadership in motivating employees through their participation in and prioritisation of cybersecurity activities. These themes are detailed in Section

4.6.3 and Section 4.6.4, respectively. The participant said that unless there is a drive from management, employees will not take cybersecurity seriously.

"I think if employees feel that there's no real drive from management from the executive from national to really change the way we do things from a cybersecurity point of view, I think that definitely will influence employees in the way they react towards protecting and defending the organisation." (P4).

In discussing how cybersecurity attacks such as ransomware have affected other organisations, one participant mentioned that employees who are aware of these incidents could relate them to their organisation. This awareness consequently influences employees to be more cyber secure. This concept is discussed in greater detail under the theme peer institutions in Section 4.7.1. To illustrate this, the participant said:

"So, once it hits home and employees see that if we are attacked or we are affected by a similar ransomware attack, it really affects us individually, monetary wise it affects our work. It would mean it's not business as usual and I think its important." (P4).

Another participant highlighted that employees would be motivated to be more cyber secure when they are made accountable for cybersecurity. This theme is discussed in greater detail in Section 4.6.10. The participant mentioned that:

"I think the word accountability will come into play here probably the keyword. So, accountability, when employees are made accountable." (P7).

Participants viewed employee motivation to protect and defend the organisation as influenced by numerous factors. For example, general cybersecurity threat awareness and creating a personal connection to cybersecurity, cybersecurity training, external influences, performance appraisal, rewards and punishments, leadership participation, leadership prioritisation, employee accountability and responsibility were all viewed as significant motivating factors for employees.

4.6.9 Employee knowledge

Participants viewed employee cybersecurity knowledge as an essential aspect of shaping the cybersecurity culture in the organisation. A dominant view amongst the participants is that employees should have at least a basic level of knowledge and awareness to keep themselves and the organisation safe from cyber attacks. One participant said:

"I believe it starts with just having some basic knowledge and awareness." (P8).

The participant then highlighted how to create a basic understanding of how cybersecurity attacks may affect the organisation. The participant mentioned:

"Understanding the impact and your knowledge of what these attacks are. I suppose if you understand the impact that these attacks can have and the repercussions thereof after. It's the same as protecting your pin on your bank card. So, if you understand the importance of protecting your pin on your card, you will understand the importance of protecting your own organisation." (P8).

Another participant highlighted the links between knowledge and awareness, discussed in Section 4.6.6, and knowledge and training, discussed in Section 4.8.2. The participant mentions:

"Awareness will be key and crucial because once one is made to be aware of something then they have a different perspective with regard to it. So awareness brought about by training, awareness brought about by knowledge sharing in terms of other organs of state attacks. So that is what influences our employee's growth." (P9).

These three key dimensions of awareness, training and knowledge significantly contribute towards shaping employees' cybersecurity behaviours.

4.6.10 Employee accountability and responsibility

Participants felt that employees who are made accountable for cybersecurity, whether as part of their job function or as part of policy compliance, are more likely to display the correct cybersecurity behaviours required by the organisation. One participant mentioned that making employees accountable for their credentials is one way to instil a culture of cybersecurity. The participant said:

"Once you make them accountable. Do you understand that by giving you a PC for instance? Your password and your username is solely belong to you. You'd still find people that are sharing their password and username with others. We can't have that. I'm saying that a lot more needs to be done to instil that they are solely accountable for their credentials." (P7).

The participant further indicated that within their branch, they have made employees specifically accountable for cybersecurity. The participant said:

"I think our staff are more aware of that accountability. I do have names next to people changing out configurations on devices. That accountability is also key to make sure that if they are not configuring properly or making the device vulnerable, it does become an issue for training. Consequently, I think in terms of cybersecurity are key aspects." (P7).

Another participant highlighted that they had not created this level of awareness and accountability within their branch. Therefore, more needs to be done to extend this practice to other parts of the business and to all employees, not just those working on the technical systems. The participant mentioned:

"For example, someone configuring a modem out on site. If they understand that, If they misconfigured this device it could shut down the economy of Durban. I don't think that level of awareness has been created at this point." (P4).

This example highlights the impact to the organisation if cybersecurity is not considered in the business practices and processes. This theme is discussed in Section 4.8.1. Moreover, the example further highlights the importance of using employee accountability to shape the desired cybersecurity behaviours.

4.6.11 Employee commitment

Participants viewed that if employees are committed to the organisation, they are more likely to behave in ways that will keep the organisation safe from cybersecurity attacks. Participants viewed employee motivation, discussed in Section 4.6.8 and employee general threat awareness, as discussed in Section 4.6.6, as key aspects determining employee commitment. One participant highlights how these concepts combine to influence employee behaviour such that they are committed to protecting the organisation. The participant said:

"I think that once at that level of awareness is created, it will really influence behaviour and it's not just behaviour that they have to do the work because it's part of their work schedule, but it's more like from an ethical point of view whereby they feel it's the right thing to do rather than they doing it just because it's part of their work schedule." (P4).

Achieving this level of commitment is vital to establishing a culture of cybersecurity because if employees feel that it is the right thing to do, they will naturally behave in ways to secure the organisation.

4.6.12 Trust

Participants at the executive management level expressed the view that there is a high level of trust placed in employees who manage the organisation's critical systems. The participants viewed professional bodies, discussed in Section 4.7.4, as an external influence that motivates these employees to behave professionally, ethically, and undertake activities that will not compromise the organisation's cybersecurity posture. One participant said:

"Maybe a bit irresponsible of us. But we got a high degree of trust for employees that are implementing these systems. So, I'm talking about our engineers, our technicians, and technologists that implement distribution automation for example." (P6).

The participant then elaborates on the reason for placing a high level of trust in these employees by mentioning:

"This is largely because the people that are dealing with these various projects that are in the 4 IR arena, are professionals in terms of registration with the engineering council of South Africa. We tend to put a lot of weight on the fact that they are registered professionals that are bound by the ECSA code of conduct. So, based on that, we by default assumed that they act ethically and morally at all times and will not compromise cybersecurity, by the nature of the fact that they are registered as professionals." (P6).

This view was also shared by another participant at the executive management level who said that these employees display the required level of professionalism in keeping the systems secure. The participant said:

"But I guess the kind of good news to an extent is those key staff that have access to the system. I think they themselves, generally speaking, display the required professionalism we expect out of them." (P3).

Participants from the executive management level view professional registration as an important aspect of establishing trust in employees who work on the organisation's critical systems.

4.6.13 Interdepartmental collaboration

To effectively secure the organisation against cybersecurity threats requires collaboration between the various departments and branches on cybersecurity matters. Participants described the various formal and informal cybersecurity teams and groups and provided insight into why collaboration between the various branches posed a challenge for the organisation.

One participant discussed cybersecurity collaboration at the organisational level, where the various branches got together to address cybersecurity in the Operational Technology (OT) domain. The participant mentioned that a committee to address this challenge exists but is no longer active, alluding to changes in business strategy impacting the functioning of this committee.

"Within the business Unit where there was an ICT Technical Committee that was established to discuss cybersecurity risks within the OT domain, but the committee is essentially frozen at this point in time, so it is a committee, but the committee has not met or action any items, probably in the last two or three years which may or may not be related to the COVID pandemic or changes in our organisational strategy." (P2).

Another participant highlighted that interdepartmental collaborations are informal and lack a concerted effort towards delivering organisational objectives. The participant said:

"There is interdepartmental collaboration on matters of security. Do they follow a specific strategy, and do they meet regularly, and do they fulfil the business missions? I would say no,

because it's incoherent and inconsistent and they are not working towards a common vision." (P4).

However, the same participant saw value in the informal collaborations between branches as there was a benefit from spillover activities that helped the SCADA branch with audit compliance.

"The informal collaboration has assisted in that some of the functions that have been taking place over the last few years within the IT department has now spilled over onto the SCADA systems. So whenever the auditor comes in and does compliance checks and so forth. We get the collaboration with IT which really helps in assisting the OT branch with those investigations and so forth." (P4).

At the branch level, participants mentioned that each branch had taken its own approach towards addressing cybersecurity by forming branch level project teams and groups. One participant said:

"Within the communication network branch. Where a formal project has been launched with respect to cybersecurity. There's a team within the branch as a little project team to look at cybersecurity." (P2).

"There is also a team within the High Voltage Network Control branch which has also been working on cybersecurity challenges at the application level." (P2).

The exitance of independent branch level cybersecurity groups indicates a lack of top-down focus or drive for organisational cybersecurity. One participant mentioned that there would have been a formal and concerted collaboration between the various branches if cybersecurity was a high-level organisational requirement. The participant said:

"So, in essence if that was a high-level organisational requirement, then we could have restructured the committees to have a more formal interaction." (P2).

One participant at the executive management level took note of the level of collaboration between the operational technology branches and highlighted that collaboration can be reinforced between them. The participant said:

"I notice maybe not a concerted effort amongst the three core, communications and operations functions of the Unit. I think there may be some element of collaboration that can be strengthened between those groups." (P3).

This observation by executive management is important as top-down direction and support is required to strengthen formal collaboration between the branches. One participant mentioned:

"I think because the fact that there's no line of sight and because there's no top-down objectives being driven down from executive, it will continue to remain informal." (P4).

The participant then mentioned that the organisation needs to have someone at the executive level that can drive and coordinate the cybersecurity activities across the organisation. However, for the business to do so, it first needs to appreciate the impact of cybersecurity.

"So perhaps once the business understands where they are currently and what the impact is of not implementing security, will they appoint someone to manage security for the organisation across, you know, the different branches and environments being IT and OT." (P4).

Participants view interdepartmental collaboration as a key aspect for holistically securing the organisation against cybersecurity threats. The following section discusses the theme of external influences on the organisation's cybersecurity culture.

4.7 External influences

The word cloud in Figure 4.4 illustrates the participant's views collated under the theme of external influences. The word cloud illustrates words that were frequently said by the participants. For example, the words culture, external, electricity, comply, and audits were frequently mentioned for the theme of external influences.

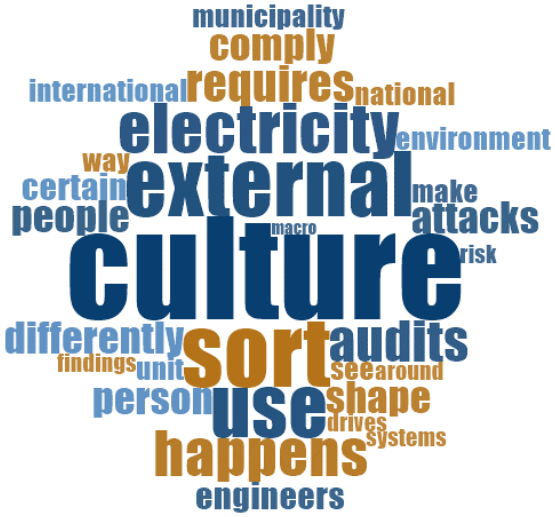


Figure 4.4: Word cloud - external influences.

Participants viewed the organisation's cybersecurity culture as having external influences from peer institutions such as other organs of state, external rules and regulations in the form of government acts and industry regulations, societal cybersecurity culture, and professional bodies. The following subsections discuss each of the external influences in detail.

4.7.1 Peer institutions

Participants felt strongly that the organisational cybersecurity culture of the Unit could be influenced by cybersecurity incidents that have affected comparable organisations. Participants shared this common view and indicated that the Unit had not experienced any cybersecurity attacks. However, these incidents indicate that the risk is real, is increasing, and could materialise at any time. One participant said:

"To show that while. We may have not have experienced an attack or a risk. The risks are present and they are increasing so the fact that you have attacks or potential attacks at other companies and organisations is an external influence." (P2).

Another participant added that:

"I think when you listen in to what happened at the Port recently, you know, and it's the more incidents you hear out there, the more it should make those that are responsible wake up and see what they need to do differently." (P3).

However, another participant mentioned that there had not been a drive from the government to highlight or communicate cybersecurity incidents to other organs of state to prepare themselves better. The participant highlighted that the lack of drive from the government shapes the poor culture of cybersecurity. The participant said:

"There was no real consolidated effort that was put into place to deal with that from a government point of view. That lack of consolidated approach really drives that culture or the poor culture that exists because there's no urgency that's coming from higher up, which means that higher up is not seeing it as a key risk indicator." (P4).

Key customers of eThekwini Electricity are also viewed as having an external influence on the organisation's cybersecurity culture through the type of cybersecurity requirements imposed by these customers. One participant mentions:

"Key industries like Engen, SAPREF, Mondi and so forth, their cybersecurity strategies inevitably have an impact on how we deliver services to them. If they have a specific approach towards cybersecurity, that would definitely influence how we look at cybersecurity internally in order to support that solution." (P4).

Participants also viewed service providers who have a very strong cybersecurity posture as a significant external influence. One participant also suggested the Unit partake in cybersecurity information sharing sessions with other organs of state such that the collaborations are mutually beneficial. The participant said:

"We need to be able to have engagements with not just only internal stakeholders, but maybe have sister municipality information sharing sessions where we discuss these things." (P9).

4.7.2 External rules and regulations

External rules and regulations imposed by the government and regulatory bodies define the legal environment in which the organisation operates. Participants expressed their views on several sources of external influence. For example, one participant mentioned that if there were any statutory requirements for cybersecurity in the electric utility environment, those would have influenced the actions taken by the Unit. The participant said:

"If this in fact is a critical risk through the country or region, ideally we would have seen some sort of national standard being established. Because what you will find is statutory Acts is a simple way to create direction or drive towards initiatives. If there was some sort of Act or even standards directed to us towards cybersecurity that may influence some of the action that we may take." (P2).

Another participant added that the lack of mandatory requirements meant that the organisation was not forced, and therefore does not have anyone representing cybersecurity at the executive level. The participant said:

"There are no mandatory requirements to appoint, say a cybersecurity officer, cybersecurity specialist etc. It doesn't work, and so we can't actually use the appointments that will impact in terms of accountability in the cybersecurity space." (P3).

Another participant highlighted that when the South African energy regulator adopts international standards that define requirements for power assurance, there will be a top-down drive to make cybersecurity a priority. Until then, there will be no real emphasis on accountability. The participant said:

"Only once we have that push from national or some sort of regulatory framework, then will we see a driver at the executive level for someone with the education and more awareness around cybersecurity being part of their decision making." (P4).

The participant also mentioned that there is a critical infrastructure cybersecurity plan being proposed at the national level; however, it has not been approved and hence has not affected the Unit's culture. The participant said:

"The regulation hasn't been really promulgated to a point whereby we are being monitored and we need to comply. So that really hasn't affected our culture." (P4).

Participants also mentioned that acts such as the POPI Act shape how things are done and serve as drivers for a more focused cybersecurity effort within the organisation. External audits by the auditor general were also viewed as necessary in shaping the culture. One participant said:

"Those audits really helped define the culture within the branch because it really creates that definition of what needs to be done within the branch. And, because you're going to be audited the year after and monitor the progress on what has been audited previously or the findings. I think that also sets the culture within the branch." (P4).

4.7.3 Societal cybersecurity culture

Participants indicated that employees are influenced by the cybersecurity culture they experience in their social lives. For example, one participant said that the cybersecurity awareness and culture of the people in the eThekwini region influences the cybersecurity culture that employees bring into the organisation. The participant said:

"I think when it comes to external influences, I think the major one would have been awareness in, call it, citizens or customers or consumers within the region of eThekwini at large around the area of cybersecurity. So, I think if the region of eThekwini was more aware of cybersecurity challenges or the adoption of technology and the risks, it would automatically filter into the organisation." (P2).

Other participants supported this view and added that societal cybersecurity culture should be shaped from the schooling level. One participant said:

"If you think about cybersecurity, it's not necessarily cybersecurity only at the workplace. It's it really starts from the time a person gets in at the schooling level. Are there sufficient training courses at the school level, at the university level that are really shaping the attitudes and behaviours of people around cybersecurity and obviously that spills over." (P4).

4.7.4 Professional bodies

Participants at the executive management level had strong views on how professionally registered employees are influenced to act ethically and professionally in line with desired cybersecurity behaviours to keep the organisation safe. One participant provides an example of how professionally registered employees are motivated to act ethically and not intentionally jeopardise the organisation's systems. The participant said:

"ECSA requires you to follow a code of ethics. So, if you're meant to occupy this post you got to be a professional. Right, and then, if you do something wrong, let's say you were caught involved in a cybersecurity attack on our own systems. Right, we are then bound to report you to ECSA and they will strip you of your PR. And when they strip you of your PR because you were involved

in illegal unethical things in your company. How are you going to find a job elsewhere using your PR? Who's going to employ you easily when you when you get stripped off your PR? So that also plays and, should play and influence." (P3).

This example illustrates the significant influence of professional bodies on employees' cybersecurity behaviour. The following section discusses the theme of organisational mechanisms that leaders can use to shape the organisational culture.

4.8 Organisational Mechanisms

Leaders use organisational mechanisms to shape the organisational culture. The word cloud in Figure 4.5 illustrates the participant's views collated under the theme organisational mechanisms. The word cloud illustrates words that were frequently said by the participants. For example, the words people, policies, managers, security and training were frequently mentioned for the theme of organisational mechanisms.

Figure 4.5: Word cloud - organisational mechanisms.

Participants indicated that leaders could use various organisational mechanisms to influence employee behaviour towards the desired cybersecurity culture. The following subsections discuss each of the subthemes that emerged.

4.8.1 Strategy, policy, procedures

Having an overarching cybersecurity business strategy that ties in the Units objectives with the initiatives undertaken at the Branch level was seen as a vital aspect for achieving a consolidated effort towards addressing cybersecurity risks and developing a culture of organisational cybersecurity.

As detailed in Section 4.6.13 interdepartmental collaboration, each Branch has developed and implemented its strategies or tactical plans to address cybersecurity. Attempts to form an

organisational cybersecurity strategy were made. However, participants indicated that it was problematic due to the lack of declared values and governance structures that prevented the development of a consolidated strategy for cybersecurity. Section 4.4 details these challenges. One participant said that addressing these challenges starts with the alignment between the core business functions and cybersecurity. Once that alignment is made in terms of an overarching cybersecurity strategy, the culture of achieving it will be directed by the branches' concerted operational and tactical plans. The participant said:

"I think the biggest thing that's needed is that alignment, that alignment between what is our business function and how can cybersecurity support that business function. So, I think once that that sort of gap is filled or that requirement is completed. I think there after everything will unfold." (P4).

The alignment and resulting organisational cybersecurity strategy will tie together all the organisational mechanisms discussed in Section 4.8, creating a uniform and directed approach to cybersecurity and developing a cybersecurity culture for the Unit.

Participants viewed the development and communication of cybersecurity policies, discussed in Section 4.8.3, as a vital aspect of communicating the desired behaviours and establishing a cybersecurity culture to protect employees and the organisation. One participant said:

"At the executive level you need to create the policies, the guidelines, the standards, the procedures that can be put into place that can ensure that humans are not exploited even when they're unaware of it." (P4).

In discussing how a culture of cybersecurity can be institutionalised through defined, repeatable processes, one participant viewed incorporating cybersecurity into standard operating procedures as a vital aspect to ensuring consistency, especially when all employees are trained against them. Cybersecurity training is discussed in Section 4.8.2. The participant said:

"The best thing would be to incorporate cybersecurity into the SOP or standard operational procedures. One for design, for specification, for installation and construction, for maintenance and so on. So, it would have to be incorporated within that." (P1).

4.8.2 Cybersecurity training

Participants viewed training as an essential aspect of developing and reinforcing cybersecurity knowledge within employees. Section 4.6.9 details the aspects of employee knowledge that are required. Participants mentioned the importance of scenario-based training for employees to understand the signs of cybersecurity attacks and to create a basic level of awareness. One participant said:

"Training and development of the people themselves to be able to understand the modus operandi of cybersecurity attacks, threats, and signs of attack. Similar to the physical world, how to identify suspicious behaviour." (P2).

Participants also indicated that training is required to improve the skill sets of those responsible for operating the organisation's systems and delivering cybersecurity functions. One participant suggested that the organisation upskill the existing municipal training academy to deliver cybersecurity training internally, similarly to other compulsory training courses such as ethics and anticorruption.

"The training Academy. We could set up some sort of training courses around cybersecurity to specifically train staff within the IT function and also these champions that exist within the different branches." (P4).

The participant also mentions the training of cybersecurity champions, discussed in Section 4.8.10. Participants view specialised training courses delivered through the work skills plans of employees as a significant contributor to shaping the culture of cybersecurity. One participant said:

"Putting cybersecurity as part of their workplace skills plan definitely will influence employees to really play a bigger role in protecting and defending the organisation against cybersecurity attacks." (P4).

A common view was that cybersecurity training should be done as part of induction when new employees join so that the cybersecurity culture can be inculcated from the start. One participant mentioned the importance of frequent and varied training to complement cybersecurity awareness training delivered during employee induction. Section 4.8.4 on recruitment discusses the initiatives undertaken. One participant said:

"I don't believe one training is enough it should be an ongoing thing it must be more for workflow as opposed to just give him one induction into ticker box that employee has done this, because the human mind forgets and then we become complacent in general." (P5).

Participants also drew parallels to the frequent health and safety training that all employees undertake. Moreover, one participant highlighted the positive impact cybersecurity training has had on employees as they can now understand and relate to aspects of keeping the organisation secure. One participant said:

"I have sent staff for training even electricians as well and the response when they got back was. Hey, I know what you guys are talking about. I can relate to when you say we need to be more

cyber secure or we can relate to certain aspects when we do talk about the network, so again, knowledge is key here." (P7).

This finding highlights the importance of cybersecurity training in creating an understanding of cybersecurity concepts, therefore, increasing cybersecurity awareness.

4.8.3 Communications channel

Communications channel refers to the methods managers use to convey information to employees. Participants described the current methods that are employed to disseminate cybersecurity information, such as policies to employees. Participants shared a common view that the cybersecurity policies were communicated via broadcast email. In addition, posters have been set up in shared spaces to create cybersecurity awareness on specific topics. Even though this creates some awareness, participants marked this as inadequate. Participants mentioned that employees need to be engaged with and communicated about incidents that occur at other organisations and how cybersecurity attacks can affect them personally. Section 4.6.8 on employee motivation details this theme. One participant mentions:

"I also saw posters that have been set up at the notice boards and so forth around cybersecurity threats. Again, whether that's a good way to digest information that's questionable, but there definitely has been some sort of effort to improve the cybersecurity culture over the last few years, and that's mainly stemming from the IT branch." (P4).

One participant mentioned using online platforms such as Microsoft Teams as a communication channel to create awareness, discuss cybersecurity issues, and specifically communicate to employees what's expected of them from a cybersecurity point of view. The participant said:

"Where the heads or the executive team picks on something and goes and presents the issues. Let's say in this case cybersecurity culture. It could be many things, but they take an opportunity to also add in there cybersecurity culture, not just overall culture but cybersecurity issues and what the executive expects off staff." (P3).

4.8.4 Recruitment

Participants viewed recruitment as a key method of introducing the requisite cybersecurity skills into the organisation. They also viewed the induction process as an important point to communicate the expected behaviours in terms of establishing and integrating new employees into the organisation's cybersecurity culture.

Participants stressed that the organisation needed skilled resources to deal with the cybersecurity challenges because the cybersecurity function is so critical that it cannot be outsourced entirely. One participant said:

"The entire cybersecurity kind of philosophies and approaches methodology has to be developed in house using the required engineering resources. So, as long as we can get the right technical skills in place. We can try and then implement better quality solutions to address cybersecurity and all our other issues." (P3).

The same participant mentioned that because cybersecurity is complex, it requires people who can learn and adapt quickly to address threats. Therefore, the participant advocates for recruiting the highest calibre candidates.

"So, you need to recruit the best of the best in this space to effectively and timeously deal with these kinds of threats." (P3).

Other participants shared similar views and noted that recruiting the required cybersecurity skills is a common challenge in the industry. As part of the induction, one participant at the executive management level took on the responsibility of addressing recruits. The participant notes that these sessions were valuable in communicating the expectations in terms of behaviour but are not enough to shape the culture of employees.

"I pushed the issue of values, what we value, what we expect of you and the issue of what is corrupt practices, what does theft, what does bribery, etc. linked to in terms of inappropriate behaviour or any forms of misconduct. I used to try and kind of teach them in terms of what we expect of you now. One session, I spend an hour and a half with them, it's not enough, but at least it informs them in terms of what we expect from them." (P3).

Another participant took up the responsibility to induct recruits on the cybersecurity practices of the organisation. The participant mentions that it is not ideal but believes it is essential to conditioning new employees' cybersecurity behaviour.

"When new employees are taken on, I discovered that IT did not have a slot when there's an induction session, so I approached them, and they've made me like a permanent representative dong the induction. So, I do my presentations revolving just a few key elements. We did the cybersecurity passwords. I believe it's better than nothing, but I'm not entirely satisfied, but it's better than not doing it." (P5).

4.8.5 Human resources

Participants shared their views on how human resources can shape the cybersecurity culture of the organisation. Participants said that the current human resource constraints do not allow for cybersecurity to take focus. Providing dedicated resources for cybersecurity ensures that activities are prioritised and are seen to completion. One participant mentions:

"When it comes to the cybersecurity point of view. There's very little individuals or teams that are actually looking at this. Those individuals are actually also assigned or are working on other things, so cybersecurity is a secondary there." (P1).

Another participant provides a view on the impact of dedicated resources to create awareness and a culture of cybersecurity.

"It meant that yeah, we need to have more resources to be able to introduce initiatives that focus on the people within eThekwini to create more cybersecurity awareness." (P2).

Participants also shared a common view concerning establishing the organisational structure to support cybersecurity. The organisation's challenges from these perspectives are discussed in Section 4.4.4 on organisational structure and Section 4.4.8 on public versus private sector. Participants felt that the organisation needs to have an agile organisational structure adaptable to the fast-changing cybersecurity environment. One participant highlighted the importance of having the requisite human resources in the cybersecurity domain by saying:

"You know, so it's the people and technical skills that you need and excellent technical skills that you need, based on meritocracy, that will ensure we could effectively and timeously deal with any cybersecurity threat, its people, nothing else." (P3).

4.8.6 Cybersecurity systems

Participants mentioned that cybersecurity systems were necessary to ensure that the policies and practices of the organisation are enforced and that cybersecurity attacks do not exploit employees. In addition, cybersecurity systems act as a safety net if an employee inadvertently or deliberately compromises the organisation's security. One participant said that management must ensure that the appropriate systems are in place to support the cybersecurity strategy and to protect employees.

"So, from the from a management point of view, you need to provide the facility or mechanisms to assist employees to do their work in a conducive way without being exploited and putting in mechanisms to prevent them from accessing websites that your policy prohibits them from accessing. So, the issue around technologies like access control technologies. There's different technologies that exists to help prevent the exploitation of human vulnerabilities." (P4).

Participants also shared a common view that technology essentially forces certain types of user behaviour, which ultimately will impact the cybersecurity culture. Moreover, management also needs to implement cybersecurity systems that make it easier for employees to comply with the policy. One participant provided an example of a single sign-on solution and said:

"It shows management's commitments to providing technology to support their cybersecurity initiatives, and I think that will obviously help improve this cybersecurity culture because it shows that management is just not directing. They also trying to assist with making the process much easier to support cybersecurity." (P4).

Therefore, management needs to establish cybersecurity systems that enable employees and develop a culture of cybersecurity.

4.8.7 Performance evaluation

Performance evaluation is viewed as one of the significant motivating factors of employee behaviours. In addition to the motivating factors discussed in Section 4.6.8, participants said that leadership could use the organisation's performance management systems to influence the desired cybersecurity culture.

"I think one of the bigger ones is to incorporate it in performance plans. So, if we are monitored on cybersecurity and we managed on it, I think it definitely instils or changes their behaviour because naturally people want to work towards that KPI." (P4).

Another participant highlights employees' attitudes towards activities that are not part of their performance plans. For example, the participant mentions that many employees do not consider or understand cybersecurity and are likely not to do anything related to cybersecurity if it is not on their performance plans.

"A lot of people feel it its not on their performance plan they don't need to do anything about it. Like Yeah, I don't think people really understand the impact of it, so they don't really consider it and do anything about it. I think one of the easiest things that managers could use is people's performance plans, to encourage and to make people more aware of cybersecurity." (P8).

As indicated by this participant, a common view is that performance plans are an easy method of creating cybersecurity awareness and establishing the desired cybersecurity behaviours.

4.8.8 Change management

Participants highlighted that the concept of change management is required to successfully incorporate cybersecurity into the organisation's practices, which over time become a culture of cybersecurity. Participants also viewed change management as vital to ensuring that stop-gap solutions for cybersecurity are not implemented. One participant said:

"The change management aspect when you're delivering new technologies, that's also an important point. Make sure it's managed in a coordinated way. Don't try and change existing processes too much but try and integrate cybersecurity into the existing processes that will definitely help shape the culture." (P4).

An important aspect of closing cybersecurity gaps that are left when, for example, an employee resigns or is dismissed is revoking their access to critical systems. One participant said this is vital to protecting the organisation from disgruntled employees. In highlighting this, the participant said:

"How do you make sure that you removed all previous access through a very formal process?" (P3).

Participants viewed change management as a requirement to ensure that cybersecurity is integrated into every aspect of the business, from the time new technology or employees are brought into the organisation up until they are no longer a part of the organisation. One participant drew a parallel to safety culture where the current practice in terms of change management is for contractors to supply the municipality with a safety plan. The participant asked why is the same not done for cybersecurity.

"Let me give you a parallel example, OK. Safety is very important as a culture in the organisation. When we go out on tender, we actually specify that the person must give us a safety plan as part of the as part of the submission. That's because we deem within safety is very important in organisation. So, similarly when we go out on technical specifications where there's an element of communications attached to it. Why are we not asking the suppliers to give us a cybersecurity plan?" (P6).

4.8.9 Financial resources

Participants shared a common view that leadership can initiate and direct cybersecurity activities by defining and controlling the budgets for cybersecurity activities. The leadership role in creating the organisational culture is discussed in Section 4.6.1. One participant highlights how management can use financial resources to create a cybersecurity culture by saying:

"Management has the biggest role to play because management is in charge of defining and shaping the organisational culture. Management has the budget in order to essentially create that. They have the budget to create the awareness campaigns to deliver on cybersecurity training, cybersecurity boot camps and so forth." (P4).

By directing already constrained financial resources towards cybersecurity activities, management indicates its commitment to making organisational cybersecurity a priority for the organisation. This theme is discussed in Section 4.6.4 under leadership priority.

4.8.10 Cybersecurity champions

Participants viewed the role of cybersecurity champions as essential in disseminating cybersecurity culture throughout the various branches of eThekwini Electricity. Participants made recommendations for the establishment of cybersecurity champions in every branch. A common view was that these individuals could consolidate the information received from cybersecurity working groups or other strategic initiatives and create workshops within their individual branches to disseminate information regarding cybersecurity. One participant provided an example of how the cybersecurity champions may be used to align the cybersecurity aspects of the Units digitalisation strategy. The participant said:

"I believe that if we do have these cybersecurity champions within the business, anything that goes digital within the branch that champion within the branch will really consolidate all the technologies and have a real view of the cybersecurity issues pertinent for their product." (P4).

4.8.11 Rewards and punishments

Participants viewed rewards as a beneficial mechanism that leaders could use towards shaping the cybersecurity culture. However, participants viewed the use of punishments as difficult and ineffective in their environment. One participant said:

"I think they can be effective. But it would not just obviously be on its own. Because you are starting now to affect not just your operational part of the business, but also your IR part of the business, so it would also mean that then that some of these sanctions and or rewards to be incorporated in your human capital policies as well." (P1).

Another participant added to this view and mentioned that it is difficult to implement sanctions in this environment. The participant posed that the rewards be gamified to create interest and competition amongst employees for incentives. The participant said:

"With the baton, yeah, you know that approach doesn't work. It is difficult in our environment. You can make it more gamified where people can get incentives. You know you can make a ladder board, make sure that everyone within that department can see who's performed the best for the month, you know we start investing in incentives outside your normal salary." (P5).

Therefore, the use of rewards and punishments needs to be carefully considered in its implementation. The following section discusses the theme of safety culture and how aspects of safety culture can be applied to creating an organisational cybersecurity culture.

4.9 Safety culture

Participants expressed their views on how aspects of the organisation's safety culture could be applied to cybersecurity. The word cloud in Figure 4.6 illustrates the participant's views collated under the theme of safety culture. The word cloud illustrates words that the participants frequently said. For example, the words similar, risk, something, culture, and parallel were frequently mentioned for the theme of safety culture.

Figure 4.6: Word cloud - safety culture.

Many participants drew parallels between the organisation's safety culture and the development of an organisational cybersecurity culture. Numerous aspects of safety culture can be applied to creating a cybersecurity culture, and participants provided several examples of how safety practices could be applied from a cybersecurity perspective. For example, participants provided examples on aspects such as personal protective equipment versus cybersecurity tools; safety incident investigation versus cybersecurity incident investigation; safety root cause analysis and enhancing operating procedures versus cyber incident root cause analyses and enhancing operating procedures; safety checks and inspections versus cybersecurity penetration testing. Participants drew numerous parallels between the two cultures. One participant provides an example of the parallel between safety culture and developing a cybersecurity culture. The participant said:

"So, I equate this potentially to safety, so an electrical utility itself has a high awareness or high risk as electricity itself is a high-risk environment, so there is a high safety element within all the safety activities or all the work activities that they undertake from the time that they specify equipment, there must be safety aspect of that. There are considered from the operational work. That that is undertaken, from construction, maintenance, there is safety. That is always an

element an aspect of safety. We need a similar kind of awareness and incorporation into cybersecurity." (P1).

The participant draws another parallel with safety culture, where individuals understand their responsibilities for keeping themselves and others safe from injury. The participant stresses that a similar culture can be applied to cybersecurity. The participant said:

"So, for instance with safety, you know that at first I'm responsible for my own safety and then those that are around me. Again, there can be similar culture as well in cybersecurity where everybody is now responsible for their own sort of secureness and ensure that others around them or the organisation is secure with respect to cybersecurity." (P1).

Another participant viewed reinforcing, which is an important aspect of developing a culture, as a beneficial parallel from safety culture. Reinforcing cybersecurity behaviours until they become embedded in employees. The participant said:

"I think the concept of reinforcing it has to be something that I think like a parallel to safety becomes part of our daily operation. Where cybersecurity is not a separate activity, but it's an activity that's embedded within the organisation." (P2).

Safety is taken seriously in the organisation because electricity is a life-threatening product. Therefore, the organisation is mandated by the occupational health and safety act to have legal appointments at the executive level that are accountable for health and safety. One participant draws a parallel to this by saying:

"If you make that analogy to safety, it's a national directive through the OSH Act. Like there was a national drive for compliance to NERC that's happening in the US. Then when I spoke about those cyber champions where every branch you got a cybersecurity rep as well. So, there's a very similar analogy to that." (P4).

As discussed in Section 4.6.5 leadership accountability and Section 4.7.2 external rules and regulations, participants viewed the lack of mandatory appointments for cybersecurity as a challenge in using accountability at the executive level to drive a cybersecurity culture. Participants said cybersecurity would only become a priority, similar to safety, when the South African energy regulator adopts international standards that define mandatory cybersecurity requirements. The following section discusses the theme of employee behaviours that are a result of the organisational cybersecurity culture.

4.10 Behaviours

Employee behaviours in terms of their actions or inactions with regards to cybersecurity are a result of the organisation's cybersecurity culture. Participants expressed their views on how the organisations cybersecurity challenges, discussed in Section 4.4, external influences, discussed in Section 4.7, cybersecurity awareness, discussed in Section 4.5, organisational mechanisms, discussed in Section 4.8 and safety culture, discussed in Section 4.9, all influence the cybersecurity culture, discussed in Section 4.6, which ultimately results in the cybersecurity behaviours displayed by the employees.

The word cloud in Figure 4.7 illustrates the participant's views collated under the theme of behaviours. The word cloud illustrates words that the participants frequently said. For example, the words focus, employees, compliance, management, and reinforcing were frequently mentioned for the theme of behaviours.

Figure 4.7: Word cloud - behaviours.

One participant indicated that the required cybersecurity behaviours need to be reinforced in employees. Furthermore, monitoring of the behaviours needs to be undertaken to ensure that employees are complying with the policy. The participant said:

"I think where we are not adequately addressing, is the concept of reinforcing. I think that's where you know in terms of continuous improvements. So, you will find that maybe with the lower-level staff that is not as frequent. We could have reinforced these policies, so I think also where we are failing or it's not adequate is we've not yet been able to implement the concept of auditing to confirm that the policies are actually being fully complied with." (P2).

The above extract echoes the other participants' sentiments in that there is a lot more that needs to be done in establishing an effective organisational cybersecurity culture. As detailed in Section

4.6, the current state of the organisational cybersecurity culture is varied and immature, with many participants viewing that even though a few initiatives are being undertaken around cybersecurity, a lot more needs to be done to create a culture of cybersecurity at the organisational level.

4.11 Chapter summary

This chapter presented the results from the research conducted at eThekwini Electricity. Ten participants who represent the various levels of leadership in the organisation were interviewed. All the participants have in-depth knowledge of the organisation's cybersecurity programs and were able to convey their knowledge to the researcher effectively. The process of thematic analysis revealed several themes and subthemes from the interviews. Each of these themes was presented, and participants' views supporting the theme were provided as evidence. Participants responses to the interview questions provided a deeper understanding of the leadership role and challenges of establishing an organisational cybersecurity culture. The next chapter undertakes an analysis of the results that are presented in this chapter in relation to the literature presented in Chapter Two.

CHAPTER 5: DISCUSSION

5.1 Introduction

This chapter discusses the research findings detailed in Chapter Four by comparing and contrasting to literature and previous studies discussed in Chapter Two. In doing so, the researcher supports the research findings by distinguishing similarities and differences from existing literature.

This chapter begins by providing an overview of the study participants and discusses the motivation for their selection. Thereafter, the seven themes and thirty-six sub-themes identified in the research findings are discussed with respect to the study's objectives and the literature presented in Chapter Two, which provides the theoretical lens from which to analyse and interpret the results.

5.2 Study participants

Ten participants were selected based on their leadership positions and cybersecurity knowledge. Participants from executive management, senior management, and senior technical expert levels of leadership were selected based on their in-depth knowledge of the organisation's cybersecurity programs. This selection of participants provided the researcher with the perspectives of leaders regarding organisational cybersecurity culture and the role of leaders in its development.

5.3 The current state of organisational cybersecurity culture

5.3.1 Cybersecurity challenges

The findings revealed that the organisation faces numerous cybersecurity challenges. Participants indicated that the nature of electricity distribution and its close ties to the economy of the eThekwini region makes it an attractive target for individuals who want to cause widespread damage and disrupt society. This perspective is shared with McLaughlin et al. (2016) and Miller et al. (2021), who showed that cyberattacks on critical infrastructure organisations such as electric utilities have become more frequent and have severe implications such as disrupting economies and loss of life. It was found that the digitalisation drive is the primary activity that introduces cybersecurity risk to the organisation. Jeyaraj and Zadeh (2020), who support this view, describe internet-enabled industries as lucrative targets for cybercriminals. Notably, participants held the view that humans pose the most significant cybersecurity risk to the organisation. This view is corroborated by Da Veiga (2016), who cite the risk posed by humans as the primary cause of cybersecurity concern.

The findings also revealed that the lack of priority for organisational cybersecurity resulted in misalignment between the core business function of electricity distribution and cybersecurity activities, which resulted in gaps that create vulnerabilities, exposing the organisation to cybersecurity attacks. Furthermore, it was found that the organisational structure did not support digitalisation and, therefore, cybersecurity, which resulted in silos where each department took an isolated approach to address cybersecurity vulnerabilities within their area. Glaspie and Karwowski (2017) show that leaders prioritise cybersecurity by aligning the organisational strategy and structure with the cybersecurity objectives. Moreover, it was found that departments have implemented technology solutions to address cybersecurity within their domains with minimal effort placed on securing the human element. This finding is consistent with the findings of Malatji et al. (2019), who highlight the vulnerabilities created by the socio-technical gap formed when organisations focus primarily on technology dimensions of cybersecurity.

Insider threats, particularly disgruntled employees, were viewed as the most significant risk to the organisation. Participants viewed the risk from insiders as greater than that posed by external threats, mainly because of the intimate knowledge that employees have of the organisations critical systems and networks. The findings also revealed that creating a cybersecurity culture can help address the challenge presented by employees who intend to disrupt the organisation. This view is consistent with Georgiadou, Mouzakitis and Askounis (2021), who describe securing the organisation against malicious insiders as the most difficult challenge. They advocate creating a cybersecurity culture that aims to strengthen the bond between the employee and the organisation.

The findings indicated that the lack of cybersecurity incident experience has resulted in cybersecurity not being a priority for the organisation. In a resource-constrained organisation, this reflects in the under-allocation resources and frequent reprioritisation of cybersecurity initiatives. This finding is consistent with that of Kure and Islam (2019), who added that organisations need to take a systematic approach to risk management and understand the relevant vulnerabilities of the business. In identifying critical assets and their interdependencies, organisations can justify and proactively allocate resources towards mitigating the highest levels of risk.

It was found that the organisation needed special resources and capabilities to address the complexity and multidisciplinary nature of cybersecurity challenges in the critical infrastructure environment. In addition, participants viewed the shortage of critical cybersecurity skills as an industry-wide problem. This finding is consistent with Furnell (2021), who highlight the global shortage of cybersecurity skills across all levels and types of organisations, especially those that manage critical infrastructure.

The results revealed that the bureaucracy and rigidity of public sector organisations hinder their ability to adapt and deal with the challenges brought about by the dynamic nature of cybersecurity. For example, participants felt that the enforcement of policies and restructuring the organogram to create new roles that would address the fast-changing cybersecurity environment were easier to implement in the private sector. This finding is contradictory to that of Alfawaz (2011), who shows that the authoritarian and bureaucratic culture of public sector organisations made it easier to implement information security practices.

The organisation's cybersecurity challenges stem from the Electricity Unit being an attractive target for cyberattacks, misalignment between core business functions and cybersecurity, insider threats, lack of cybersecurity incident experience, resources and capabilities, and the public sector landscape. Moreover, the participants viewed the lack of declared values, governance structures, and consolidated strategy for cybersecurity as inadequate. The findings indicate that the organisation needs a holistic approach to cybersecurity that emphasises securing employees. This view is corroborated by Huang and Pearlson (2019), who advocates taking a human approach to cybersecurity by creating a culture of cybersecurity.

5.3.2 Cybersecurity awareness

The findings revealed the importance of cybersecurity awareness in developing a culture of cybersecurity. Basic knowledge and understanding of cybersecurity concepts provide fundamental awareness of cybersecurity risks in all employees, which is key to shaping the desired behaviours. This view is supported by Da Veiga et al. (2020), who highlight the positive relationship between cybersecurity awareness and developing a culture of cybersecurity. However, it is evident that employees across all levels of the organisation do not possess a fundamental understanding of cybersecurity, let alone the concept of a cybersecurity culture. Therefore, cybersecurity is not thought about often enough for the organisation to prioritise resources towards addressing cybersecurity risks or for employees to adequately secure themselves against cybersecurity attacks. Huang and Pearlson (2019) advocate for creating cybersecurity awareness at the organisation's leadership, group and employee levels, thus establishing the prerequisite knowledge for shaping a culture of cybersecurity.

Awareness of one's involvement in cybersecurity incidents is viewed as a significant driver of a cybersecurity culture. The findings indicate that employees who are aware of how cybersecurity attacks against the organisation can impact them in their personal lives are more likely to take precautions to be more cyber-secure. This finding is consistent with that of Huang and Pearlson (2019), who argue that employees should understand the personal implications of cybersecurity. They further argue that personal involvement is the key differentiator between information security culture and cybersecurity culture.

5.3.3 External influences

External influences from peer institutions such as other organs of state, external rules and regulations in the form of government acts and industry regulations, societal cybersecurity culture, and professional bodies were found to influence the organisation's cybersecurity culture. It was found that the organisation had not experienced any cybersecurity attacks. However, recent cyber attacks at other comparable state institutions created awareness of the risk that cybersecurity attacks on critical infrastructure organisations are increasing and could materialise at any time. It was evident that these incidents motivated the participants to take notice and question the adequacy of their cybersecurity implementations. This finding is consistent with that of Barton et al. (2016), where it was found that institutional pressures shape managers beliefs to undertake cybersecurity initiatives. It was also found that key customers and service providers who have strong cybersecurity practices can significantly influence the organisation's cybersecurity culture through the type of cybersecurity requirements they impose or the solutions they provide to the Unit. This finding is consistent with the institutional mimicry theory of DiMaggio and Powell (1983), where organisations are influenced by the coercive, mimetic, and standardising processes of their industry peers to comply with the dominant practices and social expectations within their organisational field.

It was found that external rules and regulations, such as the POPI Act, shape the organisation's cybersecurity practices. However, the absence of statutory requirements for cybersecurity in the electric utility environment creates a lack of top-down drive, which influences the poor cybersecurity culture. In addition, the limitation of non-compulsory requirements for cybersecurity appointments meant that the organisation was not forced, and therefore does not have anyone representing cybersecurity at the executive level. It was found that cybersecurity representation at the executive level will only be established when a regulatory framework for critical infrastructure cybersecurity is passed in South Africa. It was also found that external audits created an awareness that positively influenced the cybersecurity culture within the branches that were audited. These findings are consistent with those of Huang and Pearlson (2019), who found that regulations from the government or other regulatory bodies significantly influence cybersecurity culture. Therefore, the lack of these types of external influences drives the poor organisational cybersecurity culture that exists within the Unit.

The findings revealed that the cybersecurity awareness and culture of the people in the eThekwini region influences the cybersecurity culture that employees bring into the organisation. Participants mentioned that cybersecurity awareness and knowledge should be fostered at the schooling level to increase societal cybersecurity culture. This finding correlates to that of Uchendu et al. (2021), who showed that societal cybersecurity culture plays a fundamental role in influencing and developing an organisational cybersecurity culture.

Executive management viewed professional bodies as a significant external influence that motivated professionally registered employees to act ethically and professionally, in line with desired cybersecurity behaviours. Professional registration is viewed as an occupational asset; therefore, employees will not risk their professional registration and undertake activities to jeopardise the organisation's cybersecurity systems. This finding is supported by the rational choice theory founded by Scott (2000) and the deterrence theory founded by Williams and Hawkins (1986). As discussed in Chapter Two, the rational choice theory notes that people weigh the perceived benefits and costs of their actions prior to determining how to proceed. Deterrence theory describes the psychological process that deters individuals from contravening laws based on the perceived severity of the penalty, the certainty of application, and the speed of enforcement (Williams and Hawkins, 1986).

5.3.4 Cybersecurity culture

The findings revealed that there was no organisational cybersecurity culture present in the Electricity Unit. However, participants viewed that the organisation is at the initial stages of developing an organisational cybersecurity culture. It was found that, due to the different job functions and levels of awareness, certain groups of employees displayed aspects of the desired cybersecurity culture. Several branch level efforts are in progress to improve the level of employee's awareness and knowledge. However, the initiatives are left up to a few individuals and do not cut across the organisation. It is evident that the cybersecurity culture is not sufficiently developed to defend against cyber threats. Participants felt that a lot more needed to be done to develop and improve the organisational cybersecurity culture. It was also found that the primary reasons for the inadequate organisational cybersecurity culture stemmed from a lack of management awareness around cybersecurity and the absence of a holistic cybersecurity policy for the organisation.

Employees general cybersecurity threat awareness is a significant driver of behaviours that support the organisational cybersecurity culture. It was found that employees should be made aware of cybersecurity attacks by communicating how they could be affected personally. For example, a cybersecurity attack on the organisation could disrupt the systems that pay employee salaries. Participants viewed that if employees understood their connection to cybersecurity attacks, they would be more aware of the risks. This view is supported by the findings of Huang and Pearlson (2019). However, this approach had not been taken in the organisation, and employees currently view cybersecurity as the organisation's problem, not theirs. The findings revealed that although initiatives are being undertaken to create cybersecurity awareness, it is evident that the organisation needs to emphasise awareness and training such that cybersecurity resides in the minds of all employees, securing them in their personal and professional lives. This

finding is consistent with that of Yildirim (2016), who advocate for leaders to take a holistic approach to cybersecurity.

Employees are currently made aware of cybersecurity policies via emails. However, this was found to be inadequate for employees to understand the information contained in the policy and what is actually required of them. Participants felt that the organisation needs to be more proactive, using alternative methods of creating awareness and reinforcing cybersecurity policies, therefore creating an understanding of cybersecurity policy and the personal connection to cybersecurity. This view concurs with that of Glaspie and Karwowski (2017) who, view that effectively communicating cybersecurity policy such that employees understand the expectations is key to shaping the cybersecurity culture.

It was found that various factors motivated employees to protect and defend the organisation against cybersecurity attacks. For example, factors such as their level of cybersecurity threat awareness, awareness of their personal connection to cybersecurity, cybersecurity training, external influences, performance appraisal, rewards and punishments, leadership participation and leadership prioritisation were all significant motivating factors. This view is supported by the findings of Huang and Pearlson (2019). It was further highlighted that employee accountability and responsibility was significant in motivating employees to be more cyber secure. This finding corroborates with that of Tang, Li and Zhang (2016), who found that employee accountability influences cybersecurity culture.

Employee knowledge was seen as an essential aspect of shaping the cybersecurity culture in the organisation. It was found that all employees need to have a minimum level of knowledge brought about by awareness and training to keep themselves and the organisation safe from cyber attacks. This finding is supported by Uchendu et al. (2021), who cite knowledge as an essential aspect of creating and maintaining a cybersecurity culture.

It was found that if employees are committed to the organisation, they are more likely to behave in ways that will keep the organisation safe from cybersecurity attacks. Employee motivation and general threat awareness were viewed as influencers of employee commitment. This finding is consistent with that of Nævestad et al. (2018), who found that both top management commitment and employee commitment are essential factors for developing a cybersecurity culture.

The findings revealed that executive management places a high degree of trust in employees who manage the organisation's critical systems. This trust is due to those employees holding professional registration with the Engineering Council of South Africa (ECSA). This binds the employees to a code of conduct to operate ethically and morally and not undertake activities that will compromise the organisation's cybersecurity posture. This finding is supported by the

findings of (Uchendu et al., 2021), who view trust as an essential factor in establishing a cybersecurity culture.

The lack of formalised interdepartmental collaboration on cybersecurity matters was highlighted as a challenge in developing the organisational cybersecurity culture. Participants viewed current informal interdepartmental collaborations as lacking a consistent and concerted effort towards delivering organisational objectives. This finding is underpinned by Cannon-Bowers and Salas (2001) shared team cognition theory. Reegård et al. (2019) say that establishing formal cybersecurity teams and committees increases knowledge sharing, mitigating cybersecurity risks. It was found that because cybersecurity is not seen as a high-level organisational requirement, it lacks the top-down focus and drive that is imperative to establish formal interactions between the branches. Moreover, participants advocate the need to have someone at the executive level to drive and coordinate cybersecurity activities across the organisation. This finding is consistent with the findings of Uchendu et al. (2021), who identified top management support and leadership involvement as the most important factor in developing a cybersecurity culture.

5.4 Leadership role in developing the current cybersecurity culture

5.4.1 Leadership role

It was found that leadership plays an essential role in shaping the cybersecurity culture within the Unit. It was evident that leaders need to drive the development of a cybersecurity culture through their accountability, knowledge, participation and priority of cybersecurity initiatives. In doing so, leaders can influence others by leading by example, providing and directing organisational resources towards cybersecurity, and constantly reinforcing the desired behaviours to shape the cybersecurity culture. This finding is consistent with that of Huang and Pearlson (2019), who show that leaders play a critical role in defining the organisational cybersecurity culture.

The findings indicate that leaders need to accept responsibility and accountability for cybersecurity because of its impact on business operations and service delivery. Participants highlighted that activities are tracked to completion when leaders are made accountable. It was also discovered that leaders display ownership and commitment to cybersecurity when they accept accountability for activities such as cybersecurity audits. This finding concurs with that of Da Veiga et al. (2020), who view leadership accountability as the foundation of developing a culture of cybersecurity. It was evident that the organisation has a well-established safety culture that is driven by accountability at the executive level. However, it was found that a lack of statutory requirements for cybersecurity posed a challenge in using accountability at the executive level to drive a cybersecurity culture.

It was evident that leaders needed to understand cybersecurity as a key risk to the business. In order to have this understanding, leaders need to have knowledge about cybersecurity and how it

can impact the organisation. It was found that participants from the senior management and senior technical expert levels were knowledgeable about cybersecurity and the organisation's vulnerabilities. However, the executive management level participants understood the implications of cybersecurity attacks but did not have any cybersecurity knowledge. It was found that leaders who possess cybersecurity knowledge are more likely to undertake activities to secure the organisation against cybersecurity threats, therefore, shaping a culture of cybersecurity in the process. This finding is consistent with that of Huang and Pearlson (2019), who view leaders that have cybersecurity skills and competencies as more knowledgeable about the organisation's cybersecurity vulnerabilities and, therefore, will take actions to mitigate risks to the organisation. Van't Wout (2019) further supports this finding by highlighting that a lack of leadership knowledge about the organisation's cybersecurity risks and vulnerabilities causes a disconnect between the core business functions and cybersecurity. To overcome these challenges, participants advocated for compulsory cybersecurity training for those in leadership positions.

It was found that participants from senior management and senior technical levels participated in various cybersecurity initiatives within their respective branches. Their participation helped to influence the cybersecurity culture at the branch level. This finding is consistent with that of Glaspie and Karwowski (2017) and Huang and Pearlson (2019), who found that employees are influenced to participate in cybersecurity when management is seen participating in cybersecurity initiatives themselves. However, it was evident that the participants at the executive management level have minimal involvement in cybersecurity activities. Moreover, leaders at this level only participate when it is a legislative or audit requirement to do so. Reegård et al. (2019) view the participation of executive management as essential to shaping the organisational cybersecurity culture.

Examining the findings revealed that participants at the executive management level have not made cybersecurity a priority for the organisation. It was found that other strategic business initiatives were prioritised over cybersecurity projects because the risks from cybersecurity threats have not materialised. This is evident in the inadequate allocation of resources towards organisational cybersecurity. However, participants at the senior management and senior technical level felt that cybersecurity was important, and therefore they found ways to prioritise cybersecurity within their branches. This finding is consistent with that of Huang and Pearlson (2019), who highlight that leaders will only make cybersecurity a priority if they believe that cybersecurity is important for the organisation. The importance will be reflected in the strategic direction leaders set as well as the allocation of resources towards cybersecurity.

5.4.2 Organisational mechanisms

The study found that leaders could use various organisational mechanisms to influence employee behaviour towards the desired cybersecurity culture. Participants view an organisational cybersecurity strategy as the fundamental aspect for achieving a consolidated effort towards addressing cybersecurity risks and developing a culture of cybersecurity. However, it was found that the organisation did not have an overarching cybersecurity strategy that ties in the business objectives with the cybersecurity initiatives undertaken at the branch level. This finding is consistent with the observations of Van‘t Wout (2019), who found that inadequate leadership knowledge about the organisation’s cybersecurity risks and vulnerabilities results in a bottom-up approach to cybersecurity strategy that is disconnected from the core business functions.

It was found that cybersecurity training is essential for developing and reinforcing knowledge within employees. Further, it was evident that cybersecurity awareness and knowledge is a significant contributor to shaping the culture of cybersecurity. This view is supported by Huang and Pearlson (2019), who say that cybersecurity training is necessary to increase employee awareness around cybersecurity issues, educate employees about cybersecurity, and develop the skills and competencies required for employees to assume cybersecurity roles. It was also found that regular and varied training is required to support the once-off cybersecurity awareness sessions that are provided to new employees. This finding concurs with that of Glaspie and Karwowski (2017), who say that regular training establishes and reinforces habits that support the cybersecurity policy and, therefore, fosters a culture of cybersecurity.

Employees are made aware of cybersecurity policies and practices through broadcast email, document repositories and posters displayed in shared spaces. It was found that, although this creates awareness, it is inadequate to engage employees on cybersecurity effectively. Participants viewed taking a proactive approach and hosting cybersecurity sessions to communicate policy, awareness campaigns, incidents that occur at other organisations, and how cybersecurity attacks can affect them personally. This finding is supported by Huang and Pearlson (2019), who view the use of appropriate communications channels as key to ensuring that cybersecurity information is received timeously and in the appropriate form for employees to digest.

It was evident that recruitment is a key process used to bring essential skills into the organisation. It was found that to adequately address the cybersecurity challenges, the organisation needed to recruit the highest calibre candidates. This finding concurs with that of Alfawaz (2011), who found that the recruitment of critical cybersecurity resources and capabilities is essential to the success of cybersecurity initiatives and developing a culture of cybersecurity. It was also found that executive management used the induction process to personally address recruits on the organisation’s values and the executives’ expectations regarding ethical behaviour. Another

participant at the senior technical expert level used employee induction to create basic awareness about cybersecurity. Huang and Pearlson (2019) show that the personal involvement of leadership establishes the importance of cybersecurity to employees.

It was found that leaders should establish cybersecurity systems to ensure that the policies and practices of the organisation are enforced and that cybersecurity attacks do not exploit employees. In addition, participants felt that cybersecurity systems are essential in forcing certain types of user behaviour towards the desired cybersecurity culture. This view is underpinned by the technology acceptance model, Davis (1985), and is consistent with Da Veiga et al. (2020), who found that not having the appropriate cybersecurity systems to support the strategy is an obstacle to creating a culture of cybersecurity.

It is evident that performance evaluations are a significant motivating factor in shaping employee behaviours. It was found that employees only consider tasks that appear on their performance plans as necessary. Therefore, employees will not undertake activities related to cybersecurity if it does not appear on their performance plans. It is evident that leadership could use the organisation's performance management systems to influence the desired cybersecurity culture. This view is underpinned by expectancy theory, Lawler III and Suttle (1973) and supported by Huang and Pearlson (2019), who view performance evaluation as a significant driver of cybersecurity behaviours and, therefore, cybersecurity culture.

Change management is seen as an essential part of integrating cybersecurity into all business functions, from the time new technology or employees are brought into the organisation until they are no longer a part of the organisation. Furthermore, it was evident that change management is vital to adapting employees to change and curbing the current practice of using stop-gap solutions to address cybersecurity challenges. This finding is supported by the findings of Al Hogail (2015) and Da Veiga et al. (2020), who show how change management principles applied to systems, operations and employees, assist in integrating cybersecurity into the business, therefore influencing the cybersecurity culture.

The findings indicate that management can initiate and direct cybersecurity activities by allocating financial resources towards cybersecurity initiatives. It was also found that leaders display commitment when they direct constrained financial resources towards cybersecurity. This finding is supported by Uchendu et al. (2021), who found that the commitment of resources to cybersecurity in resource-constrained organisations significantly influences the cybersecurity culture.

It was found that cybersecurity champions are essential in disseminating cybersecurity culture throughout the organisation by consolidating the information received from cybersecurity working groups and sharing it within their branches. This finding is underpinned by social control

theory, Janowitz (1975), and supported by Alshaikh (2020), who show that establishing a cybersecurity champion network supports the development of a cybersecurity culture through spreading cybersecurity information, creating awareness and delivering cybersecurity training.

It was found that leaders need to consider the use of rewards and punishments carefully. Participants viewed rewards as effective and punishments as difficult and ineffective in shaping the cybersecurity culture. This finding is underpinned by the rational choice theory of Scott (2000) and the deterrence theory of Williams and Hawkins (1986). This finding is also corroborated by Blythe, Gray and Collins (2020), who view punishments as challenging in that it affects employee performance and can erode trust between managers and employees. However, this finding contradicts that of Glaspie and Karwowski (2017), who view that organisations with severe consequences achieve better compliance and therefore have stronger cybersecurity cultures.

5.4.3 Safety culture

It was found that health and safety are very important in the organisation. Therefore, top management has driven a culture of safety to mitigate the risks to the organisation. Participants drew parallels between safety culture and cybersecurity culture in terms of the tools, incident investigation methods, root cause analysis, inspections, and organisational mechanisms that leaders use. It was evident that many of the aspects that are applied to shape the organisation's safety culture could be applied to developing an organisational cybersecurity culture. This finding is supported by that of Reegård et al. (2019), who demonstrate the similarities in the conceptualisation and managerial levers used to develop a safety culture and those used to develop a cybersecurity culture. They provide further support by saying that the managerial levers used to shape safety culture can be used to develop an organisational cybersecurity culture.

Electricity is a life-threatening product; therefore, the organisation is mandated by the occupational health and safety act to have accountability at the executive level. It was found that the lack of a regulatory framework that imposes mandatory appointments at the executive level for cybersecurity poses a significant challenge in using accountability to drive a cybersecurity culture. Huang and Pearlson (2019) show that establishing accountability at the executive level ensures that cybersecurity initiatives are formulated and actioned effectively to drive a culture of cybersecurity. However, it is evident that cybersecurity would only become a priority, similar to safety, when mandatory cybersecurity requirements are imposed; until then, there will be no real emphasis on accountability.

5.5 Organisational cybersecurity culture model

The current study revealed that many factors influence the organisational cybersecurity culture of the Electricity Unit. It was found that the cybersecurity challenges facing the organisation, the

external influences acting upon the organisation and the cybersecurity awareness of all employees influence the organisational cybersecurity culture. It was found that leaders use organisational mechanisms to influence the cybersecurity culture through their role, knowledge, participation, priority, and accountability of cybersecurity. Moreover, the cybersecurity culture was found to influence the organisational mechanisms. It was evident that the organisational cybersecurity culture influences the behaviours of employees, and in turn, the behaviours of employees influence the organisation's cybersecurity culture. The interpretation of the findings of this study revealed a model of the organisational cybersecurity culture. Figure 5.1 illustrates the constructs that were found to influence the organisational cybersecurity culture at the Electricity Unit. The dashed lines used for safety culture indicate that the approach taken to develop a safety culture could be applied to influence the development of the cybersecurity culture.

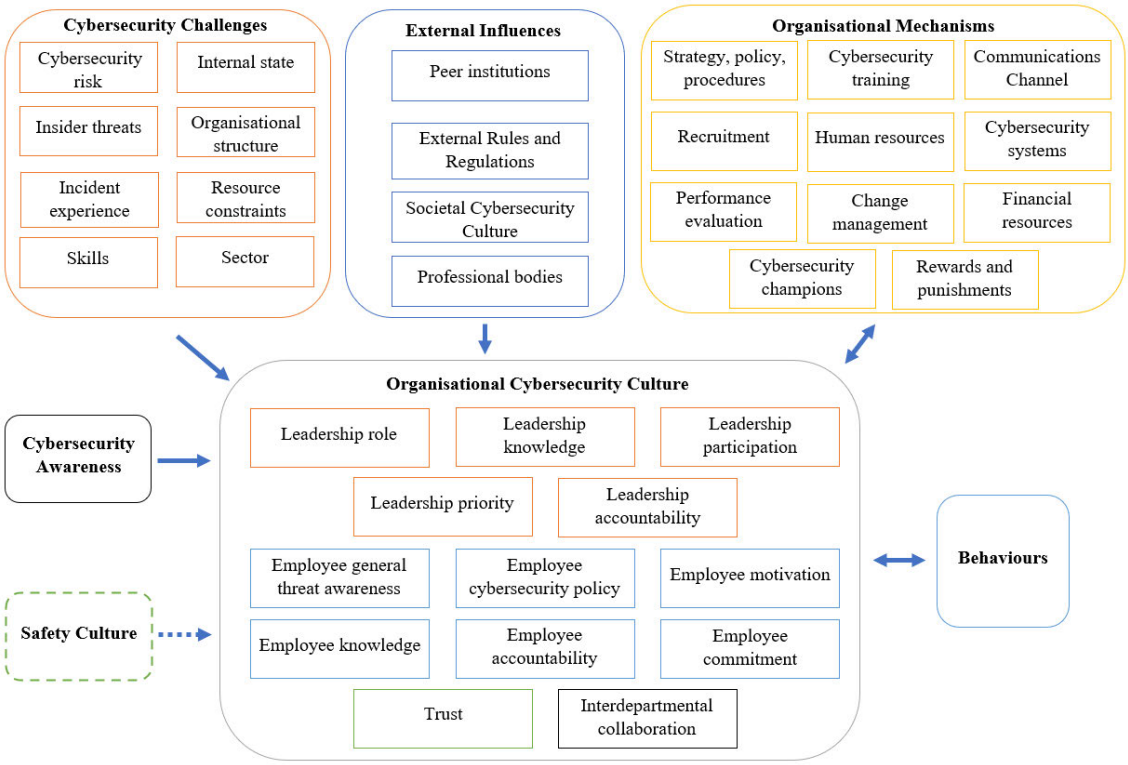


Figure 5.1: Organisational cybersecurity culture model.

It was evident that there are many commonalities in the conceptualisation and managerial levers used for developing and shaping a safety culture and those used for a cybersecurity culture. It was found that the organisation could apply a similar approach to that of the well-established safety culture to influence the development of the organisational cybersecurity culture. However, the lack of accountability for cybersecurity at the executive level limits the effectiveness of this approach.

5.6 Chapter summary

This chapter discussed the results of the research findings presented in Chapter Four in relation to the literature review discussed in Chapter Two, with the aim of addressing the research objectives discussed in Chapter One. Several themes and sub-themes relating to the current state of organisational cybersecurity culture and the leadership role in developing the current cybersecurity culture were discussed. The theoretical framework and conceptual model of organisational cybersecurity culture, discussed in Chapter Two, provided support for the identified themes and sub-themes. Lastly, a model of the organisational cybersecurity culture was proposed. The model comprises the factors that appeared to influence the development of an effective organisational cybersecurity culture at the eThekwini Electricity Unit. The next chapter presents the conclusions and recommendations of this study. Additionally, the limitations of this study and further areas of research are discussed.

CHAPTER 6: CONCLUSIONS AND RECOMMENDATIONS

6.1 Introduction

This chapter brings the study to a close by drawing conclusions and making recommendations to eThekwini Electricity on fostering a culture of organisational cybersecurity. This study explored the current state of organisational cybersecurity culture and the role of leadership in developing the cybersecurity culture at the eThekwini Electricity Unit. This research contributes to addressing the gap in the literature by undertaking qualitative research and exploring the role of leadership in creating an organisational cybersecurity culture to secure organisations that manage critical infrastructure.

The literature review focused on examining how culture, leadership, and cybersecurity contribute to understanding how leaders can develop an effective organisational cybersecurity culture to secure against cyber attacks aimed at exploiting human vulnerabilities. The theoretical framework and the conceptual model of organisational cybersecurity culture, discussed in Chapter Two, was used to support this study. The study employed a qualitative research methodology using purposive sampling to select ten participants based on their leadership positions and in-depth knowledge of the organisation's cybersecurity programs. Data was collected using semi-structured interview techniques. The results were obtained through thematic analysis of the interview transcripts to identify themes that emerged. Analysis of the results against the study objectives and the theoretical framework provided insight into the role of leadership in creating an organisational cybersecurity culture.

This chapter begins by addressing the objectives of this study. Then, recommendations to solve the research problem based on the findings of this study are made. The recommendations suggest various ways to improve the organisational cybersecurity culture at the eThekwini Electricity Unit. Thereafter the implications and limitations of this study are discussed. Lastly, recommendations are provided for future research on organisational cybersecurity culture in the electrical utility context.

6.2 Addressing the research objectives

6.2.1 The current state of organisational cybersecurity culture at the eThekwini Electricity Unit

The first research objective of this study was to explore the current state of organisational cybersecurity culture at the eThekwini Electricity Unit. Using the theoretical framework and conceptual model of organisational cybersecurity culture by Huang and Pearlson (2019), it was found that there was no organisational cybersecurity culture present. However, the research

findings indicate that the organisation is at the initial stages of developing an organisational cybersecurity culture, with groups of employees displaying aspects of the desired cybersecurity culture. In addition to the constructs developed by Huang and Pearlson (2019), this study also identified several themes and subthemes such as cybersecurity challenges, cybersecurity awareness, professional bodies, safety culture and trust, that contribute to the organisational cybersecurity culture at the eThekwini Electricity Unit. The research findings further indicate that the main reasons for the inadequate organisational cybersecurity culture at the eThekwini Electricity Unit stem from a lack of top management awareness around cybersecurity and the absence of a holistic cybersecurity strategy for the organisation.

6.2.2 The extent of the leadership role in developing the current cybersecurity culture at the eThekwini Electricity Unit

The second research objective was to determine the extent of the leadership role in developing the current cybersecurity culture. The analysis of the results revealed that leaders needed to drive the development of a cybersecurity culture through their accountability, knowledge, participation, and priority of cybersecurity initiatives. Participants from the senior management and senior technical expert levels were knowledgeable about cybersecurity, participated in cybersecurity initiatives, and prioritised cybersecurity within their branches. However, participants from the executive management level were not knowledgeable about cybersecurity, did not make cybersecurity a priority, and did not participate in cybersecurity initiatives unless it was a legislative or audit requirement.

This study also identified that leaders need to understand their role in driving a cybersecurity culture and accept accountability for cybersecurity because of its impact on business operations and service delivery. However, the lack of statutory requirements for cybersecurity remains a challenge in using accountability at the executive level to drive a cybersecurity culture. Therefore, the role of leadership in developing the current cybersecurity culture at the eThekwini Electricity Unit is limited.

6.2.3 Recommendations to improve the organisational cybersecurity culture at the eThekwini Electricity Unit

The final objective of this study was to provide recommendations to improve the organisational cybersecurity culture at the eThekwini Electricity Unit. Section 6.3 details the recommendations to the organisation.

6.3 Recommendations to address the research problem

This section provides recommendations that outline the role of leadership in improving the organisational cybersecurity culture at the eThekwini Electricity Unit. In undertaking the

following recommendations, leaders can increase their level of cybersecurity knowledge, participation, and priority for cybersecurity initiatives, shaping the organisation's cybersecurity culture so that all employees actively participate in reducing risk from the cyber domain.

6.3.1 Leadership accountability

The organisation needs to create accountability for cybersecurity at the executive level to drive the development of a cybersecurity culture. Establishing leadership accountability for cybersecurity will ensure that leaders participate in and prioritise cybersecurity activities. A formal appointment of an executive to coordinate cybersecurity activities and drive a culture of cybersecurity across the organisation needs to be made. The organisation should not wait for an external influence such as a regulatory framework for critical infrastructure cybersecurity to make this appointment.

Furthermore, leaders across the organisation need to accept the shared responsibility for addressing the cybersecurity challenges facing eThekwini Electricity by fostering a culture of organisational cybersecurity. Senior managers and employees at leadership positions need to be assigned the responsibility of developing and reinforcing a culture of cybersecurity.

6.3.2 Organisational cybersecurity strategy

The Electricity Unit needs to understand cybersecurity as a high-level organisational requirement and establish values, governance structures, and a consolidated strategy for cybersecurity. The Unit needs to create a consolidated strategy for cybersecurity that integrates into the core business functions and the digitalisation strategy such that cybersecurity is considered in every aspect of the business. Moreover, the strategy needs to tie in branch-level cybersecurity efforts towards the overall business objectives, establishing an alignment between core business functions and cybersecurity.

6.3.2.1 Organisational structure

To support the holistic cybersecurity strategy, the organisational structure needs to be aligned with the digitalisation drive in the business. Therefore, the organisation needs to establish an organisational structure to support digitalisation and hence cybersecurity. Several key cybersecurity positions need to be established. The organisation needs to create positions for a Chief Information Security Officer (CISO) at the executive level and cybersecurity managers and cybersecurity champions at the branch level.

6.3.2.2 Cybersecurity systems

Organisation wide cybersecurity systems are needed to ensure that policies and practices of the organisation are enforced, employees do not inadvertently or deliberately compromise cybersecurity, and that cybersecurity attacks do not exploit employees. To contribute to

developing the cybersecurity culture, the organisation should implement cybersecurity systems that make it easier for employees to comply with the policy.

6.3.2.3 Interdepartmental collaboration

The organisation needs to take a top-down approach to establish and maintain formalised cybersecurity committees. Formalised committees encourage cybersecurity collaboration and knowledge sharing between the various departments and branches, creating a concerted effort towards fulfilling business objectives and securing the organisation against cybersecurity threats.

6.3.2.4 Change management

The organisation needs to implement a formal change management system that integrates cybersecurity into all business functions, therefore creating a culture of cybersecurity over time. Change management will also assist the organisation in eliminating the current practice of implementing stop-gap solutions to address cybersecurity vulnerabilities.

6.3.2.5 Recruitment

The complexity and the multidisciplinary nature of cybersecurity requires a special set of skills. Furthermore, cybersecurity poses substantial risks to the business. Consequently, the cybersecurity function cannot be outsourced entirely. Therefore, the organisation needs to recruit the highest calibre candidates that can learn and adapt quickly to mitigate cybersecurity threats effectively and timeously. In addition, scarce skills remuneration packages need to be implemented to attract and retain top talent in the cybersecurity domain.

6.3.3 Cybersecurity champions

The organisation needs to formally appoint one person in every branch as a cybersecurity champion. The cybersecurity champion will consolidate information from the cybersecurity committees and coordinate cybersecurity initiatives within their branch. In addition, the cybersecurity champion network supports the development of a cybersecurity culture through spreading cybersecurity information, creating awareness and delivering cybersecurity training in each branch.

6.3.4 Cybersecurity training

Formal and informal cybersecurity training is required to instil basic cybersecurity knowledge and awareness in all employees. Formal cybersecurity training for all employees can be achieved by upskilling the organisations existing training centre to deliver fundamental cybersecurity training courses. Intermediate level cybersecurity training can be achieved through the work skills plans of employees that are involved in any project related to digitalisation. Work skills plans may also deliver advanced cybersecurity training for employees responsible for operating the

organisation's mission-critical systems. Informal training within branches can be achieved through the cybersecurity champions.

Cybersecurity awareness training needs to emphasise employees' personal involvement in how cybersecurity attacks against the organisation can impact them personally. A proactive approach needs to be taken in creating awareness and reinforcing policies such that employees understand what is required of them. Furthermore, to reinforce a culture of cybersecurity, the organisation needs to implement regular and varied cybersecurity training for all employees.

The organisation needs to enforce mandatory cybersecurity training for all employees at a leadership level. Compulsory cybersecurity training will establish the requisite cybersecurity knowledge in all leaders to become more aware of the organisation's vulnerabilities. Leaders will then have the knowledge to understand cybersecurity as a critical risk to the business.

6.3.5 Employee accountability

Participants viewed employee accountability as a key aspect of shaping the desired cybersecurity behaviours. Employees need to be made accountable for compliance with cybersecurity policy and compliance to cybersecurity standards and operating procedures that are part of their job functions.

6.3.6 Performance evaluations

Participants viewed performance evaluations as very effective in establishing the desired cybersecurity behaviours. The organisation's existing employee performance management systems can motivate employees to be more cyber secure by adding elements of cybersecurity onto employees' performance plans.

6.3.7 Safety culture

There are many similarities between establishing a safety culture and establishing a cybersecurity culture. Several organisational mechanisms that are applied to shape the organisation's safety culture could be applied to developing an organisational cybersecurity culture. The organisation should use the wealth of experience gained in terms of practices, top management support, and accountability in establishing the organisation's strong safety culture to drive the formation of an organisational cybersecurity culture.

6.4 Implications of this study

This study makes a significant contribution to the body of knowledge on organisational cybersecurity culture. There have been no previous studies that undertook qualitative research to explicitly focus on the role of leadership in establishing an organisational cybersecurity culture at critical infrastructure organisations such as electric utilities (Nasir et al., 2019; Uchendu et al., 2021). This study also highlights how organisations that manage critical infrastructure can

capitalise on their familiarity with existing safety culture practices to fast track the development of a cybersecurity culture. The results of this study enable eThekwini Electricity Unit leadership to develop an effective organisational cybersecurity culture to secure against cyber attacks aimed at exploiting human vulnerabilities.

This study can also benefit other electrical utilities in South Africa and abroad that face similar cybersecurity challenges. The study also provides researchers in this field with practical industry insight, opening areas for future research around organisational cybersecurity in the electrical utility context. Researchers may also find the study useful and choose to apply a similar approach to a different industry.

6.5 Limitations of this study

This study undertook qualitative research to explore the status of organisational cybersecurity culture at eThekwini Electricity at a single point in time, providing the basis to make recommendations for leadership to improve the organisational cybersecurity culture. The study does not undertake the implementation of the recommendations to solve the cybersecurity challenges facing the organisation. However, leaders can use the recommendations to shape the organisation's cybersecurity culture and conduct further longitudinal studies to determine the level of adoption and the success of the implementations. Therefore, indicating if a cybersecurity culture is being developed and maintained. This limitation serves as a key recommendation for future studies.

6.6 Recommendations for future studies

The organisation should conduct future longitudinal studies to assess the adoption of the recommendations and their effectiveness in developing an organisational cybersecurity culture. In assessing the cybersecurity culture, the organisation should employ a quantitative or mixed methods approach to sample a larger population of employees effectively.

A quantitative study may be conducted to assess employees' perspectives on the role of leadership in establishing an effective organisational cybersecurity culture. This perspective can provide valuable insight and complementary recommendations.

The framework used in this study may be applied at the municipal level. For example, future studies can explore the role of leadership in establishing an organisational cybersecurity culture in eThekwini Municipality or at other Business Units.

This study also creates opportunities for future research to focus on examining how organisations with a strong safety culture can influence the development of an organisational cybersecurity culture. For example, future studies can be conducted at eThekwini Electricity or at other organisations that manage critical infrastructure to determine the effectiveness of this approach.

6.7 Chapter summary

This study explored the role of eThekwini Electricity Unit leadership in creating an effective organisational cybersecurity culture at the eThekwini Electricity Unit. The findings of this study revealed the cybersecurity challenges experienced by the organisation and the current state of the organisational cybersecurity culture. The findings also revealed the extent of the leadership role in developing a culture of cybersecurity. As a result, several recommendations that outline the role of leadership in improving the organisational cybersecurity culture at the eThekwini Electricity Unit were made to address the organisation's cybersecurity challenges. This study also identified key themes such as safety culture that extended beyond the theoretical framework, indicating the contribution of this study to the body of organisational cybersecurity culture knowledge. Further studies were suggested to assess the effectiveness of the recommendations, investigate employees' perspectives, and examine the relationship between safety culture and cybersecurity culture. These recommended studies can also contribute to the body of knowledge in creating a cybersecurity culture to secure organisations against cybersecurity threats that aim to exploit human vulnerabilities.

REFERENCES

Addae, J., Radenkovic, M., Sun, X. and Towey, D. (2016). An augmented cybersecurity behavioral research model. *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC).* IEEE, 602-603.

Al Hogail, A. (2015). Cultivating and assessing an organizational information security culture; an empirical study. *International Journal of Security and Its Applications* 9(7): 163-178.

Alfawaz, S.M. (2011). *Information security management: a case study of an information security culture*. Queensland University of Technology.

Almeida, F., Santos, J.D. and Monteiro, J.A. (2020). The challenges and opportunities in the digitalization of companies in a post-COVID-19 World. *IEEE Engineering Management Review* 48(3): 97-103.

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security* 98: 102003.

Ani, U.D., He, H. and Tiwari, A. (2019). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology*.

Bandura, A. (2001). Social cognitive theory: An agentic perspective. *Annual review of psychology* 52(1): 1-26.

Bandura, A. (2005). The evolution of social cognitive theory. *Great minds in management*. 9-35.

Barton, K.A., Tejay, G., Lane, M. and Terrell, S. (2016). Information system security commitment: A study of external influences on senior management. *Computers & Security* 59: 9-25.

Bascomb, J. (2020). *Qualitative Case Study Exploring the Factors to Improve Employee Satisfaction and the Organizational Citizenship Behavior of Cybersecurity Professionals in the Department of Defense*. Northcentral University.

BBC (2019). *Ransomware hits Johannesburg electricity supply*. Available at: https://www.bbc.com/news/technology-49125853 [Accessed 20 September 2021].

Blythe, J.M., Gray, A. and Collins, E. (2020). Human Cyber Risk Management by Security Awareness Professionals: Carrots or Sticks to Drive Behaviour Change? *International Conference on Human-Computer Interaction.* Springer, 76-91.

Cannon-Bowers, J.A. and Salas, E. (2001). Reflections on shared cognition. *Journal of Organizational Behavior: The International Journal of Industrial, Occupational and Organizational Psychology and Behavior* 22(2): 195-202.

Chen, T.M. and Abu-Nimeh, S. (2011). Lessons from stuxnet. *Computer* 44(4): 91-93.

Cheng, L., Li, Y., Li, W., Holm, E. and Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security* 39: 447-459.

Chuttur, M.Y. (2009). Overview of the technology acceptance model: Origins, developments and future directions. *Working Papers on Information Systems* 9(37): 9-37.

Clarke, V. and Braun, V. (2013). Teaching thematic analysis: Overcoming challenges and developing strategies for effective learning. *The psychologist* 26(2).

Creswell, J.W. and Creswell, J.D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches.* Sage publications.

Da Veiga, A. (2016). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. *2016 SAI Computing Conference (SAI).* IEEE, 1006-1015.

Da Veiga, A., Astakhova, L.V., Botha, A. and Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security* 92: 101713.

Da Veiga, A. and Eloff, J.H. (2010). A framework and assessment instrument for information security culture. *Computers & Security* 29(2): 196-207.

Daft, R.L. (2014). *The leadership experience.* Cengage Learning.

Davis, F.D. (1985). *A technology acceptance model for empirically testing new end-user information systems: Theory and results*. Massachusetts Institute of Technology.

de Azevedo, G.P., Pellanda, P.C. and Campos, M.B. (2020). Addressing the Cybersecurity Challenges of Electrical Power Systems of the Future. *2020 12th International Conference on Cyber Conflict (CyCon)*. IEEE, 293-308.
Diesch, R., Pfaff, M. and Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *Computers & Security* 92: 101747.
DiMaggio, P.J. and Powell, W.W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American sociological review*. 147-160.
Electricity (2020). *eThekwini Electricity Annual Report 2019/2020*. Available at: http://www.durban.gov.za/City_Services/electricity/About%20Us/Documents/2019-2020%20Annual%20Report%20Final.pdf [Accessed 13 September 2021].
EMARAS (2019). DRAFT INTERNAL AUDIT REPORT (PROJECT CODE:) REGARDING ELECTRICITY UNIT: OT SECURITY - SCADA.
Ertan, A., Crossland, G., Heath, C., Denny, D. and Jensen, R. (2020). Cyber security behaviour in organisations. *arXiv preprint arXiv:2004.11768*.
Farwell, J.P. and Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival* 53(1): 23-40.
Fertig, T., Schütz, A.E. and Weber, K. (2020). Current Issues Of Metrics For Information Security Awareness. *ECIS*.
Furnell, S. (2021). The cybersecurity workforce and skills. *Computers & Security* 100: 102080.
Gcaza, N. and 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. and van Vuuren, J.J. (2015). An Ontology for a National Cyber-Security Culture Environment. *HAISA*. 1-10.
Georgiadou, A., Mouzakitis, S. and Askounis, D. (2021). Detecting Insider Threat via a Cyber-Security Culture Framework. *Journal of Computer Information Systems*. 1-11.
Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., Jabbar, S. and Baker, T. (2018). Security threats to critical infrastructure: the human factor. *The Journal of Supercomputing* 74(10): 4986-5002.
Glaspie, H.W. and Karwowski, W. (2017). Human factors in information security culture: A literature review. *International Conference on Applied Human Factors and Ergonomics*. Springer, 269-280.
Gole Babić, M. (2020). Organizational Culture Framework for Mitigating Human Factors in Cybersecurity.
Hofstede, G. (1984). Cultural dimensions in management and planning. *Asia Pacific journal of management* 1(2): 81-99.
Hsu, J.S.-C., Shih, S.-P., Hung, Y.W. and Lowry, P.B. (2015). The role of extra-role behaviors and social controls in information security policy effectiveness. *Information systems research* 26(2): 282-300.
Huang, K. and Pearlson, K. (2019). For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture. *Proceedings of the 52nd Hawaii International Conference on System Sciences*.
Hussey, J.Y. (2021). *Perceptions of Court Chief Information Officers, About Countering Cyber-Attacks: A Qualitative Case Study*. University of Phoenix.
ITU (2021). *Definition of cybersecurity, referring to ITU-T X.1205, Overview of cybersecurity*. Available at: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx [Accessed 24 August 2021].
Janowitz, M. (1975). Sociological theory and social control. *American Journal of sociology* 81(1): 82-108.
Jeyaraj, A. and Zadeh, A. (2020). Institutional isomorphism in organizational cybersecurity: A text analytics approach. *Journal of Organizational Computing and Electronic Commerce* 30(4): 361-380.
Jhanjhi, N., Humayun, M. and Almuayqil, S.N. (2021). Cyber Security and Privacy Issues in Industrial Internet of Things. *Comput. Syst. Sci. Eng.* 37(3): 361-380.

Joffe, H. (2012). Thematic analysis. *Qualitative research methods in mental health and psychotherapy* 1.
Johnson, G., Whittington, R., Scholes, K., Angwin, D. and Regner, P. (2017). *Exploring strategy : text and cases*. Harlow, England: Pearson.
Johnson, R.B. (1997). Examining the validity structure of qualitative research. *Education* 118(2): 282.
Koskosas, I., Kakoulidis, K. and Siomos, C. (2011). A model performance to information security management. *International Journal of Business and Social Science* 2(4).
Kure, H. and Islam, S. (2019). Assets focus risk management framework for critical infrastructure cybersecurity risk management. *IET Cyber-Physical Systems* 4(4): 332-340.
Lawler III, E.E. and Suttle, J.L. (1973). Expectancy theory and job behavior. *Organizational behavior and human performance* 9(3): 482-503.
Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*.
Leidner, D.E. and Kayworth, T. (2006). A review of culture in information systems research: Toward a theory of information technology culture conflict. *MIS quarterly* 30(2): 357-399.
Liang, G., Weller, S.R., Zhao, J., Luo, F. and Dong, Z.Y. (2016). The 2015 ukraine blackout: Implications for false data injection attacks. *IEEE Transactions on Power Systems* 32(4): 3317-3318.
Lombardi, M., Pascale, F. and Santaniello, D. (2021). Internet of Things: A General Overview between Architectures, Protocols and Applications. *Information* 12(2): 87.
Lu, Y. (2018). Cybersecurity research: A review of current research topics. *Journal of Industrial Integration and Management* 3(04): 1850014.
Malatji, M., Von Solms, S. and Marnewick, A. (2019). Socio-technical systems cybersecurity framework. *Information & Computer Security*.
McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A.-R., Maniatakos, M. and Karri, R. (2016). The cybersecurity landscape in industrial control systems. *Proceedings of the IEEE* 104(5): 1039-1057.
Miller, T., Staves, A., Maesschalck, S., Sturdee, M. and Green, B. (2021). Looking back to look forward: Lessons learnt from cyber-attacks on Industrial Control Systems. *International Journal of Critical Infrastructure Protection* 35: 100464.
Minkov, M. and Hofstede, G. (2011). The evolution of Hofstede's doctrine. *Cross cultural management: An international journal*.
Nævestad, T.-O., Meyer, S.F. and Honerud, J.H. (2018). Organizational information security culture in critical infrastructure: developing and testing a scale and its relationships to other measures of information security. *Safety and Reliability–Safe Societies in a Changing World. Proceedings of ESREL 2018, June 17-21, 2018, Trondheim, Norway*.
Nasir, A., Arshah, R.A., Ab Hamid, M.R. and Fahmy, S. (2019). An analysis on the dimensions of information security culture concept: A review. *Journal of Information Security and Applications* 44: 12-22.
Nel, F. and Drevin, L. (2019). Key elements of an information security culture in organisations. *Information & Computer Security*.
NERC (2021). *Critical Infrastructure Protection Standards*. Available at: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx [Accessed 05 September 2021].
NIST (2006). *Glossary: information security*. Available at: https://csrc.nist.gov/glossary/term/information_security [Accessed 25 August 2021].
NIST (2017). *Glossary: Cybersecurity*. Available at: https://csrc.nist.gov/glossary/term/cybersecurity [Accessed 17 September 2021].
OECD (2005). The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries. DOI: doi:https://doi.org/10.1787/232017148827.
Ogden, S.E. (2021). CYBERSECURITY: CREATING A CYBERSECURITY CULTURE.

Okere, I., Van Niekerk, J. and Carroll, M. (2012). Assessing information security culture: A critical analysis of current approaches. *2012 Information Security for South Africa.* IEEE, 1-8.

Onumo, A., Cullen, A. and Ullah-Awan, I. (2017). An empirical study of cultural dimensions and cybersecurity development. *2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud).* IEEE, 70-76.

QSR (2020). *Nvivo qualitative data analysis software*. Available at: https://www.qsrinternational.com/nvivo-qualitative-data-analysis-software/about/nvivo [Accessed 29 November 2020].

Quinn, R.E., Hildebrandt, H.W., Rogers, P.S. and Thompson, M.P. (1991). A competing values framework for analyzing presentational communication in management contexts. *The Journal of Business Communication (1973)* 28(3): 213-232.

Rajivan, P. and Cooke, N. (2017). Impact of team collaboration on cybersecurity situational awareness. *Theory and Models for Cyber Situation Awareness*. Springer, pp.203-226.

Ramchunder, N. (2018). Communication Networks Branch Cyber Security Strategy.

Reegård, K., Blackett, C. and Katta, V. (2019). The Concept of Cybersecurity Culture. *29th European Safety and Reliability Conference.* 4036-4043.

Reid, R. and Van Niekerk, J. (2014). From information security to cyber security cultures. *2014 Information Security for South Africa.* IEEE, 1-7.

Reva, D. (2021). *Cyber attacks expose the vulnerability of South Africa's ports*. Available at: https://issafrica.org/iss-today/cyber-attacks-expose-the-vulnerability-of-south-africas-ports [Accessed 20 September 2021].

Robbins, S.P. and Judge, T.A. (2013). *Organizational behavior.* New Jersey: Pearson Education.

Robinson, O.C. (2014). Sampling in interview-based qualitative research: A theoretical and practical guide. *Qualitative research in psychology* 11(1): 25-41.

Rogers, R.W. (1975). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology* 91(1): 93-114.

SA Government Gazette (2015). *National Cybersecurity Policy Framework*. Available at: https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf [Accessed 10 August 2021].

Saleem, Y., Crespi, N., Rehmani, M.H. and Copeland, R. (2019). Internet of things-aided smart grid: technologies, architectures, applications, prototypes, and future research directions. *IEEE Access* 7: 62962-63003.

Salmons, J. (2012). Designing and Conducting Research with Online Interviews, Cases in Online Interview Research. *Pada http://sagepub. com/sites/default/files/upmbinaries/43888_1. pdf. Diakses Jumat* 17.

Sas, M., Hardyns, W., van Nunen, K., Reniers, G. and Ponnet, K. (2021). Measuring the security culture in organizations: a systematic overview of existing tools. *Security Journal* 34(2): 340-357.

Saunders, M., Lewis, P. and Thornhill, A. (2009). *Research methods for business students.* Pearson education.

Schein, E.H. (2010). *Organizational culture and leadership.* John Wiley & Sons.

Scott, J. (2000). Rational choice theory. *Understanding contemporary society: Theories of the present* 129: 671-685.

Spremić, M. and Šimunic, A. (2018). Cyber security challenges in digital economy. *Proceedings of the World Congress on Engineering.* 4-6.

Sutherland, E. (2017). Governance of cybersecurity-the case of South Africa. *The African Journal of Information and Communication* 20: 83-112.

Tang, M., Li, M.g. and Zhang, T. (2016). The impacts of organizational culture on information security culture: a case study. *Information Technology and Management* 17(2): 179-186.

The Presidency (2013). *Protection of Personal Information Act 4 of 2013*. Available at: https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf [Accessed 18 September 2021].

Thomson, K. and Van Niekerk, J. (2012). Combating information security apathy by encouraging prosocial organisational behaviour. *Information Management & Computer Security*.

Uchendu, B., Nurse, J.R., Bada, M. and Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security* 109: 102387.
van Muijen, J.J. and al, e. (1999). Organizational Culture: The Focus Questionnaire. *European Journal of Work and Organizational Psychology* 8(4): 551-568.
Van Niekerk, J. and Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security* 29(4): 476-486.
Van‘t Wout, C. (2019). Develop and maintain a cybersecurity organisational culture. *ICCWS 2019 14th International Conference on Cyber Warfare and Security: ICCWS*.
Von Solms, R. and Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security* 38: 97-102.
Watt, D. (2007). On becoming a qualitative researcher: the value of reflexivity. *Qualitative Report* 12(1): 82-101.
Williams, K.R. and Hawkins, R. (1986). Perceptual research on general deterrence: A critical review. *Law and Society Review*. 545-572.
Yildirim, E. (2016). The importance of information security awareness for the success of business enterprises. *Advances in human factors in cybersecurity*. Springer, pp.211-222.

APPENDIX A: INTERVIEW SCHEDULE

UNIVERSITY OF KWAZULU-NATAL
GRADUATE SCHOOL OF BUSINESS AND LEADERSHIP

MBA Research Project
Researcher: Naren Ramchunder ([redacted])
Supervisor: Dr Xoliswa Majola (0312607680)
Research Office: Ms Mariette Snyman (031 260 8350)

Exploring the role of eThekwini Electricity Unit leadership in establishing an effective organisational cybersecurity culture

Interview Questions

1. Organisational cybersecurity culture

1.1. What are the cybersecurity challenges facing electric utilities such as eThekwini Electricity?
1.2. Do you feel that the cybersecurity implementations at the Electricity Unit have adequately addressed these challenges? Please elaborate.
1.3. What would you regard as external influences that shape the cybersecurity culture at eThekwini Electricity?
1.4. Are there any formal or informal cybersecurity teams/groups or inter-departmental collaboration on maters of cybersecurity? If so, what are they? If not, why do you think they don't exist?
1.5. How do you think the Electricity Unit can secure against cybersecurity attacks aimed at exploiting human vulnerabilities?
1.6. In your opinion what is the current state of the organisational cybersecurity culture at eThekwini Electricity?

2. Leadership role in developing the current cybersecurity culture

2.1. What do you believe influences employees to protect and defend the organisation against cybersecurity attacks?
2.2. How are employees made aware of the cybersecurity policies and practices of the organisation? Is this adequate? Please elaborate.
2.3. Have you been personally involved in cybersecurity related activities such as strategies, projects, training etc? Please elaborate.
2.4. Have you made cybersecurity initiatives a priority for the organisation? How was this achieved? Please elaborate.
2.5. How knowledgeable are you about cybersecurity in the organisation? Do you have any skills, competencies, or knowledge about cybersecurity and the vulnerabilities of the organisation?
2.6. What managerial levers can be used to influence the cybersecurity culture of the organisation? Please provide examples.
2.7. How do you view the role of leadership in cultivating a cybersecurity culture eThekwini Electricity?

3. Recommendations for improving the organisational cybersecurity culture

3.1. What recommendations can you suggest that will improve the organisational cybersecurity culture at the eThekwini Electricity Unit?

3.2. In your opinion, what can leaders do to contribute to the improvement of the organisational cybersecurity culture at the eThekwini Electricity Unit?

3.3. Is there anything else that you would like to add that may contribute to this study?

APPENDIX B: INFORMED CONSENT

UNIVERSITY OF KWAZULU-NATAL
GRADUATE SCHOOL OF BUSINESS AND LEADERSHIP

Dear Respondent,

MBA Research Project
Researcher: Naren Ramchunder ([redacted])
Supervisor: Dr Xoliswa Majola (0312607680)
Research Office: Ms Mariette Snyman (031 260 8350)

I, Naren Ramchunder am a Master of Business Administration (MBA) student, at the Graduate School of Business and Leadership, of the University of KwaZulu Natal. You are invited to participate in a research project entitled: "Exploring the role of eThekwini Electricity Unit leadership in establishing an effective organisational cybersecurity culture". The aim of this study is to explore the role of leadership in creating an effective organisational cybersecurity culture at eThekwini Electricity.

Through your participation I hope to understand to what extent does the role of leadership influence the development of an organisational cybersecurity culture at eThekwini Electricity. The results of the interview are intended to contribute to this field of research and to make recommendations to improve the organisational cybersecurity culture at the eThekwini Electricity Unit.

Your participation in this project is voluntary. You may refuse to participate or withdraw from the project at any time with no negative consequence. There will be no monetary gain from participating in this survey/focus group. Confidentiality and anonymity of records identifying you as a participant will be maintained by the Graduate School of Business and Leadership, UKZN.

The interview should take about 45 minutes to an hour. I hope you will take the time to participate.

Sincerely

Investigator's signature_____ Date_____

This page is to be retained by participant

UNIVERSITY OF KWAZULU-NATAL
GRADUATE SCHOOL OF BUSINESS AND LEADERSHIP

MBA Research Project
Researcher: Naren Ramchunder ([redacted])
Supervisor: Dr Xoliswa Majola (0312607680)
Research Office: Ms Mariette Snyman (031 260 8350)

CONSENT

I……(full names of participant) hereby confirm that I understand the contents of this document and the nature of the research project, and I consent to participating in the research project.
I understand that I am at liberty to withdraw from the project at any time, should I so desire.

I hereby consent/do not consent to record the interview.

SIGNATURE OF PARTICIPANT DATE

……

This page is to be retained by researcher

APPENDIX C: GATEKEEPERS LETTER

1 Jelf Taylor Crescent
Durban 4001

PO Box 147
Durban 4000

Tel: (031) 311 1111
Fax: (031) 311 9010

ETHEKWINI MUNICIPALITY
Trading Services Cluster
Electricity Unit

To: Maxwell Mthembu

REQUEST FOR PERMISSION TO PERFORM RESEARCH INTO EXPLORING THE ROLE OF ETHEKWINI ELECTRICITY UNIT LEADERSHIP IN ESTABLISHING AN EFFECTIVE ORGANISATIONAL CYBERSECURITY CULTURE

1. **Introduction**
   The purpose of this request is to obtain your approval to conduct research into exploring the role of eThekwini Electricity Unit leadership in establishing an effective organisational cybersecurity culture within the Electricity Unit of eThekwini Municipality. This study is towards partial fulfilment of the requirements for a Master's in Business Administration (MBA) qualification at the University of Kwa-Zulu Natal (UKZN).

2. **Background**
   Managing a modernised electrical grid that comprises of thousands of electrical substations requires sophisticated Industrial Control Systems (ICS) supported by robust communication networks. As the complexity of the system increases so too does the coupling between cyber and physical electrical components, increasing the vulnerability of the electrical grid to cyber attacks. Cyber attacks on critical infrastructure have been highlighted by the discovery of malware such as Stuxnet, that was designed to specifically target ICS. This highlights the need to address cybersecurity challenges facing electric utilities. However, using technical security controls on their own have shown to be ineffective in securing organisations, as many successful cybersecurity attacks have exploited human vulnerabilities. Creating an organisational cybersecurity culture that aims to align the values, attitudes and beliefs of the organisation with cybersecurity objectives is vital to effectively securing the organisation. This research is aimed at investigating the role of leadership in creating an effective organisational cybersecurity culture at the eThekwini Electricity Unit.

3. **Research Methodology**
   A qualitative research approach using semi-structured interviews will be used to gather empirical data to explore and gain insight into the role of eThekwini Electricity Unit leadership in establishing an effective organisational cybersecurity culture. Participants from various parts of the organisation will be selected to be interviewed. Participants shall be provided with an informed consent form, outlining the requirements and their decision to participate in the study.

4. **Financial Implications**
   There will be no direct financial implications that will be incurred by eThekwini Electricity during this research.

5. **Confidentiality**
   All information collected and analysed during this research will be treated as confidential. The research will only be used as partial fulfilment of the requirements towards my MBA qualification. The researcher shall maintain the anonymity of participants and confidentiality of data according to the Protection of Personal Information Act.

6. **Conclusion**
   This research will provide further insight into addressing the cybersecurity challenges facing eThekwini Electricity by fostering a culture of organisational cybersecurity. In examining the current state of organisational cybersecurity and determining the key challenges inhibiting its development, leadership within the organisation can better equip themselves to shape the values, attitudes and beliefs of the organisation with the cybersecurity objectives, effectively securing the organisation. Results from this study may be used to improve policy and decision making within the Unit. Furthermore, this study will also benefit other electrical utilities in South Africa and abroad that face similar challenges in securing their organisations against cybersecurity attacks aimed at exploiting people.

I hope that my request to conduct this research will be reviewed and granted.

Date: 09/07/2021

[redacted]

Naren Ramchunder
Student number: 205500531

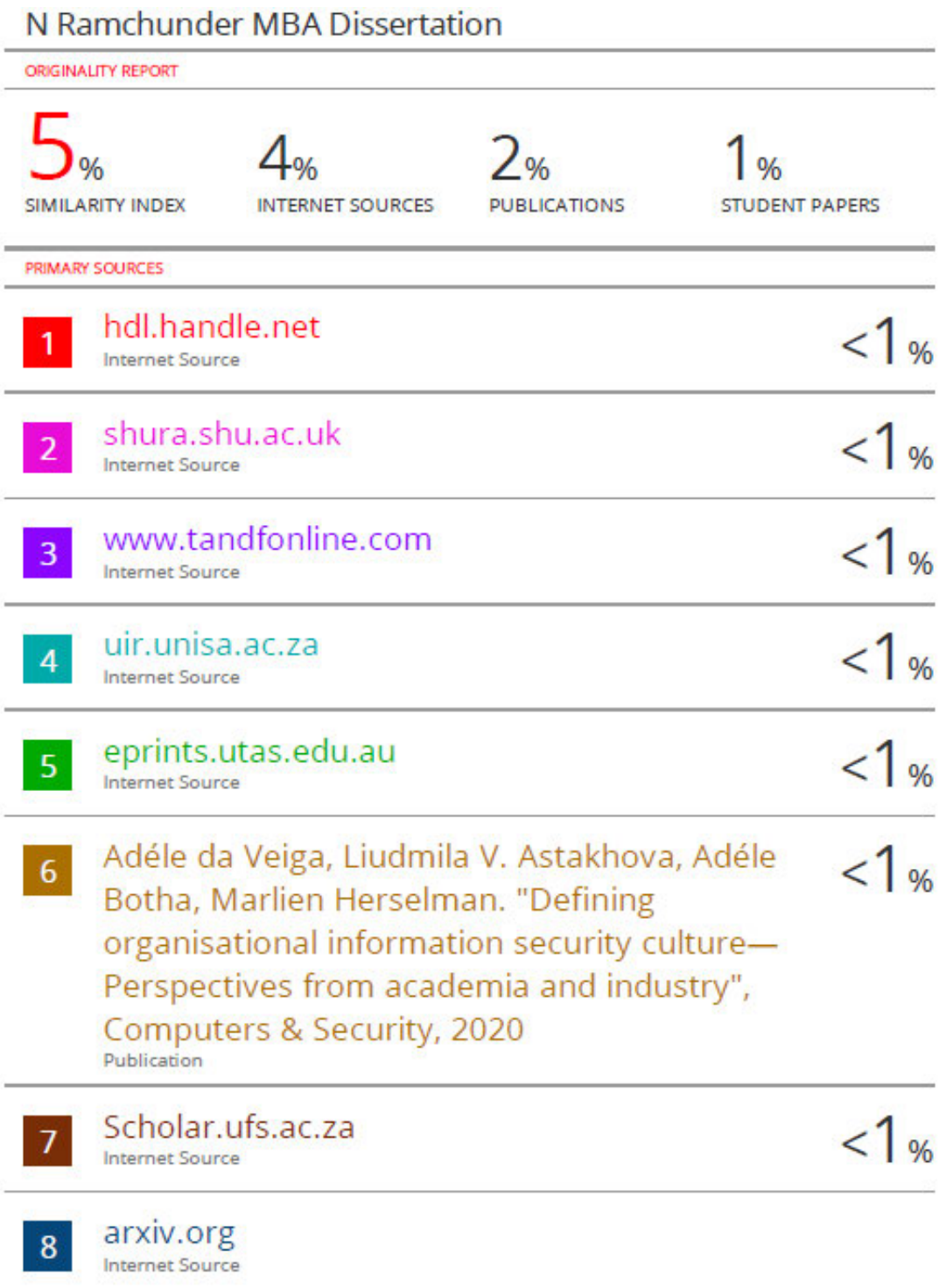
I Maxwell Mthembu, hereby **give** / ~~**do not give**~~ permission for Naren Ramchunder (Student number 205500531) to conduct this research.

Date: 2021-07-21

[redacted]

Maxwell Mthembu
Head: Electricity Unit

APPENDIX D: TURNITIN REPORT



N Ramchunder MBA Dissertation

ORIGINALITY REPORT

5%	4%	2%	1%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	hdl.handle.net Internet Source	<1%
2	shura.shu.ac.uk Internet Source	<1%
3	www.tandfonline.com Internet Source	<1%
4	uir.unisa.ac.za Internet Source	<1%
5	eprints.utas.edu.au Internet Source	<1%
6	Adéle da Veiga, Liudmila V. Astakhova, Adéle Botha, Marlien Herselman. "Defining organisational information security culture—Perspectives from academia and industry", Computers & Security, 2020 Publication	<1%
7	Scholar.ufs.ac.za Internet Source	<1%
8	arxiv.org Internet Source	

APPENDIX E: ETHICAL CLEARANCE CERTIFICATE

UNIVERSITY OF KWAZULU-NATAL
INYUVESI YAKWAZULU-NATALI

05 September 2021

Mr Naren Ramchunder (205500531)
Grad School Of Bus & Leadership
Westville campus

Dear Mr Ramchunder,

Protocol reference number: HSSREC/00003268/2021
Project title: Exploring the role of eThekwini Electricity Unit leadership in establishing an effective organisational cybersecurity culture
Degree: Masters

Approval Notification – Expedited Application

This letter serves to notify you that your application received on 26 August 2021 in connection with the above, was reviewed by the Humanities and Social Sciences Research Ethics Committee (HSSREC) and the protocol has been granted FULL APPROVAL.

Any alteration/s to the approved research protocol i.e. Questionnaire/Interview Schedule, Informed Consent Form, Title of the Project, Location of the Study, Research Approach and Methods must be reviewed and approved through the amendment/modification prior to its implementation. In case you have further queries, please quote the above reference number. PLEASE NOTE: Research data should be securely stored in the discipline/department for a period of 5 years.

This approval is valid until 05 September 2022.
To ensure uninterrupted approval of this study beyond the approval expiry date, a progress report must be submitted to the Research Office on the appropriate form 2 - 3 months before the expiry date. A close-out report to be submitted when study is finished.

All research conducted during the COVID-19 period must adhere to the national and UKZN guidelines.

HSSREC is registered with the South African National Research Ethics Council (REC-040414-040).

Yours sincerely,

[redacted]

Professor Dipane Hlalele (Chair)

/dd