

https://dspace.org/

The role of leadership in cybersecurity culture within the South African financial services

Mataruse, Robert Tutsirayi

2020
https://hdl.handle.net/10539/30074

Downloaded from a DSpace repository. https://dspace.org/

The role of leadership in cybersecurity culture within the South African financial services

Robert Tutsirayi Mataruse

A research report submitted to the Faculty of Commerce, Law and Management, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Management in the field of Digital Business

Johannesburg, 2020

(Version 2019-2020)

ABSTRACT

The purpose of this study is to explore the role of leadership in cybersecurity culture within the South African financial services sector. The study is based on a qualitative case study on one of South Africa's major financial services institution. The organisation in this study processes large volumes of transactional data containing personally identifiable information daily and is currently undergoing a massive organisational transformation aligned to its new strategy.

Face to face semi-structured interviews conducted with senior managers in the organisation served as the primary source of data collection. The interviews were recorded and transcribed for analysis. Publicly available documents and observations of the context provided secondary data sources.

The findings of the study show that awareness education is critical in the communication and creation of a common and shared understanding of the cybersecurity risks and expected behaviour and attitudes. The development of a shared understanding within an organisation is critical to the development of desired behaviours and norms and in turn, culture. The leadership reinforces the awareness message for desired behaviour by being exemplary and authentically living out the values through their leadership style. The leaders' leadership styles vary on the transactional-transformational leadership continuum.

The organisation has a well-formed compliance culture for risk mitigation. Cybersecurity is an emerging risk type making the development of cybersecurity culture complementary to the existing compliance culture. Due to the qualitative nature of this single case study, the results are not representative of all organisations in the sector; however, they can be used to evaluate how other organisations are developing cybersecurity culture both within and without the sector.

KEYWORDS

Cybersecurity culture, Leadership, Leadership style, Organisational culture, Organisational design, Change management

DECLARATION

I, Robert T. Mataruse, declare that this research report is my own work except as indicated in the references and acknowledgements. It is submitted in partial fulfilment of the requirements for the degree of Master of Management in the field of Digital Business at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination at this or any other university.

Name:Robert T. Mataruse Signature:

Signed at ……

On the ……31st……day of ……March…… 2020

DEDICATION

I dedicate my dissertation work to my family and many friends. A special feeling of gratitude to my loving mum, whose words of encouragement and push for tenacity ring in my ears. My wife Nyasha who has never left my side during the journey and is very special and dear.

I also dedicate this dissertation to my many friends and colleagues who have supported me throughout the process. I will always appreciate all they have done, especially Anesu Marufu for introducing me to cybersecurity, Wendy Chin’ono and David Karadzandima for the many hours of last-minute proofreading of both the proposal and final report.

I dedicate this work and give special thanks to my friend Grant Chivandire and Caitlyn J. Chetty for being there for me throughout the entire master's program. Both of you have been my best cheerleaders.

ACKNOWLEDGEMENTS

I would like to express thanks and gratitude to all the people who availed themselves and contributed to the successful completion of this research report. A special thanks to my supervisor Dr Kiru Pillay for providing me with the necessary guidance and direction along the journey from the inception to the completion of this research report. You were a source of encouragement and a great sounding board, thank you for your patience and insights that made the journey tolerable.

I would like to acknowledge and thank Wits Business School for allowing me to conduct my research and providing any assistance requested. Special thanks go to the members of the Chair for Digital Business, especially Mrs Ayanda Magida for her guidance and encouragement when I came close to giving up due to work demands that required more attention.

I would like to acknowledge and thank the senior managers at Absa Group Ltd, that agreed to participant and avail time for this study. It is through your generosity with your time and patience that this research was made possible. To Mr K.L.M Makoni thank you for opening the doors and introductions to your Absa colleagues and your continued support.

Finally, I would like to thank my colleagues at Deloitte for providing an audience to test some of my thinking during the drafting of the report. Their excitement and willingness to provide feedback made the completion of this research an enjoyable experience.

TABLE OF CONTENTS

ABSTRACT ..... **ii**

DECLARATION ..... **iii**

DEDICATION ..... **iv**

ACKNOWLEDGEMENTS ..... **v**

LIST OF TABLES ..... **ix**

LIST OF FIGURES ..... **x**

LIST OF ACRONYMS ..... **xi**

CHAPTER 1. INTRODUCTION **12**

1.1 PURPOSE OF THE STUDY 12

1.2 CONTEXT OF THE STUDY 12

1.2.1 COUNTRY OVERVIEW 12

1.2.2 SOUTH AFRICAN FINANCIAL SERVICES SECTOR 12

1.2.3 ABSA GROUP LIMITED 14

1.2.4 CYBER RISK AS AN EMERGING OPERATIONAL RISK 15

1.3 RESEARCH PROBLEM 16

1.4 RESEARCH QUESTIONS 17

1.5 THEORETICAL FRAMEWORKS 18

1.5.1 THE ORGANISATION AS AN OPEN SYSTEM 18

1.5.2 ORGANISATIONAL LEVEL DIAGNOSIS – STRATEGIC ORIENTATION 20

1.6 SIGNIFICANCE OF THE STUDY 24

1.7 DELIMITATIONS OF THE STUDY 25

1.8 ASSUMPTIONS 25

CHAPTER 2. LITERATURE REVIEW **27**

2.1 INTRODUCTION 27

2.2 CYBERSECURITY 28

2.2.1 INFORMATION SECURITY 28

2.2.2 CYBERSECURITY 28

2.3 RESEARCH QUESTION 1: WHAT TYPE OF ORGANISATIONAL CULTURE SUPPORTS A CYBERSECURITY CULTURE? 30

2.3.1 CULTURE 30

2.3.2 ORGANISATIONAL CULTURE 30

2.3.3 SAFETY CULTURE 31

2.3.4 Cybersecurity Culture 32
2.4 Research Question 2: How does the leadership develop and sustain a cybersecurity culture within an organisation? 33
2.4.1 Leadership 33
2.4.2 Leadership styles 34
2.4.3 Change management 36
2.4.4 Leadership style and change management 38
2.4.5 Organisational design 39
2.5 Conclusion of the Literature Review 40

CHAPTER 3. RESEARCH METHODOLOGY 41

3.1 Research approach 42
3.2 Research design 44
3.2.1 Case Study 45
3.3 Data collection methods 46
3.4 Population and sample 47
3.4.1 Population 47
3.4.2 Sample and sampling method 47
3.5 The research instrument 49
3.6 Procedure for data collection 51
3.6.1 Data gathering process 51
3.7 Data analysis and interpretation 52
3.8 Validity and reliability 53
3.9 Demographic profile of respondents 54
3.10 Ethical considerations 56

CHAPTER 4. FINDINGS 57

4.1 Introduction 57
4.1.1 Coding Analysis 57
4.2 Results of research question 1 61
4.2.1 Underlying Assumptions 62
4.2.2 Artefacts 63
4.2.3 Espoused values 63
4.2.4 Observations 65
4.2.5 Conclusion for research question 1 65
4.3 Results of research question 2 66
4.3.1 Leadership theme 66
4.3.2 Organisational design theme 69
4.3.3 Observations 79
4.3.4 Conclusion for research question 2 79
4.4 Summary of the findings 79

CHAPTER 5. DISCUSSION OF THE FINDINGS 80

5.1 Introduction 80
5.2 Discussion on Research Question 1 81

5.2.1 Organisational culture 81
5.3 Discussion on Research Question 2 87
5.3.1 Leadership 87
5.3.2 Organisational Design 89
5.4 Conclusion 93

CHAPTER 6. CONCLUSIONS & RECOMMENDATIONS 96

6.1 Introduction 96
6.1.1 Summary of the research process 96
6.2 Conclusions regarding research: Question 1 97
6.3 Conclusions regarding research: Question 2 99
6.4 Recommendations 100
6.4.1 Practitioners 100
6.4.2 Academics 101
6.5 Suggestions for further research 101
6.6 Conclusion 102

REFERENCES 104

APPENDIX (A) Interview Request Letter 116

APPENDIX (B) Participant's Information Sheet Error! Bookmark not defined.

APPENDIX (C) Participant Agreement Form 117

APPENDIX (D) Instrument 118

APPENDIX (E) Qualitative Coding 121

APPENDIX (F) Ethics Approval 127

LIST OF TABLES

Table 1 Inclusion & Exclusion Criteria 48

Table 2: Profile of participants 49

Table 3: Demographics of respondents 55

Table 4: Coding analysis output 60

Table 5: Findings summary 61

Table 6: Organisational culture-related sentiment codes 62

Table 7: Leadership related codes 66

Table 8: Technology related codes 70

Table 9: Structure related codes 73

Table 10: Management Systems Related Codes 73

Table 11: Human Resources Systems Codes 79

LIST OF FIGURES

Figure 1: Organisation as an Open System 19

Figure 2: Organisational Strategic Orientation Framework 20

Figure 3: Kotter's 8-Step Change Model 24

Figure 4: Coding analysis approach 58

Figure 5: A modified Kotter’s Organisational Change Model 82

Figure 6: The Divisions of the Organisation 90

Figure 7: The Group’s Security Functional Structure 90

LIST OF ACRONYMS

ARO……..Africa Regional Offices

BCM……..Business Continuity Management

CDO…….Chief Digital Officer

CE……..…Chief Executive

CEO…….….Group Chief Executive Officer

CIB……..…..Capital and Investment Banking

CIO……..…..Chief Information Officer

CRO……..….Chief Risk Officer

CSI……....Corporate Social Initiatives

CSO……..Chief Security Officer

CVF……...Competing Values Framework

ENISA……..……European Agency for Cybersecurity

ERM……....Enterprise Risk Management

Exco……..…Executive Committee

FD……..Financial Director

RBB……Retail and Business Banking

SABRIC…….South African Banking Risk Information Centre

SARB……South African Reserve Bank

CHAPTER 1. INTRODUCTION

1.1 Purpose of the study

The purpose of this research case study was to explore the role of leadership in developing a cybersecurity culture in the financial services in South Africa.

1.2 Context of the study

1.2.1 *Country Overview*

The South African economy has been growing from 0.8 to 1.3% between 2017 and 2019 and expected to rise to 1.7% in 2020, Treasury (2019). Mining and agriculture are the main drivers of the economy, and its fortunes are therefore tied to the commodity prices which have been subdued over the last few years, Treasury (2019). The financial services sector is an essential contributor to the economy accounting for 2.7% of the GDP in 2019, Treasury (2019). This industry is one of the most advanced in Africa, boasting of world-class institutions and infrastructures.

1.2.2 *South African financial services sector*

The South African financial services industry is highly regulated, and this has ensured its stability and increased barriers of entry for new entrants and reduced growth opportunities for small and medium-sized banks. The banking part of the financial services sector comprises more than 40 banks, with the top five banks accounting for 90% of the sector's assets, BMI (2017). Banking licenses determined under the Banks Act, 1990, one of the mandates of the South African Reserve Bank, which enforces high rigour in ensuring the compliance and stability of the banks. The stringent requirements have meant that very few banks have been able to be registered in the country. Critiques of the South African financial services sector argue that the sector's robust regulatory environment

promotes stability at the cost of innovation, competition, and efficiencies, BMI (2017).

The financial services sector under the Financial Sector Regulation Act, 2017 is regulated by two bodies, namely the Prudential Authority – for the regulation of compliance and prudential requirements as set out in the Basel Committee on Banking Supervision, and the Financial Sector Conduct Authority (FSCA) – regulating market conduct and the safety of financial customers.

The sector has been facing considerable challenges over the last few years. The World Bank (2020) report indicates the slow and declining economic growth rate that the country has experienced over the previous ten years. The declining growth rate has led to increased unemployment levels and widening inequality that has excluded about 23% of the population from formally engaging with the financial services sector, Intellidex (2018). The increasing number of financially marginalised people has created opportunities for the smaller banks and new entrants targeting the excluded population through innovative and customer-centric business models that seek to exploit technology to provide digitally diverse and easily accessible products. These include Capitec and the new entrants, namely TymeDigital, Discovery Bank and Bank Zero who are all technology-based banks focusing primarily on transactional banking. Telecommunications companies, through their mobile money services geared at payments, are also threatening the larger banks in the retail banking space, Roopnarain (2019).

The major banks are adopting more customer-centric strategies that leverage their reach, resources, and brand. These customer-centric strategies have seen a massive push towards digital transformation within these larger banks. The change in approach has led to significant closing-down entirely or downsizing of the physical branches in response to changing customer behaviour that is in favour of digital channels of online and mobile banking, Moneyweb (2019). The downsizing of branches has seen these banks falling to almost half of the peak number of branches; the need for operational efficiencies mainly drives this. The cost of running a traditional branch is more expensive than that of technology-based banking. These larger banks are aggressively pushing the migration of customers towards digital platforms, and this has seen intensive efforts in

modernising the technology infrastructure – a trend set to continue into the foreseeable future, Coetzee (2019).

Banks are also facing increasing competition from Fintech start-ups focusing on aspects of the value chain such as payments, lending, deposits, asset management and even advisory services. The Fintech offerings are limited to parts of the value chain, exempting from the same levels of compliance and regulatory requirements as the large banks.

A key challenge facing the sector is a skills shortage for the required competencies for the migration to technology-based operating models. The lack of expertise has led to institutions aggressively seeking strategies and incentives to retain their skilled employees.

1.2.3 *Absa Group Limited*

Absa is one of the top financial services companies in South Africa with an asset base of R1.3trillion, Reuters (2020). Absa offers retail, business, corporate, investment banking and wealth management, as well as insurance products and services. It also has operations across 12 other African countries and is a listed entity on the Johannesburg stock exchange, Absa (2020).

Barclays PLC acquired a controlling stake of 62% in Absa in 2005 and rebranded it, Barclays Africa, cementing its presence on the continent with operations in 12 countries (BusinessTech 2019 and Absa, 2019). In 2017 Barclays PLC reduced its shareholding in Barclays Africa to about 14.8% with the Absa Group becoming the majority shareholder.

The reduction in shareholding led to the uncoupling of the Absa Group from Barclays PLC's operational and information technology. The separation of the Absa Group from Barclays Plc is expected to be completed in 2020. Along with the systems, the separation has seen the brand transitioning from Barclays Africa to Absa Group for operation in other African countries. The split involved the creation and embedding of new brand identity and culture. The separation from Barclays Plc allowed Absa Group to make a significant strategic and cultural reset

to enable it to be relevant to its customer base. One of the core strategic objectives in the Group's current 2019 – 2021 strategy is to build a scalable digitally-led business Absa Group Limited (2020).

Absa Group has noted the impact of the increasing competition from the new technology-based entrants to the market as a threat to their relevance for its customers and its ability to remain competitive, Absa Group Limited (2019). Absa acknowledges the potential impact of Fintech start-ups and the digitally-led new entrants on customer behaviour. Absa's objective includes building a brand with a focus on innovative products delivered via scalable digital platforms.

Together with the adoption of the new business model to be a technology-led bank comes with an increased risk of cyber-attacks, fraud and financial crimes. The separation combined with strategic organisational change also comes with the inherent business, people and reputational risks. To mitigate these risks and threats the group has put in place processes and technologies to monitor, detect, prevent and manage the risk, the adoption of an Enterprise Risk Management Framework. The framework sets out activities, tools, techniques and practices to;
(i) comply with regulatory frameworks, and to

(ii) identify and manage material risks.

1.2.4 *Cyber risk as an emerging operational risk*

Operational risk may result in losses due to inadequate or failed internal processes, people and systems (technology) or external events, Absa Group Limited (2019). An organisation faces many of these operational risks every day. Operational risks are predominantly due to failures and weaknesses in an organisation's processes and procedures, identified and reported on using risk-audits, Matthews (2008).

As Absa transforms into a technology-led bank, this increases the cybersecurity risk - an operational risk that needs to be actively monitored and tracked. Absa has elevated cyber risk from an operational risk under technology risk to a stand-alone principle risk (non-financial) reported on separately. The Group is making

a significant investment into systems and ensuring world-class processes and procedures are in place to mitigate the cybersecurity risk. Thus, their effectiveness may be measured and quantified. The return on investment in reducing the people risk, especially of employees, and its effectiveness is hard to measure and quantify, and only visible through a change in behaviour and mindset. However, human behaviour presents a weak link in the security chain.

This study seeks to explore how organisational leaders develop and sustain a behaviour-based approach to cybersecurity. The motivation of this study is to understand the critical mechanism in building, embedding and sustaining a cybersecurity culture of an organisation.

1.3 Research problem

South Africa remains one of the countries with the highest number of cyber-attacks according to a South African Banking Risk Information Centre, SABRIC report, SABRIC (2019). Malware is the most common form of attack; however, ransomware attacks are also on the rise at a rate of 10% in 2019 CISOMAG, (2020) and 80% of successful cyberattacks exploit the human element (Ray et al., 2019). Attack vectors that exploit the human element employ more elaborate and sophisticated social engineering schemes increasingly (Ray et al., 2019). Human weaknesses susceptible to social engineering attacks are the most prevalent causes of reported cyber incidents, Mimecast (2020). These include breaches by employees as internal perpetrators or as victims of weaknesses due to complacency or lack of awareness of cybersecurity risks and methods of mitigating them. Mobile attacks provide a vector for credential attacks. The impact of a successful cyber breach includes relationship and reputational damage, emotional, financial and legislative costs.

The majority of the organisations, including those in the financial services sector, treat cybersecurity as a component of information security and rely on current compliance and control mechanisms for managing cyber risk. Compliance does not mean security, and there is a need to change the ways of working as well as the attitude and behaviour towards cybersecurity – a culture shift.

The South African financial services sector and the banking industry, in particular, is one of the areas of the economy, leading the charge in the digital revolution, FitchSolutions (2020). All the major banks are at various degrees of implementing their digital strategies ranging from focusing on customers to operational efficiencies and changing their business models altogether, FitchSolutions (2020). Organisations in this sector deal with large volumes of both transactional and personally identifiable data making them a prime target for cyberattacks and breaches, SABRIC (2019). As such, cyber risk is a high priority emerging with a lot of investment in cybersecurity technology and process and procedure best practice.

Insider threats due to either malicious or accidental acts provide the most significant risk to an organisation's cyber assets, whether the organisation is transforming into a digital business or is a digital-native business, Decisions (2020). The use of behaviour-based approaches to mitigating risks of insider threat requires changes in the ways of working and expected actions and attitude towards security, Reid & Van Niekerk, (2014b). Changing an organisation's culture, making it more aligned to security – cybersecurity – and changing the mindset is an effective way of mitigating the risks associated with insider threats. The new behaviours, attitudes and norms concerning cybersecurity based on the mindset shift make it everyone's responsibility to protect the organisation's cyber-physical assets. The change in attitudes and actions transforms all employees into the first line of defence – a human firewall.

This study seeks to explain the role of leadership in creating an organisation that enables and maintains a culture shift towards an increased security consciousness throughout the organisation.

1.4 Research questions

Organisations have a dominant personality, the organisational culture and multiple subpersonalities-subcultures that have additional unique values to the organisational culture. Cybersecurity culture exists as a subculture within an organisation that is distinctively identifiable through its promotion of vigilance and

safe cybersecurity hygiene integrated seamlessly into the organisation's ways of work. Understanding the existence of a cybersecurity culture within an organisation requires an understanding of the organisation's culture and how it influences its many subcultures. This study, in part, seeks to explore the relationship between organisational culture and a cybersecurity subculture as determined by research question 1.

The leadership of an organisation are critical change agents for transformative organisational change. The leaders' personalities and leadership style have a strong influence on the outcome of the organisational change and the attitudes of the followers to the change. The change management approach adopted is also vital. The study also considers the role of leadership in managing change and sustaining the new behaviours of the members of the organisation as highlighted by research question 2.

The study explores the following two research questions.

1. What type of organisational culture supports a cybersecurity culture?
2. How does the leadership build and embed a cybersecurity culture within an organisation?

1.5 Theoretical frameworks

1.5.1 *The organisation as a closed system*

Organisations act as closed systems comprising of different components and include business units, departments, functional and operational teams and individuals. These need to work together to achieve the organisation's desired goal or strategy. Cummings & Worley (2009)'s closed system model states that organisations operate in larger environments that affect how they perform and achieve their goals and strategies.

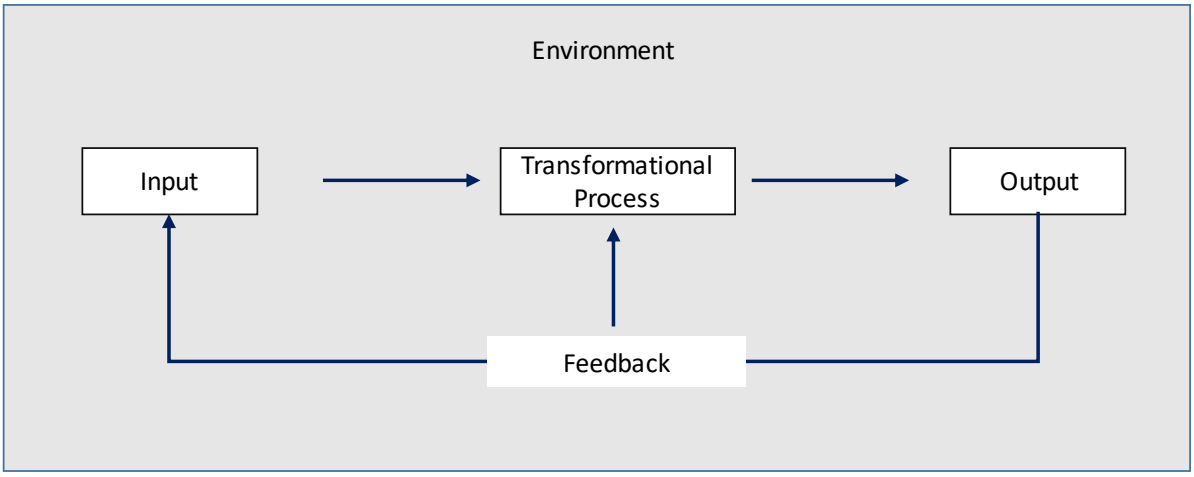


Figure 1: Organisation as a Closed System, Cummings & Worley (2009)

The environment is everything external to the organisation that may directly or indirectly influence the performance of the system. For the organisation, the environment primarily comprises of the macro-economy. The organisation is continuously sensing and exchanging information and resources with the environment to monitor and mitigate any changes that might arise (Cummings & Worley, 2009, p. 111).

The inputs converted into desired output through the transformational process. The transformational process comprises social and technology components with the social part focusing on the people and the technology on the tools and processes required for the conversion of the inputs into outputs.

The achievement of the desired goal and strategic performance results is the output of the transformational process and is sent to the environment (Cummings & Worley, 2009, p. 92).

The feedback mechanism comprises information from the results of the output that is channelled back into the organisation as a form of control mechanism. It provides information to the organisation as to how well the transformational process is working to meet the strategy and whether interventions may be required to improve the performance (Cummings & Worley, 2009, p. 92).

An effective transformational process, in part, is dependent on the degree to which the components of the organisation are aligned to achieve the desired goal

or strategy. Alignment concerns the relationship between the various parts of the system – organisation.

1.5.2 *Organisational Level Diagnosis – Strategic Orientation*

To understand the role of leadership in building a sustainable cybersecurity culture within an organisation, a diagnosis of the organisational system design is necessary. The open system model is used to diagnose the overall organisation's strategy, people, processes, technology and performance. Figure 2 below shows the standard input, transformational process (design components) and output elements considered for an organisational level diagnosis. The transformational process represents the way the organisation implements its intended strategy to achieve the desired output. According to Cameron & Green (2009), Kotter's organisational dynamic provides the framework for the organisational level diagnosis to understand how it is implementing its strategy. The organisation's leadership is not only critical in the strategy formulation in response to environmental stimuli but also in the implementation of the strategy. Organisational change approach, according to Brisson-Banks (2010) provides a more practical approach to the strategy implementation process in which the leadership exemplifies the desired behaviours.

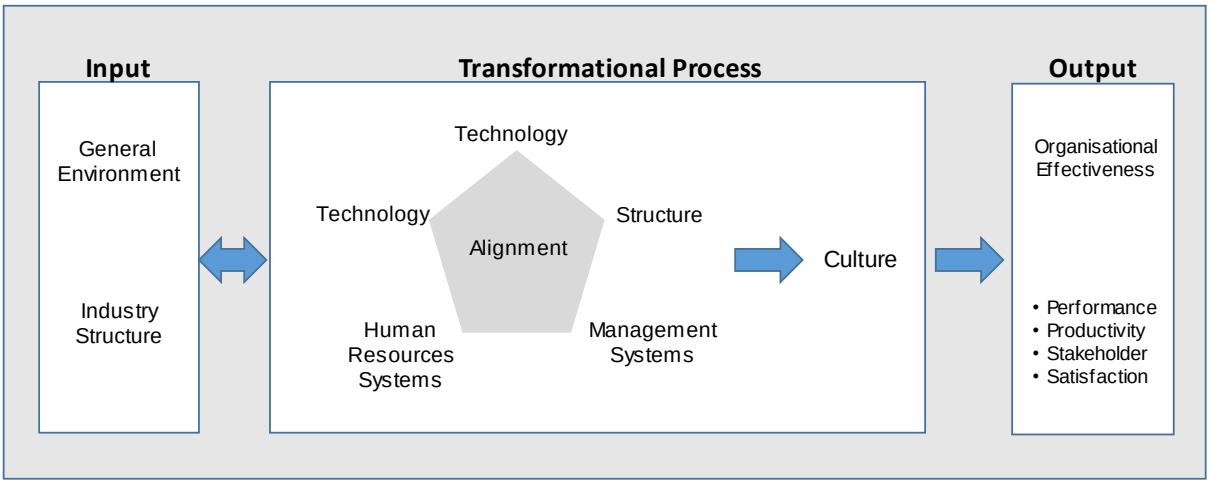


Figure 2: Organisational Strategic Orientation Framework Cummings & Worley (2009)

The environment provides the input of the strategic orientation of an organisation. It also comprises the general environment and the task environment, Cummings & Worley (2009). The general environment includes all the external forces that may influence an organisation's performance and effectiveness. These external forces include effects due to micro and macro socio-economic factors. Porter's Five Forces framework defines the forces due to the industry structure/ task, and these include supplier power, buyer power, competition among rivals, the threat of new entrants and substitutes. When combined, Porter's Five Forces can cause a potential risk to the success of an organisation. The rate of change and the complexity of the environment (general and task) are vital considerations in the decision-making process for organisations on how to respond to environmental stimuli. Organisations need to respond appropriately to environmental pressures by perceiving their environment. The core beliefs and values held by the organisation inform the way an organisation understands its situation. This perceived environment is the enacted environment. For an adequate response to the environment, the organisation's enacted environment should accurately represent the general and task environments.

The way organisations respond to environmental stimuli is influenced by the varying degrees of information uncertainty and resource dependence, Cummings & Worley (2009). These two factors highlight the degree to which the operational environment constraints organisations. The speed of responsiveness required increases, with the increase in the degree of information uncertainty and resource dependence. The financial services sector is one such sector characterised by high levels of information uncertainty (market & currency volatility) and resource dependence (skills shortage) and is required to be highly responsive. The ability to respond timeously and appropriately is critical for organisations to remain relevant to their customers due to increased competition from both traditional and non-traditional competitors.

The transformational process in Figure 2 above illustrates the five design components – strategy, technology, structure, management systems and human resources systems- which is key in the transformation of inputs into the target goal, Cummings & Worley, (1989). Culture is an intermediary output and a vital

component of the transformational process's design components. The effective alignment of the design component to the inputs, the environment and each other enables the organisation to deliver on its strategic goal and performance. A closer look at the design components:

1. Strategy defines how an organisation allocates and deploys resources (people, capital and technology) to achieve the organisation's target goals and gain a competitive advantage. The organisation's mission statement, goals and objectives, strategic intent and functional policies articulate an organisation's strategy.

2. Technology refers to the tools, processes and systems utilised by an organisation in the delivery of the desired outputs from inputs. Technology is at the centre of the transformational process.

3. The structure defines how the configuration of the organisation for optimum exploitation of its human resources is to achieve its strategic objectives. The configuration is dependent on the tasks and effort required and the level of maturity of the employees.

4. Management systems are responsible for capturing, analysing and reporting on the organisation's operational activities and performance, and as such act as a form of control mechanism for managing deviations from the expected target. Effective management systems support the organisation's structure and are closely linked to the organisation's strategic objectives. These systems need to provide reliable, timely and trusted information useful for aiding in the decision-making process for operational improvements.

5. Human resources systems are involved in the complete employee lifecycle from selecting, hiring, rewarding, developing and exiting. The incentive mechanism employed by the organisation is coupled with the management system as the incentives are allocated based on achieving the agreed key performance indicators, KPIs monitored and tracked by the management systems.

6. Culture is the final design component that defines the commonly shared beliefs, norms and attitudes within the business. It also dictates how organisations accomplish their objectives through their established ways of working. Since culture is intangible, it is difficult to measure and quantify and often overlooked as part of the strategic orientation. Developing the right culture and creating an appropriate climate to embed and nurture it are critical in developing the behaviours necessary for the organisation to succeed. Culture is vital in aligning the employees to the organisation's goals. Culture is also the most difficult to change design component and therefore presents a constraint in the strategy implementation process. An understanding of the organisation's culture and how it aligns to the other design components are significant in explaining the organisation's performance and effectiveness, Cummings & Worley (2009).

The output of the strategic orientation framework consists of three categories, namely:

1. Organisational performance – concerns financial output.
2. Organisational productivity – refers to the internal measurement of efficiency.
3. Stakeholder satisfaction – refers to how well the organisation is meeting the stakeholder expectation.

Core to the effectiveness of the organisation's strategic orientation is its alignment with the inputs and how the design components align with each other, Cameron & Green (2009).

Kotter (2012)'s model for leading change provides the theoretical framework for the creation of the required alignment between the strategic orientation, environment, input, and design components. The eight stages of the model are clustered along with the three categories, as shown in figure 3 below and are concerned with the following:

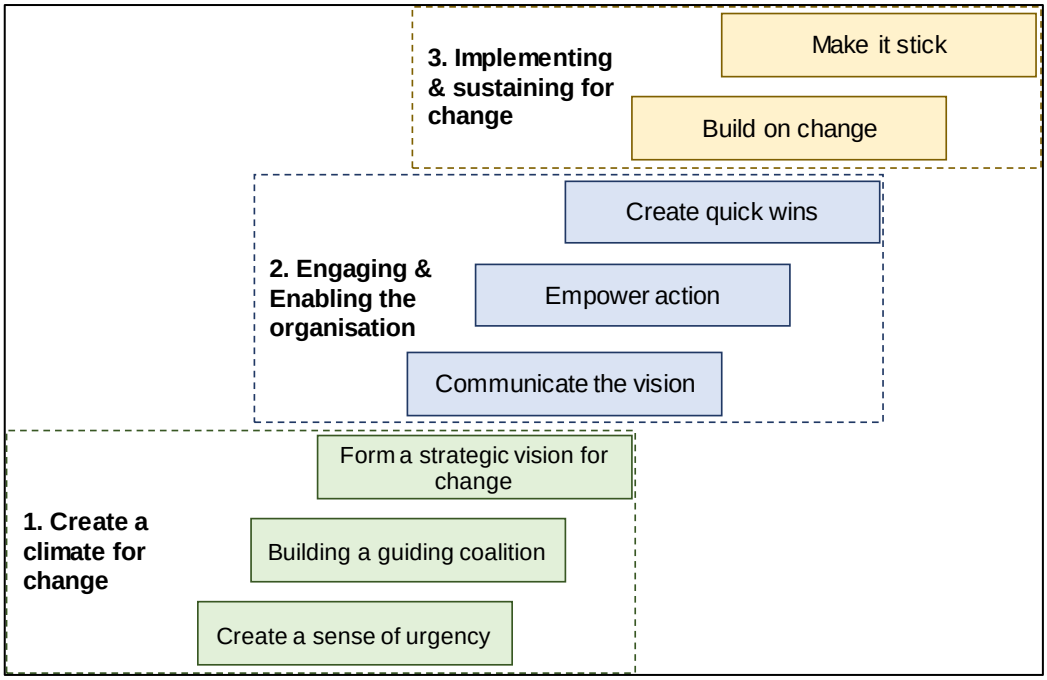


Figure 3: Kotter's 8-Step Change Model

1. Creating a climate for change and a shared sense of urgency for the required organisational change.
2. Engaging the employees and enabling them to effect the transformation in the organisation.
3. Implementation and sustaining change.

1.6 Significance of the study

This study might contribute to the academic body of knowledge to assist in understanding the role of leadership in cultivating a new culture with the business alongside well-established traditions and norms. Cybersecurity is considered a subculture of the organisational culture and introduces new behaviours and attitudes towards the handling and managing of the organisation's cyber assets. Building and embedding a cybersecurity culture into an organisation serves as reinforcement and a defence mechanism for the protection of strategic assets like data.

The findings from this research will provide lessons for leadership in any sector seeking to understand how to build and sustain cyberculture (subculture) within

their organisations. Other cybersecurity practitioners, including risk managers, will gain visibility of the gaps in the current cybersecurity measures and substantiate a business case for creating a human firewall by building and embedding a cybersecurity culture.

1.7 Delimitations of the study

This research focuses on a specific organisation within the financial services industry in South Africa. The participants in the study are derived from different departments within the organisations and are part of the senior manager level of leadership. Senior managers are instrumental in the building, embedding and sustaining of a cybersecurity culture within the organisation. This study focuses on the leaders' view of the strategy implementation and not the strategy formulation, which would have focused on the experiences of executives and their role in strategy formulation.

1.8 Assumptions

Current legislation in South Africa mandates that companies which experienced cyber breaches involving personally identifiable information should notify the authorities and the public, DoJ&CD (2013). Given the increased reports on the number of cybersecurity breaches in the media, the organisation acknowledges cyber risk as an essential risk to the organisation. One of the key objectives in the organisation's financial reports, Absa Group Limited, (2019), stated concerns about investments in technology and processes to safeguard the organisation against cyberattacks.

Most of the reported cyber incidents seem to be due to attacks by external threats, SABRIC (2019). However, organisations seem not to acknowledge the danger posed by insider threats. The organisation's employees may be its weakest link, thus constituting the most significant risk in its cyber defence strategy. Governance systems and frameworks enable organisations to define and control internal processes and technology; however, not the people element of an organisation.

Leaders create the climate within an organisation that either promotes or stifles the desired behaviours concerning cybersecurity. What gets measured gets done, as the adage goes; the leadership should identify appropriate metrics and incentives to drive the desired behaviours while discouraging unfavourable ones.

The design components of the strategic orientation framework usually focus on technology and processes, with little emphasis on people. Organisations have well-developed control mechanisms built into the governance and compliance of their operations, but not much in place to control people. Compliance to regulations and legislation does not guarantee security.

CHAPTER 2. LITERATURE REVIEW

2.1 Introduction

Advances in networking and computing technologies have propelled the emergence of the digital economy. In the digital economy, data has become a strategic asset since it enables businesses to innovate and compete, Bollinger & Smith (2001). Bukht & Heeks (2017), states that the technology adoption is fundamental to the production of digital products and services that are core to the digital economy. Data has emerged as a strategic asset in the digital economy. Strategic assets are resources that are crucial in a business's ability to maintain a sustainable competitive advantage. Data provides valuable insights into the users' behaviours and preferences which enables companies to serve their customers better Hartmann & Henkel (2020). The vast and varied amount of data frequently generated from the physical environment and transaction history have led to the explosion of big data. The availability of big data coupled with the available computing power and advances in analytics is responsible for the sense-making of these massive datasets. Big data and analytics enable businesses to cater to a market of one. To be competitive and relevant, organisations have had to rethink their strategies to take advantage of the data they have and to become digital businesses.

The data within a business consists of clients' and employees' personally identifiable information, transaction histories, designs and intellectual property, company strategy, etc. (Sun et al., 2014). Traditionally, organisations stored client and employee data as paper records in storage safes and data warehouses. However, during the past few decades, the storage and format of files have gone digital. Migration to the digital format and the strategic nature of data have increased the vulnerability and risks associated with its storage, usage and protection (Kumar et al., 2006).

2.2 Cybersecurity

2.2.1 *Information Security*

Business Continuity Management (BCM) and information security are the current methods employed by organisations to protect and ensure availability and access to their data assets, Phillips & Tanner (2019). The availability and speed of recovery of a data system after a system failure or a disaster constitutes BCM, a critical component of any business. Redundancy is the key to ensuring quicker recovery and system recovery for increased availability, thus underpinning BCM. Information security, on the other hand, focuses on ensuring the confidentiality, availability and integrity of the data (Kumar et al., 2006). A mixture of technology, policy and procedures provides information security for businesses' data assets by providing restrictions on who has access and what they can do after accessing the data. These two methods were initially ideal for internal physical threats (Kumar et al., 2006); however, the emerging strategic nature of data and the interconnectedness of businesses had given rise to cybercriminals' activities, Hohman (2015). The attacks on digital assets, transform the nature of the threats to an organisation. Cybercriminals employ sophisticated social engineering techniques such as phishing, vishing, ransomware, malware, amongst others, to gain access to company data networks and technology – thus complicating the nature of attacks. As such, physical protection and quick recovery alone are not enough to provide adequate protection in the current business environment. Moreover, cyberattacks target company employees since they present a weak link in the business' value chain, Reid & Van Niekerk (2014a).

2.2.2 *Cybersecurity*

Reid & Van Niekerk (2014b) assume that cybersecurity, while used interchangeably with information security, is distinguishable from information security because cybersecurity also includes aspects of information privacy and safety in its focus. Cybersecurity refers to the safety and privacy of people and assets (physical and digital). The authors further argue that information privacy is concerned with methods of collection, usage, storage and sharing of personally

identifiable data. Safety is the protection of people and both physical and digital assets from the destructive tendencies of cyber attackers such as cyberbullying, amongst others, Teoh & Mahmood (2017). Therefore, implicitly, cybersecurity strategies combine hard (usage of technology) and soft (human behavioural attitudes) approaches to fortify both physical and digital assets.

According to the Gordon-Loeb model (Gordon et al., 2015) of the cybersecurity investment section, organisations should spend about 37% of their IT budget on cybersecurity. A review of the allocation of resources by companies to fortify their data assets shows that there is a disproportional amount of investment in hard tools compared to soft tools, Reid & Van Niekerk (2014a). Hard tools include investment in technology, while soft tools include corporate awareness campaigns.

In general, corporate awareness campaigns focus on identifying and highlighting the potential risks posed by cyber-attacks and mitigation processes, Bada & Sasse (2015). These campaigns also include internal staff training, which exposes and sensitizes employees to the company's policies and procedures for managing cyber risks. The awareness training additionally focuses on specific expected employee behaviours to social engineering attacks. There has been some investment in these forms of awareness campaigns. However, Bada & Sasse (2015) argue that awareness alone is not enough to drive the desired behaviours amongst employees. There is, consequently, still a security gap due to employee behaviour.

Moreover, the author argues that a focus on awareness could only fall short of the desired outcomes because of the prescriptive nature of current forms of training. The reliance on awareness training alone does not adequately equip employee responses to the dynamic nature of cyberattacks. The employee may act in a manner that further exposes the organisation.

While information security technology has advanced and kept pace with advancements in the sophistication levels of education and awareness of the risks posed by cyber-attacks, it has not received much investment within most organisations. With employees proving to be the weakest link in the protection of

an organisation's information, investments in education and awareness would be vital in providing a more cybersecurity conscious and vigilant workforce. Education and awareness training are effective ways that organisations use to drive desired behaviour, Reid & Van Niekerk (2014b). Bada & Sasse (2015) posit that for cybersecurity awareness campaigns and education to be effective, they must be contextual, relatable, relevant, engaging and easy to understand for all members within an organisation. When designed as too general and unrelatable, employees do not embody the learnings and view it as obligatory. Instead, their behaviour and attitude towards cybersecurity will remain unchanged.

2.3 Research Question 1: What type of organisational culture supports a cybersecurity culture?

2.3.1 *Culture*

Different groups and gatherings of people with a shared belief system stay connected by their shared culture, also called "societal culture", Schein (2010). Organisational culture is a subset of this societal culture and dictates the commonly shared norms and beliefs of employees within an organisation. It has the power to influence their behaviours and attitudes to the extent that a set informs an employee's behaviour or beliefs and norms that are a product of the culture of their environment (Dolan et al., 2010; Schein, 2010). The culture may include employees' actions when faced with cybersecurity threats (Dolan et al., 2010; Schein, 2010). If one is to augment the softer side of the cybersecurity strategy, one would need to understand the construct of organisational culture (including the security and cybersecurity subcultures), its antecedents, moderating factors as well as its outcomes in an organisational context.

2.3.2 *Organisational Culture*

Organisational culture is a stable, complex and holistic construct shared by members of an organisation that provides a frame of reference for the observed behaviours and attitudes of the organisation. A shared history often guides it, and shares learning and leadership (Guldenmund, 2000; Schein, 2010). Culture is

influenced by both external factors and the internal processes of an organisation – often at the behest of the leadership Guldenmund (2000). Culture creates stability and ensures continuity within the organisation. Organisational culture can act as a defence from unknown and unwanted external influences and is the prerogative of an organisation's leadership (Guldenmund, 2000; Schein, 2010). The leadership of an organisation has a significant influence on the culture of its members through the culture they cultivate in the organisation.

2.3.3 *Safety Culture*

Safety culture is a subculture within an organisation that focuses on employees' attitudes and behaviour on the security of the company's resources to achieve stability or survival. Safety culture is about reducing and minimizing the number of life-threatening incidents. As organisational culture is about how things get done within an organisation, in an organisation with a safety culture safety is everyone's business to ensure no loss of life or damage to the community or environment. Similar to organisation culture, safety culture is influenced by both external factors and internal processes of the organisation – often at the behest of the leadership.

Regulation is one of the most important, if not the most crucial – drivers of an organisation's safety culture. For example, regulatory factors drive the safety cultures of organisations in healthcare, mining, aviation, energy and resources. Internal processes that drive safety culture include management systems and human resources systems that comprise of employee incentives and performance management.

The outcome of the safety culture in these industries is relatively low – there are but a few incidences of accidents or security breaches, Pidgeon (1998). Nieva & Sorra (2003) posit that the number of fatalities in these industries is low, and incentives are built into the performance metrics for compliance as a way of driving the desired behaviours and attitudes.

As stated, the leadership of an organisation builds and embeds the organisational culture. Therefore, the leaders drive and insert the organisation's security culture

to ensure a total buy-in from the whole organisation. The culture creation is evidenced in awareness building initiatives and framing of the message to communicate the dangers of unsafe behaviour in a manner that is unambiguous and concise, and that does not incite resistance (de Bruijn & Janssen, 2017; Dolan et al., 2010).

2.3.4 *Cybersecurity Culture*

The recent rise of cyberattacks has elevated the significance of cybersecurity above other security, thus building a case for practitioners and academia to further unpack and understand cybersecurity as a construct. It is, therefore, not merely a component of security culture building and embedding of a cybersecurity culture. ENISA (2018) defines cybersecurity culture as “the knowledge, beliefs, concepts, perceptions, attitudes, assumptions, norms and values of employees regarding cybersecurity and how they manifest themselves in an employee’s behaviour with information technology”. Cybersecurity culture is influenced by both external factors and the internal processes of the organisation – often at the behest of the leadership.

Business processes are supported by technological platforms to provide a layer of security against cyber-attacks from both internal and external threats. Technology reduces the burden on employees to focus on compliance to the extent that it hampers their performance. Adopting a cybersecurity culture requires embedding cybersecurity into the daily behaviour and attitude of the employees. Cybersecurity culture requires a change in mindset and promotes security awareness and risk perception while maintaining a close organisational culture rather than trying to coerce the desired behaviour, Merritt (2002). Top leadership – the board and executive management – need the building of a cybersecurity culture within the organisational culture, and the employees will adopt it. Senior leadership buy-in can either make or break the success of the development of cybersecurity culture. An organisation embodies the cybersecurity culture when its employees exhibit a security-first mindset resulting in improved resilience against cyber-attacks initiated through social engineering techniques.

2.4 Research Question 2: How does leadership develop and sustain a cybersecurity culture within an organisation?

Shared values and lived experiences are the basis of an organisation's culture. The shared values and lived experiences of members influence the behaviour and norms of the individuals within the group. To develop a cybersecurity culture within an organisation, the individuals should share the same values of the importance of mitigating risk against cyber-attacks.

2.4.1 *Leadership*

Leadership is a social influence process in which the leader seeks the voluntary participation of followers to achieve a strategic objective for the organisation, Nanjundeswaraswamy & Swamy (2014). The leader is one or more people responsible for delegating, motivating and influencing their followers within the organisation to pursue a common organisational target, Gandolfi & Stone (2017). The leadership there refers to the process of influencing others and also the individual or group of individuals involved in the process of leading others. The process of influence involves the approaches of inspiring and motiving followers to willingly work towards a goal through personal motivation, Shaver (2014). These approaches are guided by the leadership processes and the leader's leadership style and personalities.

Organisations are adopting digital strategies to remain relevant and maintain a competitive advantage in a hyper-competitive market. These digital strategies mandate that the organisation realigns its organisational design and culture to the new digital strategy. Digital strategy involves the application of technologies such as cloud, mobility, analytics, social media, etc. to business models to create distinct competitive advantages that allow the organisation to create value for its customers while capturing value for its shareholders, (Kane et al., 2015). The realisation of a digital strategy requires alignment of the strategy implementation, design components and strategic objectives. These components include technology, human resources, management systems and structure, Cummings & Worley (2014). Drucker states that in today's business environment business

needs to pursue not only operational competitiveness but also creative competitiveness that requires a change in organisational culture as a starting point. Leadership has the role of defining, creating and nurturing the desired culture. For competitiveness, organisations need to be continually experimenting and learning from experience from the market. The “Upper Echelon Theory” by Hambrick & Mason (1984) posits that leadership is central to the implementation of strategy and therefore, by extension, the development of the organisational culture.

2.4.2 *Leadership styles*

The leadership’s style of the leaders within an organisation influences the organisational culture and the resultant organisational performance. The leader’s immediate and extended influences significantly contribute to the leader’s leadership style, Nanjundeswaraswamy & Swamy (2014). These influences are culturally oriented stemming from traditional beliefs, norms and values. Research into leadership styles focuses on the leader/follower relationship and how the actions of one impact the other, Gandolfi & Stone (2017). Key elements involved in leadership are influence, intentionality and perception, Gandolfi & Stone (2017).

Leadership styles are characterised into two broad categories, namely, trait-based and skills-based styles of leadership, Gandolfi & Stone (2017). The trait-based leadership theory focuses on the personality of the leader and fails to account for the environment in which the leader has to operate. The skills-based leadership theory argues that leaders can be developed through focused, intentional skills development. Gandolfi & Stone (2017) argue that the skills-based while limited provides the foundation of newer leadership theories such as situational leadership, transformational and transactional leadership.

2.4.2.1 Situational leadership

The situational leadership theory proposes that effective leadership requires a rational understanding of the situation and the appropriate response. This leadership style relates to the leader’s style to the maturity level of the followers

with the leader's behaviour being either task or people-focused. The effective leader will engage a mixture of task and relation behaviours. Situational leadership emphasizes the importance of the level of maturity of the followers as a context that leaders need to establish the correct fit between the leader and follower, Bass (2008).

2.4.2.2 Transformational leadership

Transformational leadership style concentrates on the development of followers as well as their needs. Managers with the transformational leadership style concentrate on the growth and development of a value system of employees, their inspirational level and moralities with the preamble of their abilities, Nanjundeswaraswamy & Swamy (2014). The leaders achieve results by employing idealized influence, inspirational motivation, intellectual stimulation, and individualized consideration (Bass & Riggio, 2006; Bass & Bass, 2009). The transformational leader demonstrates each of these four elements to varying degrees to drive the desired organisational outcomes through their followers. Transformational leaders share a vision, inspire followers, mentor, coach, respect individuals, foster creativity, and act with integrity, Bolden (2010).

2.4.2.3 Transactional Leadership

Transactional leadership focuses on the exchanges that occur between leaders and followers. These exchanges allow leaders to accomplish their performance objectives, complete required tasks, maintain the current organisational situation, motivate followers through contractual agreements, direct behaviour of followers toward the achievement of established goals, emphasize extrinsic rewards, avoid necessary risks and focus on improving organisational efficiency, Nanjundeswaraswamy & Swamy (2014).

In turn, transactional leadership allows followers to fulfil their self-interest, minimize workplace anxiety, and concentrate on clear organisational objectives such as increased quality, customer service, reduced costs and increased production. Leaders influence followers through contingent rewards and negative feedback or corrective coaching, Gandolfi & Stone (2017).

2.4.3 *Change management*

With the organisation embarking on a new strategic direction, the process of transforming the company comes with significant changes to the organisation. These changes include changes in organisational design and culture. Todnem BY (2005) states that organisational change is inherent in any change in organisational strategy. Successful management of the change process is vital in the achievement of the company's strategic objectives, Brisson-Banks (2010).

Change management depends on the leadership's ability to enact it and implement the new strategy, the resultant organisational design and the culture shift, McKnight (2013). Successful leaders share the broad vision, have an identity and destiny, will be creative and inclusionary, and be open for personal and organisational continuous learning. These leaders build consensus, create a unified purpose, and sustain the change for a competitive advantage for the future.

Organisational change may be gradual or punctuated, depending on the desired outcomes. Gradual change is continuous and incremental, and leaders focus more on planned change management strategies with established timelines, evaluations and reconfiguration, McKnight (2013). Punctuated changes are usually a result of internal or external pressures, and the changes themselves are abrupt – often requiring significant organisation redesign and culture. Punctuated changes are transformational and need leaders with a transformational leadership style to guide the organisation in the change process, Todnem BY (2005). The leaders should create, share and implement the collective vision of the future of the organisation. Transformational leaders influence the changes to the organisations through behavioural integrity. Behavioural integrity is the convergence of values expressed by words and actions, McKnight (2013). The credibility and trust of the leaders are dependent on their levels of behavioural integrity. Leaders need to show empathy towards the employees and be authentic in their actions. According to Merritt (2002), change is easier to implement when the meployees feel engaged to the cause through the leadership's attitudes.

Transformational change within an organisation requires increased flexibility and responsiveness among all its members since it is usually a response to an external threat or an opportunity to gain a competitive advantage.

There are several approaches for implementing change available, including the Lewin-three step model and Kotter's eight-step model. Kurt Lewin's three-stage theory of change often referred to as the Unfreeze, Transition, Freeze model is the earliest change model, Brisson-Banks (2010) and focuses on breaking from tradition to form new habits. The unfreezing stage involves the process of preparing for change by sharing an understanding of the expected change and the need to step out of the comfort zone. This stage is critical in breaking down the barriers to change. The transition stage involves the process of reacting to the change. Individuals respond differently to change, and leaders need to support the organisation to transition. Resistance to change may be faced at this stage and require delicate management through training, coaching, etc., Connelly (2016). The final stage of freezing is focused on establishing stability with the organisation, marking the end of the change with the new normal. The Lewin-3 stage approach is useful for the analysis of the start and end states and constant evaluations of progress, (Cameron & Green, 2009, p. 148). Critics of the model question its simplicity in dealing with the complex change initiatives.

Many organisations have implemented changes in response to market threats and opportunities with varying degrees of success. Kotter identifies 8-steps crucial for leaders to follow for the successful implementation of change initiatives, Brisson-Banks (2010). The sequence of the steps is significant in the successful execution of the change provided below:

1. Establish a sense of urgency
2. Form a guiding coalition
3. Create a powerful vision
4. Communicate the vision
5. Empower others to act on the vision
6. Plan and create short-term wins
7. Consolidate improvements and build on the change
8. Sustain the change

According to Kotter, the first three steps are vital in creating the desire to change and overcome resistance by creating a shared understanding of the dangers of not changing (Cameron & Green, 2009, p. 148). Kotter's 8-step approach is ideal for organisations undertaking transformational change regardless of their sizes. The model's linear approach to change makes it suitable for planned change with a predefined outcome.

2.4.4 *Leadership style and change management*

The rise of the threats of cybercriminals and cyber-attacks create business environments that are increasingly complicated and complex to manage. There is a consideration in the decision-making processes for complications due to the increasing number of internal and external factors. These considerations include regulations, shareholders, employees, society, etc., all with different expectations from the organisation. Complicated situations are ambiguous; and usually managed through a set of rules, policies and procedures with known and predictable desired outcomes. The complexity arises from the unpredictable nature of the various types and sources of external factors such as cyber-attacks on a business that is usually related to future events. Due to their unpredictable nature, the best way in which a company can manage complexity is through measures to mitigate the effects rather than trying to solve it. Developing a cybersecurity culture presents a challenge for leadership to manage both complications and complexities within the business, Richardson (2008). The leadership needs a balance of complicated thinking skills and a complex mindset to help drive the creation of the cybersecurity culture within the organisation. Leadership with expedient problem-solving skills is needed to help drive the creation of a cybersecurity culture within the organisation.

The volatile, uncertain, complex and ambiguous business operating environment requires leadership that is flexible and adaptable to the dynamic conditions. The required leaders for the organisations should exhibit both complicated thinking skills and a complex mindset balancing the traits of both transactional and transformational leadership. The transactional part is responsible for managing the complications, while the transformational part is accountable for managing

complexity, Bass (1990). However, these traits may not be present in a single individual, and this, therefore, requires a leadership team, not an individual, (Bolden, 2010; Holten & Brenner, 2015). Such a team should collectively embody these traits to drive the change in the organisational culture to incorporate a cybersecurity culture. The leadership significantly influences the organisation's culture; hence, having suitable leadership traits is critical in the development of the cybersecurity culture within the organisation. The leadership act as the agents of change and need to understand and implement change management.

2.4.5 *Organisational design*

Transformational change often results in organisational development focusing on altering the current ways of work, the organisational structure, human resources structure and – or – its management systems (Cummings & Worley, 2009, p. 505). Organisational development is fundamental in supporting organisation-wide transformation by altering the beliefs, attitudes and behaviour of the organisation in line with the strategic changes (Rana et al., 2015, pp. 39–48). Organisational development defines the building blocks for organisational design to support strategies, such as outlining new structures that enable the business to be more responsive to changes or more participatory by pushing decision-making further down the organisation. It also incorporates organisational learning to facilitate collective understanding required to effect organisational change. The ability of an organisation to continuously learn is vital for an organisation that is continually changing and adapting to its environment.

Organisational development interventions refer to the process of improving organisational performance through enhancing the organisational design and altering the culture. Interventions need careful planning, design and diagnosis if they are to deliver on the expectation of the leadership (Cacioppe & Edwards, 2005; Saadat & Saadat, 2016; Tiller, 2012; Wang & Ahmed, 2003).

The intervention types include techno-structural and structure redesign. The techno-structural intervention focuses on an organisation's processes and technology that influence the ways of working, Cummings & Worley (2009). The design of the interventions improves the efficiencies in the processes by

introducing management systems to support the operations. Employees are provided with more control to coordinate the workflows.

Structural redesign interventions focus on the organisational configuration into a business unit, functional units and subunits in line with the organisation's size, its environment, technology and strategy, Tiller (2012). Structure designs usually deal with core functions or customer segments.

Senior leadership is responsible for strategy formulation and implementation, and is, therefore, guides the overall performance of the business. Strategy implementation requires buy-in from the whole organisation, and the leaders should be able to provide and articulate this vision and create a conducive environment. It is for this reason that leaders can either make or break an organisation based on the environment they create and the culture they foster.

2.5 Conclusion of the Literature Review

Behaviour-based transformation is as much an integral component of cybersecurity as technology. The defence provided by technology is critical in protecting data assets from the outside but might not be as effective against threats from within. Increasing awareness against cyber threats develops a culture which has a strong influence on behaviours and attitudes. The impact of culture on an individual's behaviour and attitude is more potent than any level of education. The leadership in any organisation is responsible for creating and nurturing the desired behaviour within the organisation.

CHAPTER 3. RESEARCH METHODOLOGY

This chapter describes the research paradigm, approach, and design used to achieve the purpose of the study.

This study explores the role of leadership in the building of a cybersecurity culture within the South African financial services. It is based on the constructivist paradigm and employs a case study approach.

Several reasons compelled the adoption of a qualitative approach for this study. First, qualitative research methods are useful for exploring the context of the research and the activities that occur in that context in greater detail, Yin (2014). The qualitative case approach was ideal due to the exploratory nature of the research questions, Stake (1995). The research questions in the study began with “how” or “what”, allowing the researcher to gain an in-depth understanding of the context (Patton, 2016; Seidman, 2006). This study explored participants’ experiences with behavioural-based approaches to cybersecurity that were underpinned by the existence of a cybersecurity culture within the organisation.

Second, a qualitative study allows the researcher to explore phenomena, such as feelings or thought processes, that are difficult to extract or learn about through conventional research methods, Strauss & Corbin (1998). For the present study, non-verbal cues to some of the interview questions provided valuable insights not verbalised by participants.

Third, qualitative research methods are the best approach when studying phenomena in their natural settings, Denzin & Lincoln (2008) and when striving to understand social processes in context, Esterberg (2002). The current study focused on a senior manager’s experiences of the organisational culture and how it promoted the creation of a cybersecurity culture.

Fourth, qualitative methods emphasise the researcher’s role as an active participant in the study, Creswell & Poth (2017). For the present study, the researcher was the critical instrument in data collection and the interpreter of data findings, Creswell & Poth (2017). Research approaches used in this study included the following: Purposive and snowball-sampling, semi-structured

interviews, and content analysis of the primary data. An on-going interpretive role of the researcher is prominent in any qualitative case study, Stake (1995).

Qualitative methodologies are fundamentally anchored in developing a depth of understanding, both of a particular phenomenon and construction of meaning that individuals attribute to their experiences. Attending to the complex dynamics that emerge from the data-gathering processes requires due care, Jones (2002). The intent of qualitative research is, through an in-depth examination, to illuminate and better understand the vibrant lives of human beings and the world in which they live (Jones et al., 2011).

The qualitative approach strives to understand social processes in context while exploring the meanings of social events for those who are involved in them, Esterber (2002). Qualitative research involves an interpretive, naturalistic approach to the world – studying things in their natural settings while attempting to make sense of and interpret phenomena in terms of the meanings people bring to them, Denzin & Lincoln (2008).

In addition to the components and foundations that guide qualitative research serve as the means to contextualize and understand the research questions in this study. A qualitative approach is most appropriate for this study because it fosters a better understanding of the lived experiences of the participants (senior managers) and their perceptions of the behavioural based approaches to cybersecurity. This study allows participants the opportunity to articulate, in an unrestricted manner, the ways their understanding of the cybersecurity strategy and what their role has been. The use of rich, critical description provides in-depth, detailed accounts of the participants' experiences.

3.1 Research approach

The constructivism paradigm framing this qualitative research asserts that different people construct meaning in different ways, even when experiencing the same event, Crotty (1998). There are several assumptions of constructivism, three of which are fundamental to this study:

1. Humans seek meaning from their interaction with the world around them, and hence qualitative researchers tend to use open-ended questions to explore their lived experiences in the participant's own words.
2. Humans make sense of their world and surroundings based on their historical and social perspectives.
3. The primary generation of meaning is always social, arising in and out of interaction with a human community.

The research interpretations and findings in qualitative research, therefore, are context-specific.

Constructivism is useful as the philosophical framework for this research and is a belief that knowledge is made up mainly of social interpretations rather than awareness of external reality, Stake (1995).

This research deals with interpretations of the senior managers in the financial services organisation involved in implementing the organisation’s strategy and monitoring associated operational risk. The participants in this study constructed reality as based on their individual and shared experiences: how they interacted with participants and made decisions based on actions that were based on the organisations' policies and expected behaviour.

In terms of analysis, this study was specifically interested in understanding how leadership shaped and created a climate that enabled the creation and nurturing of a cybersecurity culture. The interpretive tradition asserts that researchers should begin by examining the context to be studied through actions and inquiry, as opposed to predisposed assumptions.

The basic interpretive study exemplifies the assumption that the researcher is interested in understanding how participants make meaning of a situation or phenomenon. This meaning mediates through the researcher-as-instrument. The strategy is inductive, and the outcome is descriptive Merriam (2002). Generally, rather than beginning with a theory or preconceived notion of the way the world works, researchers should begin by immersing themselves in the world inhabited by those they wish to study Esterberg (2002). Specifically, understanding how individuals in the world construct and interpret reality should constitute the

primary emphasis Gubrium & Holstein (1998). Constructivist and interpretive approaches subscribe to the notion that all social reality is constructed, created, or modified by all the social players involved.

The constructivist paradigm of this study explores the senior managers' perceptions of the role of leadership in building a cybersecurity culture. Constructivist researchers focus on understanding and reconstructing the meanings that individuals hold about the phenomenon being studied (Gubrium & Holstein, 1998; Jones, 2002) by examining in-depth their lived experiences through the use of open-ended questions (Jones et al., 2011). Thus, for this study, interviews with eight senior managers were conducted, a review of relevant on-site documents was held, and with these data, artefacts were analysed in an attempt to understand and construct the meaning of participants' perceptions and experiences with the leadership's role in building a cybersecurity culture.

3.2 Research design

This section introduces the case study research, defines case study methodology, examines the relevance of case study methodology, and describes case study research designs as being created from case study research.

Qualitative case study research served as the principal methodology for this study. In terms of the contributions of case studies, Flyvbjerg (2006) believed that a greater number of good case studies would strengthen social science. However, the author warns researchers to be mindful of the five most significant misunderstandings of case study research, namely:

1. theoretical knowledge is more valuable than practical knowledge,
2. one cannot generalise from a single case; therefore, the single-case study cannot contribute to scientific development,
3. case studies are most useful for generating hypotheses, whereas other methods are more suitable for hypotheses testing and theory building,
4. case studies contain a bias toward verification; and
5. it is often challenging to summarise specific case studies.

3.2.1 *Case Study*

The case study methodology is a strategy of inquiry in which the researcher makes an in-depth study of a program, event, activity, process or one or more individuals (Stake, 1995; Yin, 2014). Cases are bound by time and activity, and researchers collect detailed information using a variety of data collection procedures over a sustained period. The phenomenon under investigation in this study was cybersecurity culture as a behaviour-based approach to protect an organisation's cyber assets. The case was an organisation within the financial services sector in South Africa, with data collected through in-depth interviews, observations and a review of publicly available documentation on the organisation. Due to the strategic nature of cybersecurity, the organisation could not share any internal documentation. The documents include reports on numbers and types of breaches and changes in volumes of success breaches experienced by the organisation. Specifically, interviews were conducted, recorded and transcribed with the data coded for emergent themes.

Yin (2014) named five components of effective case study research design: (1) research questions; (2) propositions or purpose of the study; (3) unit analysis; (4) logic that links data to research questions; and (5) criteria for interpreting findings. The most appropriate questions for this type of qualitative case study research were "how?" and "what?". The line of inquiry centred around how the participants defined their current organisational culture and how it impacted the creation of cybersecurity culture.

The second component of the case study research design is to define the study purpose clearly. This component is the purpose statement and is a declarative statement summarising the study's main objectives, Yin (2014).

The third component of the case study research design is the unit of analysis. (Flyvbjerg, 2006; Yin, 2014) described the unit of analysis as the area of focus that a case study analyses. Yin wrote that an appropriate unit of analysis occurs when primary research is accurately specified. This study's unit of analysis is a financial institution within the financial services sector in South Africa.

The fourth component of the case study research design is to connect data to propositions. This connection is made following the data collection phase, as themes emerge. In analysing the data, the researcher attempts to match patterns that appear in the data to the theoretical propositions of the case study. The emerging themes in this study thus serve as answers to the research questions.

The fifth component of the case study design is the criteria for interpreting findings. Commonly, the case study researcher codes the data before developing themes, Yin (2014). Following the theme development stage, the meaning is extracted from the findings to determine recommendations for the case study and future research.

3.3 Data collection methods

The primary source of data collection will be semi-structured interviews. As a rule, the interviews are carefully conducted to ensure a reliable case study. Purposeful and snowball-sampling, consideration of the individual versus a group focus and sample size provided vital decision points for the data collection process. Purposeful and snowball-sampling ensured the appropriate choice of participants for the interviews for the case.

The interview is a conversation between the interviewer and interviewee, in which the interviewer asks questions, and the interviewee responds accordingly, Esterberg (2002). Through background research into the context, the researcher should early-on determine the appropriately knowledgeable people in the organisation who will provide the best sources of rich data. This study identified senior managers as knowledgeable sources for the research since they are responsible for the strategy implementation and are also the link between the leadership and the rest of the organisation.

When conducting interviews, relationships and rapport must be established and coupled with trust. Active listening and non-judgmental behaviour are two of the standard practices prioritised when interviewing for case study research. There are six types of questions Patton (2016) employed during the interview process

for case study research: (1) experience/behaviour, (2) opinion/belief, (3) feeling, (4) knowledge, (5) sensory, and (6) background/demographic.

This study intended to make the interviews conversational. The researcher shared information about themself with the participants to establish the necessary trust and rapport for the conversation. Conducting discussions in this way allowed the researcher to put respondents at ease and allowed for an optimal interviewing environment.

3.4 Population and sample

3.4.1 *Population*

The study took place at one of South Africa's leading financial organisations – ABSA – at the head office based in Johannesburg. The financial services sector was selected as it is one of the industries in the economy leading the charge in digital transformation. Secondly, the sector handles massive amounts of transactional data, and personally identifiable data makes them give cybersecurity high priority.

The structure of the organisation is such that most of the strategy formulation for the Group occurs at the head office and cascades to the divisions and regional entities for implementation. The role of the senior manager within the business is to drive the implementation of the strategy. They act as the bridge between top leadership and the rest of the organisation and responsible for overseeing the execution of the strategy. This makes their role significant in an organisation's building and developing a cybersecurity culture throughout the organisation.

3.4.2 *Sample and sampling method*

The study considers a sample of eight senior managers of a financial services organisation. Qualitative research has smaller sample sizes compared to quantitative research. (Guest et al., 2006) proposes a minimum sample of twelve. However, the actual number of interviews will depend on the stage when the

researcher achieves coding or data saturation. Saturation is achieved when no new code emerges from the interview transcripts.

The participants for this study were selected based on a non-probabilistic strategy of both convenience and purposive sampling. The purposive sampling selection of senior managers for personal interviews used a predetermined selection criterion based on position and experience of participants, Patton (2016). This method allowed the researcher flexibility to determine the sample size and the target population. Due to the challenges in accessing participants for interviews convenience sampling was also used leveraging the researcher's contacts with the organisation, Rahl (2017). Snowball sampling, the secondary sampling technique, in which participants nominated colleagues who – they believed – were able to share more insights on the research question, Rahl (2017).

Inclusion and exclusion criteria are critical in determining who is eligible to participate in the study to ensure the right insights are obtained from the study, (Keung et al., 2020). The criteria used in this study to determine whom to include or exclude is outlined in table 1 below.

Table 1 Inclusion & Exclusion Criteria

Inclusion Criteria	
Types of Roles	Strategy Implementation Team lead
Types of Participants	Executives Senior Manager
Types of Outcomes	Lived experiences in driving strategy implementation, team building and nurturing the desired culture in the business
Types of Location	Johannesburg based
Exclusion Criteria	
Types of Roles	Strategy execution Team members Non-leaders
Types of Participants	Lower-level employees
Types of Outcomes	The adoption and execution of the strategy
Types of Location	South Africa, outside Johannesburg or Rest of Africa

For the identified case organisation, the senior managers in the following functional areas were chosen to be participants: Risk, Human Resources, Security and Change Management. The selection criteria considered their involvement in strategy implementation and risk management necessary. The descriptions of the participants in the study, as shown in table 2 are anonymised as there are several senior management roles in the various departments sampled.

Table 2: Profile of participants

Description of participant type	Number sampled
Senior Manager: Change & Risk	1
Senior Manager: Governance & Control – Insurance Cluster	1
Senior Manager: Chief Security Office	1
Senior Manager: Fraud & Anti-Money Laundering	1
Senior Manager Group Operational Risk	1
Senior Manager: Digital Transformation in Risk	1
Senior Manager: People Change Management	1
Senior Manager: Attack Monitoring	1
TOTAL number of respondents	8

3.5 The research instrument

The semi-structured interviews conducted with each participant lasted between forty and sixty minutes. Two pilot interviews, held before the start of the fieldwork, provided insights into the anticipated length of the discussions (Zikmund et al., 2013). Two colleagues assisted in the pilot interviews to calibrate the researcher's interview skills, confirm the duration and refine the interview schedule questions. All the interviews were held face-to-face, allowing the research to observe the participants in their natural environment and to observe the participants' non-verbal cues in response to the researcher's questions.

The researcher conducted pilot interviews with a senior management colleague at their workplace to allow for the refinement of the interview instrument and interview techniques (Bloomberg & Volpe, 2008; Saunders & Lewis, 2012). The pilot interviews provided valuable insights into the potential length of the interview under real interview conditions with the researcher obtaining consent from the participant and capturing notes during the meeting. The interviewer recorded the duration of the discussion, highlighting questions that needed more time.

The insights obtained from the pilot interview provided recommendations of updates to the interview instrument. First, a rapport-building introduction added to the research tool ensured trust and openness between the researcher and participant. Second, the wording of the interview questions was updated to make them more open-ended. Third, sharpening of the follow-on probes ensured that participants provided maximum insights. See Appendix D for the research instrument, the questions and inquiries used in the interviews.

The eight senior managers interviewed for this research, enabled the identification and solicitation of knowledge from the people Patton (2016) refers to as “key informants,” i.e. people who are particularly knowledgeable about the inquiry setting. These people are articulate about their knowledge, posses insights that may assist an observer in understanding events that have happened and reasons why those events happened. The study’s interview sessions took place between February 17, 2020, and March 12, 2010. For convenience, all interviews took place at the participants’ offices.

With participant approval, the interviews were recorded using a mobile phone. Handwritten notes were also taken, which tracked critical points that were returned to later in the discussion or highlighted ideas of particular interest or importance. The format and structure of the interviews were similar for all participants. Seidman (2006) proposes an interview structure that comprises three parts, background and context, present situation and reflection on past and

present experiences. The interview started with casual and general questions to ease the participants into the process and create rapport, Sorrell & Redmond (1995). The purpose of the study, research procedure, expected benefits, the respondent's right to withdraw from the study at any time, and protection of confidentiality were outlined at the beginning of the interview. Participants were allowed to ask questions about the research study or research procedures. A self-introduction by the researcher provided a positive icebreaker to establish rapport and gain trust, Patton (2016).

Given the qualitative and semi-structured nature of the interview, the researcher needed to engage and practice deep listening during the interviews. Open-ended questions were used throughout the discussions to encourage participants to respond freely and openly to queries, Esterberg (2002). Probing and follow-up questions, when necessary, urged participants to elaborate on or clarify a response, Denzin & Lincoln (2008).

The transcription process began after the first interview on February 17, 2020, and was completed by March 15, 2020. Reviewing each transcript while listening to the audio recording ensured transcript accuracy. Additionally, the transcripts were presented to each interview participant for their review further to ensure accuracy.

3.6 Procedure for data collection

3.6.1 *Data gathering process*

The audio recordings and field notes made up the data collected from the semi-structured interviews by the researcher during the interview process. The conversation comprised three segments, namely (i) introduction, (ii) research questions, and (iii) conclusion and reflection. The following paragraphs provide an overview of each of the three sections.

Every interview began with the researcher engaging in a casual chat to build rapport, as recommended by Leech (2002). It is during this informal part of the interview that the researcher inquiries about the participant's role and

responsibility within the organisation. This part of the interview served as a check on the qualifying criteria for the participants and senior manager.

The section on the research questions was more structured and formal. The follow-on questions, where necessary, were based on the participant's last response and were designed to probe further and gain deeper insights, Barriball & While (1994). Minimising repeat questions except in instances where participants explicitly requested the researcher to repeat the question signified high levels of engagement between the researcher and the participant. Upon such requests from the participants, the researcher rephrased the question. The researcher also used feedback from the earlier interviews to improve the interview questions. In later interviews, the researcher used the opportunity afforded by qualitative research to probe topics shared in earlier interviews.

The interviews, on average, lasted between forty to sixty minutes, except for one that went past the hour mark. In conclusion, the researcher posed the following question to the participants:

> "If you could do anything differently, what is the one thing that you would do to improve the status quo?"

The design of the question attempted to get the participant to reflect on areas of potential improvement from the status quo.

3.7 Data analysis and interpretation

Qualitative research studies involve a continuous interplay between data collection and data analysis, Strauss & Corbin (1998). Analysis of data began after the first interview to identify emerging patterns and facilitate subsequent data collection, Strauss & Corbin (1998). There is no single way to accomplish qualitative research since data analysis is a process of making meaning. It is a creative process, not a mechanical one, Denzin & Lincoln (2008).

This research followed the data analysis and coding procedures suggested by (Creswell & Poth, 2017; Esterberg, 2002). Creswell & Poth (2017) mandated the traditional approach in the social sciences that allows the codes to emerge during

the data analysis. A qualitative computer data analysis program assisted in the analysis of the data. ATLAS.ti, a computer data analysis program was useful in organising, sorting and searching data from the text files of the transcriptions, Creswell & Poth (2017). An inductive approach to analysing the transcriptions from the interviews followed the three-step process outlined below (Saldaña, 2015):

1. **Codes** - Prepared and organised data by breaking down the information from the transcription into smaller chunks or codes. The data codes used the participant's language and terminology.
2. **Categories** - The codes were reduced into categories by searching for patterns and the universal nature of experience among the responses and grouping them into their overarching themes. The categories were evaluated against the research questions to create themes and sub-themes.
3. **Themes** – Themes were developed as aggregate units that presented the unit of analysis and which describe and explain the phenomenon fully.

The themes that emerged from the study are based on the participants' lived experiences as seniors in implementing change and being a change agent are presented in chapter 4.

3.8 Validity and reliability

To ensure factual accuracy and validity of the captured data from the interviews, Creswell & Poth (2017) propose nine possible methods of ensuring the validity and reliability of the data. In this study, four of these methods, namely member checking, external audits, triangulation, and the use of rich thick descriptions, were employed.

1. Member-checking involves sending copies of the transcriptions to participants for verification of the accuracy of the captured information. The copies shared included the audio recordings and transcribed notes from the interview.

2. All decisions made during the data analysis process by the researcher were recorded and tracked on a log for purposes of providing an audit trail of the changes and decisions.
3. Triangulation involves the use of more than one of the research tools to validate the data collected. In this research, the researcher made use of the interview recordings and the notes from a journal with recorded participant observations.
4. Detailed thick descriptions are more descriptive and remove the ambiguity that might arise when the participant is not articulate. Rich-think descriptions obtained through probing provide more in-depth insights from the participants.

3.9 Demographic profile of respondents

The study explores the role of leadership in cybersecurity culture within a financial services organisation based in Johannesburg, South Africa. Participants' demographic variables such as age, sex, ethnic background, etc. were not a consideration in this study and that data was not collected as part of the study. Table 3 below shows the participant's demographic profiles based on the informal introductory rapport-building conversation.

Table 3: Demographics of respondents

Aliases	Case Study Participants							
	Participant 1	**Participant 2**	**Participant 3**	**Participant 4**	**Participant 5**	**Participant 6**	**Participant 7**	**Participant 8**
Area of Focus	Change Management	Risk Management	People Management	People Management	Risk Management	Risk Management	Digital Transformation	Security
Tenure in Organisation	>6 years	>6 years	>4 years	>2 years	>2 years	>4 years	>5 years	>3years
Technical/ Non-technical	Non-Technical	Non-Technical	Non-Technical	Non-Technical	Non-Technical	Non-Technical	Non-Technical	Non-Technical

3.10 Ethical considerations

The researcher respected the rights, needs, values and desires of participants and sought consent to record and use sensitive information shared in the data collection interviews. The following safeguard measures to protect the rights of the participants were taken:

1. The researcher communicated the objectives of the study to participants, both verbally and through letters written to request permission for interviews.
2. The researcher sought written consent from the participants to continue with the study.
3. Throughout the interviews, the researcher made the participants aware of the active data collection devices and other note-taking activities.
4. The researcher sought validation on the transcriptions of the interviews from participants by sharing copies of the transcripts and recordings.
5. The participants' names and position in the organisation were excluded, thus guaranteeing their anonymity, and focusing on sentiments collected during the interviews.
6. At all times during the interview process, the participants' rights and wishes came first, and the researcher respected these when it came to reporting the data.

CHAPTER 4. FINDINGS

4.1 Introduction

The focus of this research was to explore the role of leadership in building and sustaining a cybersecurity culture within a financial services organisation. The following research questions assisted in exploring the phenomenon of interest in this study:

- Research question 1) What type of organisational culture supports a cybersecurity culture?
- Research question 2) How does leadership build and embed a cybersecurity culture in an organisation?

Semi-structured interviews with research participants provided insights based on the participants' experiences of the cybersecurity culture and how leadership was enabling an environment for it to thrive.

This chapter details the research findings based on the analysis of the semi-structured interviews and the researcher's observations of the participants' responses and the environment of the interviews. The strategic orientation framework's design components guided the analysis of the research findings. Research question 1 considered the culture design component, which is an intermediate output of the organisation's strategic orientation. Research question 2 focused on leadership, the strategy, management systems, technology, structure and human resources management systems.

4.1.1 *Coding Analysis*

Coding analysis provides the methodology of analysing the transcripts with codes being assigned to groups of similar sentiments from the participants. The grouping of similar and related codes enabled the identification of various categories of data. Categories were furthermore grouped into themes, which were mapped to the research questions. Figure 4 below outlines the coding analysis approach:

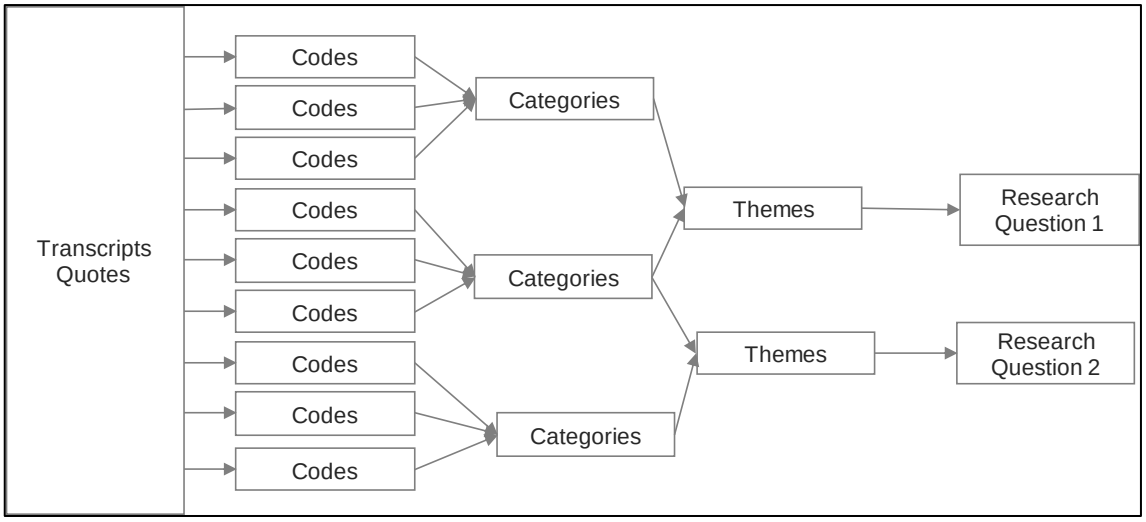


Figure 4: Coding analysis approach

The categories and the themes used in this study were predefined based on the available theory in the literature for organisational culture and development. The codes generated from the transcripts were aggregated into the associated predefined categories. The following section provides definitions for the categories used in the analysis:

Organisational culture

- Artefacts – these are the visible elements of the organisation and include language, brand, furniture, etc.
- Espoused values – these are the practice of the organisational values by members of the organisation.
- Underlying assumptions – these are the shared and widely accepted norms within an organisation that inform the values of the organisation.

Leadership

- Leadership process – focuses on the processes and procedures through which the leader influences the followers to accomplish an objective and directs the organisation in a way that allows it to optimise resources and capital.

- Leaders – these are the individuals tasked with formulating and implementing the organisational strategy and influencing the rest of the organisation to work towards achieving the strategic objectives.

Organisational design:

- Technology – this is the automated mechanism that supports the processes and activities undertaken by the organisation.
- Structure – focuses on the configuration of the organisation to ensure optimal and efficient management and coordination of activities among employees to achieve the organisation's strategic objectives.
- Management system – this is the information management system that supports the business processes.
- Human resources management – refers to the management of the human capital within the business across the complete employee lifecycle from selection to retirement.

Table 4 shows the output from the coding analysis of the interview transcripts.

Table 4: Coding analysis output

Codes	Category	Theme	Research Question(s)
Communication	Artefacts	Organisational Culture	What type of organisational culture supports a cybersecurity culture?
Culture Development	Espoused Values		
Organisational Learning			
Perceptions	Underlying Assumptions		
Awareness Building	Leadership Process	Leadership	How does the leadership build and embed a cybersecurity culture in an organisation?
Cybersecurity Strategy			
Change Management			
Cybersecurity Leadership	Leaders		
Leadership Style			
Active Monitoring	Technology	Organisational Design	
Technology-enabled Security Support			
Cybersecurity Function	Structure		
Governance & Control Function			
Effectiveness of Monitoring & Tracking	Management Systems		
Governance and Control			
Risk Management			
Whistleblowing Hotline			
Cyber Function Staffing & Retention	Human Resources Management		
Education and Awareness			
Incentives, Recognition & Rewards			

Table 5 shows the summary of the analysis of the findings, twenty codes identified and classified into seven categories, aggregated into three themes aligned to the two research questions.

Table 5: Findings summary

Code	Categories	Themes	Research Question
4	3	1	Research Question 1
16	6	2	Research Question 2

4.2 Results of research question 1

The first research question posed related to organisational culture and the support of a cybersecurity culture. Culture relates to the shared and collective beliefs about how the organisation carries out its business. Table 6 highlights the views of participants in terms of how they experienced the organisation's culture.

These experiences informed how they characterised the organisational culture and – by extension – the cybersecurity culture. Their unique position of being implementers of strategic initiatives within the organisation and proximity to the leadership of the organisation made their insights invaluable. The four codes generated three categories for the culture-related theme.

The organisation is in the process of redefining itself and forging a new identity. This process, according to some of the participants, will have created a more collaborative culture.

Table 6: Organisational culture-related sentiment codes

Codes	Category	Theme	Description
• Perceptions • Communication • Culture Development • Organisational Learning	• Underlying Assumptions • Artefacts • Espoused Values	Organisational Culture	These are the commonly accepted beliefs, norms and attitudes that influence the collective identity of the organisation. The organisation's DNA

4.2.1 *Underlying Assumptions*

4.2.1.1 Perceptions

All the participants described the organisation as going through an identity and culture-building phase, transforming the organisational culture into a more inclusive, transparent and innovative organisation with an increased focus on employee growth and development. Blame, suspicion and a lack of accountability characterised the previous organisational culture when it was part of Barclays Plc. Below are sentiments from some of the participants acknowledging that the organisation was in a culture-transitioning process:

> **Participant 2:** "We are a bank that had an old, entrenched culture where people did not trust each other, and people did not feel safe communicating. It is work in progress for the organisation, but it is improving, and we are not there yet."

> **Participant 5:** "The culture, the aspect of the culture is a very flexible culture where you have the leeway to work from wherever you wish because the business has given us the opportunity and the resources to be able to work in any office area, be it at the centre, actually even at home. It is very people-based."

> **Participant 5:** "It is a culture where teams are given opportunities, like employees going to study as well. From a training perspective, the bank is one of the best places to learn as there are many opportunities to get

significant exposure to new things. Moreover, there is extensive help and support in terms of developing individuals.”

Participant 8: “The culture of the bank is about people having the courage to speak out and speak up, appreciating people’s ideas, and it is about promoting transparency.”

4.2.2 *Artefacts*

4.2.2.1 Communication

Four of the participants acknowledged that the leadership’s openness and communication had been crucial in influencing the change in the culture, with Participant 3 remarking:

Participant 4: “I think the game-changer has been the open and honest communication from leadership, that this is not just establishing a new culture, a nice thing to do, but it is a business priority. Moreover, should we not transform our culture and improve, our bank will not be existing in five to ten years.”

The organisation uses several channels for communicating on various topics going on with the organisation, including reminders for compliance training, general awareness and feedback through town halls.

Participant 1: “So we are constantly getting reminders about our team for instance who has not done the training.”

4.2.3 *Espoused values*

4.2.3.1 Organisational learning

To be an innovative organisation, it has become a learning organisation aligned to the organisation’s objectives of employee growth and development. One of the participants highlighted that the organisation had a significant budget reserved for training:

> **Participant 8:** “One of the things that I probably left out there is that we have a massive budget – bigger than any other organisation right now in this country, I will tell you that for sure, in terms of learning and from a cyber point of view …”

Through the process of continuous learning, it keeps employees up to date with the desired attitude and actions within the organisation, including approaches to cybersecurity. A participant explained the importance placed on the training by the business as part of the culture-building process as follows:

> **Participant 2:** “We have a rigorous culture about the training in the sense that when people do not complete the training on time, we have a process of locking you out of your systems and not being able to access all systems until you do this. I guess that is how they are driving that culture of everybody having an understanding of those risks.”

4.2.3.1 Culture development

The organisation is over 40,000 employees strong, so the process of culture development cannot be taken for granted. The organisation has a dedicated team tasked with the process of culture development within the organisation. Hence, when asked for views on culture development, three of the participants were quick to highlight the fact that they had a culture team tasked with it. One response from a participant was as follows:

> **Participant 2:** “So we have a culture team tasked with the promotion of the organisational culture. In a big organisation such as this, culture is almost passed over by osmosis. And maybe that's why I'm struggling to catch on. Because you kind of just start to understand the culture by seeing how other people operate. As part of this new rollout, we had serious rollout workshops and kick-off things that everybody or 42,000 people went to, irrespective whether it is in South Africa, or another country. From the workshops, one started to kind of get a sense of how the organisation operates. I think it is a culture that's trying to generate a kind of innovative thinking about stuff, we are on a digital journey, and we know that banking

is changing. So, there is quite a lot of encouragement for people to kind of behave differently."

4.2.4 *Observations*

Two of the participants were hesitant to respond to questions around culture, and this was evident in participants that had been with the organisation longer than three years. The non-verbal cues indicated a sense of not being aligned to the words they were saying. One respondent initially cringed at the question and a second sought clarity on anonymity before responding. Participants that have been with the organisation less than three years had their non-verbal cues aligned to their verbal responses, indicating an alignment in their responses.

4.2.5 *Conclusion for research question 1*

The central theme that flows forth from the participants' responses highlights their deep-set beliefs in how the organisation works. Some aspirational norms are beginning to take hold, as indicated by the newer members of the organisation. The unit of change is the individual, according to one participant, and to focus on the individual to change behaviour is critical in the creation of a new culture. The results highlight an organisational culture focused on growing and developing the individual in an open, transparent and inclusive environment.

4.3 Results of research question 2

The implementation of the organisational strategy requires the alignment and efficient execution of the strategic orientation design components to achieve goals. Leadership is responsible for ensuring the appropriate and sufficient allocation of resources to the various parts of the organisation. The design components provide a framework for analysing the participants' experiences in the organisational climate. The tables below summarise the results of the interviews with senior managers grouped along the dimensions of the organisational design components.

4.3.1 *Leadership theme*

Leadership includes both the style of leadership and the type of climate created to execute the organisation's strategy. Leadership and organisational culture are closely interlinked since leadership is responsible for setting the tone of the expected organisational culture. The findings from the interview show the importance of communication, and availability of an individual or team with a mandate to lead the cybersecurity function and drive the interpersonal relationships. Table 7 below shows the ten categories on the leadership sub-theme that emerged from the interviews.

Table 7: Leadership related codes

Codes	Category	Theme	Description
• Cybersecurity Leadership • Leadership Style • Cybersecurity Strategy • Change Management • Awareness Building	• The Leader • Leadership Process	Leadership	Includes the personal traits of the leaders and their style as well as the processes they create for the organisational climate

4.3.1.1 The Leader

4.3.1.1.1 Cybersecurity leadership

The leadership of the organisation needs to provide its employees with a compelling vision for the organisation. The organisation appointed a security expert and senior executive with both industry and functional experience to lead the cybersecurity function. The level of the cybersecurity function leader indicates the level of priority that cybersecurity holds in the business. Five of the participants attributed that as part of the bank's cybersecurity competitive advantages, with one remarking as follows:

> **Participant 1:** "At the core, there is the leader of the function, and you want to make sure that you have somebody that is not just a technical expert, but also a senior leader and executive. So that they can lead an organisation and understand what it means to be a level-five leader. In our context, we have been lucky to get somebody experienced, and that has global exposure. Furthermore, he is now bringing that to the South African context."

The implementation of the group's cybersecurity strategy and the strengthening of information risk management and security controls requirements is the focus of the cybersecurity function's leadership. Four participants cited the merging of the security-related tasks into a single service as game-changing.

> **Participant 3:** "We put security together such that there is no separate physical and cybersecurity; it now falls under one umbrella, one leader. It is an integrated approach to security."

Participants highlight the inclusion of the security leader on one of the committees of the board, namely the Information Technology Committee. The inclusion of the leader of the cybersecurity function into an Exco board reflects the organisation's commitment to making cybersecurity a business priority.

> **Participant 4:** "So for the cybersecurity or the converge security office is a relatively new function within Absa, it is approximately three years old. It has been made a business priority and is no longer just an ad hoc support

function. Establishing an independent or separate role dedicated to converged security, the bank showed that it takes cybersecurity seriously. So our head of cybersecurity, who is our chief security officer with a budget and the mandate to protect the converged security. Since best practices consider cybersecurity integrated with physical security, and where cybersecurity and physical security converge, we are trying to reap the benefits of that as well."

4.3.1.1.2 Leadership style

Participants identified the maturity of the leaders and their ability to use motivation more than coercion as vital in changing the culture. Leaders need to be exemplary in the desired behaviour that they want to be adopted throughout the organisation.

> **Participant 1:** "Our leaders are very mature about being more pull and more carrot than stick so that they encourage you to volunteer to be more vigilant, rather than being told to be more attentive. Through role modelling events through rewarding and celebrating successes, that is through continuous support."

> **Participant 8:** "You see that ability to work together and communicate messages is a leadership thing."

> **Participant 8:** "Because it is leadership that gives direction from behaviour-wise staff members; if leadership is not able to work together, people will not be able to work together and even share information, they should completely change."

> **Participant 4:** "I think that is what the job of the leadership of the security Exco to make sure other businesses within the Group are protected in the way they interconnected with each other."

4.3.1.2 Leadership Process

4.3.1.2.1 Cybersecurity Strategy

A strategy informs the efficient allocation and assignment that the organisation implements to meet its targets. Cybersecurity awareness training was at the core of the cybersecurity strategy, a view shared by all participants.

> **Participant 4:** “So we have a cybersecurity strategy, part of the cybersecurity strategy involves awareness training. Awareness training ensures that all our stakeholders, that is, all our employees are aware of cybersecurity. We do focus on making it known that it is a joint responsibility for all staff members to be conscious of cybersecurity. Because we employ so many thousands of people, it increases our risk since one employee’s laptop could be the access point for a cybersecurity breach.”

> **Participant 8:** “So part of the cybersecurity strategy is a communication strategy to make sure that the importance of cybersecurity filters through the entire bank, from our, converge security office, to business, to all the employees. There is an upward and downward communication flow.”

4.3.2 *Organisational design theme*

4.3.2.1 Technology

Technology provides the underlying infrastructure that supports and enables the organisation’s processes and procedures, including management support. Table 8 shows the participants’ responses concerning technology’s involvement in cybersecurity. The organisation has invested significantly in technology, such as email screening technology to enable all employees to screen and report suspected breaches. According to one response this democratised cybersecurity to the end-user. Enabled by technology, no significant behavioural changes were required in the adoption of technology, making the experience seamless.

> **Participant 3:** “You are democratizing cybersecurity by putting the power in the individual’s hands, even if it is just knowledge. In some cases, technology is placed in the hands of the colleagues, at least with email,

they can secure emails themselves, and there is no need to go to the IT department."

Participant 3: "There is a whole bunch of sticks too, and those sticks range from automated sort of bots that catch instances of cybersecurity threats or breaches."

Participant 2: "We spend large amounts of money on the technology to prevent it even getting to us. The automatic screening of emails means a lot of suspicious emails are blocked before they get through and that sort of stuff. That creates a security layer around users removing the need to rely on human beings not to click on a phishing email or that sort of stuff because generally those are blocked before they even get to them."

Table 8: Technology related codes

Codes	Category	Theme	Description
• Active Monitoring • Technology-enabled Security Support	• Technology	Organisational Design	The underlying enterprise support infrastructure that enables the business to increase its operational efficiencies and improve cyber resilience

4.3.2.2 Structure

4.3.2.2.1 Cybersecurity Function

The organisation recognises the significance of cybersecurity and its impact on the organisation as it transforms into a digitally led institution. An appropriate structure is necessary to support and drive the related initiatives.

Participant 4: "In reorganizing the bank last year, we made sure that the two functional areas integrated, at least on that topic of cybersecurity management, and so we have got an end-to-end view now and once again, you know, driving this culture of cybersecurity across domains and functional areas."

Participant 3: “The converge security office is a relatively new function approximately three years old. It has a seat on the Exco. By having a seat in the Exco, it is no longer just an ad hoc function or ad hoc support source; it is a business priority.”

Participant 4: “So people and our staff now see cybersecurity not as just like three years ago as a buzzword, you know, but they see it as a necessary function of the business. Like you need an accounting department to process your taxes and your financials. You need a cybersecurity department to make sure all your services are safe and protected.”

An independent structure adequately resourced and staffed with performance targets support the cybersecurity strategy by providing governance and oversight to the business.

Participant 4: “We also have within the CSO department established a cybersecurity Exco. We have an Exco member looking after security operations. We have an Exco member looking after security consulting; we have an Exco member looking after security hardening. We have an Exco member looking after physical security. So, they all have leaders in place, leaders with teams and staff in this. They all have strategies, a budget and plans and targets to achieve.”

Participant 4: “It is not that we have not always had cybersecurity within the business. Three years ago, they decided to establish an independent security function. Before then each division used to have its own cybersecurity specialist and teams working on it. Now it is done by a central role that looks after the security services.”

Six of the participants initially responded by highlighting that they were not part of the cybersecurity and doubted their usefulness to the study.

Participant 2: “Because I am not in cybersecurity at all and we have a security officer that looks after that so I can maybe put you on to some people who would be able to answer those questions better than I can.”

They all agree that this has been instrumental in ensuring that appropriate attention and resources are provided to cybersecurity in line with the organisation's strategy. The structure is responsible for the development of the education and awareness program, communication and reporting, operations and governance of cybersecurity.

> **Participant 4:** "So we do extensive awareness training, we have got an awareness calendar as well. Each month we focus on different topics. So, we look at all the different factors. For example, look at all the different types of attacks."

> **Participant 4**: "I was in charge of a project looking at our current awareness program, externally benchmarking it, comparing the topics and advising the head of training to say that we have this, but that it is viable for you and for us to hear a few more topics that will be more comprehensive because this is what the external market is doing."

Two of the participants acknowledge the existence of an internal function that does active automated monitoring of employees' activities concerning cybersecurity to ensure that only desired behaviour. This function, in conjunction with the management systems, reports on user behaviour for any potential breaches and infringements.

> **Participant 3:** "We have established an insider threat function during the last 18 months. We are an industry leader in establishing a specific function to look at insider threats because our employees are formidable targets for bribes by hackers or blackmail, to share data or share loopholes."

4.3.2.2.2 Governance & Control Function

Cybersecurity risk is an operational risk under technology risk and managed through the existing risk management framework. The governance and control function guide the application of the risk framework.

Participant 6: “These would have come up from the assessment that we would have done on cybersecurity to say, for us to remediate these are the things that we need to do. In some cases, there is an investment required.”

Table 9: Structure related codes

Codes	Category	Theme	Description
• Cybersecurity Function • Governance & Control Function	• Structure	Organisational Design	Structure refers to the way the configuration of the business is to take advantage of its resources to achieve its goals.

4.3.2.3 Management Systems

Financial services is a highly regulated sector, and as such management systems provide a framework for governing and ensuring compliance within the organisation. Management systems provide methods of measuring the effectiveness of the strategy implementation by tracking appropriate metrics. These metrics enable leadership to adjust the allocation and assignment of resources for effective implementation. Compliance is mandatory, and a key metric, the management systems are built to ensure organisation-wide compliance. Table 10 below summarises the findings from the interviews concerning the available management systems.

Table 10: Management Systems Related Codes

Theme	Category	Codes	Description
Organisational Design	Management Systems	• Monitoring & Tracking Awareness training effectiveness • Risk Management • Whistleblowing Hotline	These are the systems, processes and procedures adopted by the business to support the control and governance of how operations function.

4.3.2.3.1 Monitoring & tracking awareness training effectiveness

The awareness training provides employees with relevant information on cybersecurity risk and expected behaviour as well as attitude towards it. The awareness training is not mandatory, and the organisation monitors and tracks compliance to completion and certification of employees.

> **Participant 4:** “So we have actual key performance indicators for our awareness training program? So, the awareness training tab has assessments to make sure that employees do have the basic understandings of the competence of cybersecurity. We also have targets, for example, we had 40,000 employees; we needed to make sure that we accessed at least 90%. And 100% of it always. However, we measure how much training we have implemented; how many people have passed.”

> **Participant 4:** “So, for example, we see that okay, since we have implemented training on phishing schemes, phishing schemes by the employees we send to the training has decreased. Is there a measurable difference in our breaching incidents? It is not directly correlated because sometimes there are other factors involved, but we do try to see the return on investment. We measure the number of attacks, the impact of training and what we have invested, for example, that X amount of training, X amount in a new technology, X amount in new staff, how much is the reduction in attacks is due to technology, new staff or due to the training.”

> **Participant 8:** “We measure our people’s understanding of what these things are. We also identify those that have failed the testing and arrange that they are then sent for further education.”

> **Participant 8**: “If there is alignment between your awareness sessions and your culture, people respond to it.”

4.3.2.3.2 Risk management

Governance and control provide the guidelines of the acceptable risk appetite and assess the materiality of the risks in each risk category. The guidelines

include the onboarding of vendors, applications and tools onto the organisation's environment.

> **Participant 7:** "So you cannot just bring in a new vendor; obviously, there is a whole vendor process you have to go through with them. There are usually five committees because we are such a large organisation; there are rules and regulations in place for introducing anything into the organisation."

> **Participant 7:** "Well, I think all the necessary controls are in place, concerning data privacy, and all of that sort of stuff ... we are under so much scrutiny with the SARBs who analyse what banks do with such detail."

4.3.2.3.3 Whistleblowing hotline

The whistleblowing hotline is an anonymous platform through which employees can raise issues of misconduct or discomfort from the operations of the business. The facility is open and accessible to all employees.

> **Participant 5**: "I think we have whistleblowing lines and all of that in place. The staff know about these things, and they are using it as well."

4.3.2.4 Human Resources Systems

Having the right skills in place is vital for the successful implementation of the strategy, and the interviewed participants acknowledge the shortage of critical skills in the market and the need to retain those they already have.

4.3.2.4.1 Cybersecurity function staffing and retention

Individuals with cybersecurity expertise are scarce and in demand as more companies adopt digital transformation strategies making their hiring and retention paramount to a cybersecurity strategy. The cybersecurity strategy includes focusing on staffing and retention of the cybersecurity function.

> **Partner 3:** "And we make sure that the function is capacitated in terms of bums on seats and, competence level. We ensure there are no vacancies

and critical vacancies are filled within a rapid timeframe, we are looking at a 36 days or less type of thing to fill critical vacancies."

Partner 3: "It took us 18 months to staff up our cybersecurity capability and going through the full battery of assessments and, and selection processes to make sure that we have the right profile of individuals on board."

Participant 4: "So we pay special attention to retaining our cyber skills, okay, and developing our cyber skills. So, we pay a large focus on making sure our cyber capabilities keep up to date with the latest training available. The latest developments in cyber technology and cybersecurity."

Participant 4: "So now we realize that the cost of hiring and the cost of replacing you might as well look after them now not only from a marketing point of view but from a development perspective of giving them a culture."

Participant 8: "In general, we are also quite very good at retaining our staff, you know, okay, we do not have a high turnover, we have an open budget for training."

As part of developing the pipeline, two of the participants indicated some of the initiatives the organisation has taken of partnering with a training academy for skills and pipeline development.

Participant 8: "Again, every year we train about 20 students that are not even part of the bank, to bring them into the cyberspace and give them some skills and awareness, you know. So that is leadership's commitment of resources."

Participant 4: "We have also commenced many initiatives, we are actually in the fourth cohort of the cybersecurity academy, where we take fresh, unemployed, unskilled school leavers. We train them on the scarce cybersecurity qualification."

4.3.2.4.2 Education and awareness

Awareness and education are vital in the creation of an understanding of the dangers and impact of cybersecurity risks resulting in a shared understanding across the organisation.

> **Participant 3:** “There has been an education and awareness campaign that kicked off last year. Furthermore, that education and awareness campaign touches all 40,000 employees.”
>
> **Participant 4:** “So we do extensive awareness training, we have got an awareness calendar as well. Each month we focus on different topics. So, we look at all the different types of attacks.”
>
> **Participant 4:** “There is a whole bouquet of topics to cover on cybersecurity, make sure that all employees have at least a basic knowledge of what cybersecurity awareness and threats are. For example, what we also do is that we do more detailed training for more high-risk employees.”
>
> **Participant 2:** “Banks are compliance heavy. Furthermore, we have a legal obligation to train up our people around all these risks. So we do have much training on topics that include cyber risks, fraud risks and money laundering.”
>
> **Participant 5:** “The compulsory training people would do just that there is more awareness around it, you know about phishing, and if you know, get these emails, and stuff do we have like security email addresses that you need to mail.”
>
> **Participant 7:** “So I would say the compliance training, including cyber risk training, is extensive. Moreover, every single colleague in Absa is almost sick to death of being trained on that.”
>
> **Participant 8:** “We also have like an educational portal, where people can go in and learn the mandatory courses. It is an online course, and if anyone does not complete it, their account gets disabled. So, it is a serious thing that it is measured. Everybody does it.”

4.3.2.4.3 Incentives, recognition and rewards

The organisations use incentives to reinforce the desired behaviours for compliance with training and completion of the compliance training. Employees exhibiting the expected behaviours are rewarded and celebrated.

> **Participant 5:** “I will say that because of the initiatives that were introduced in the organisation, to make sure that we get involved and also the recognition that we get yearly from a performance rating point of view.”

> **Participant 2:** “So the primary measure has just been one about as I said, locking people out of the system has been the key. Previously, it was too easy to go, “I will do it next week and just get ramped up”. Okay, so until now there was no level of consequence management.”

> **Participant 8:** “If something is done well, you know, people are rewarded. We tell people about it, we communicate it, it becomes part of our DNA.”

4.3.2.4.4 Skills development

Table 11 highlights some of the key themes that emerged from the interviews concerning the human resources management systems that manage the complete employee lifecycle from selection to exiting.

Table 11: Human Resources Systems Codes

Codes	Category	Theme	Description
• Cybersecurity Function Staffing & Retention • Education and Awareness • Incentives, Recognition & Rewards	• Human Resources Management Systems	Organisational Design	Talent and staff management is the key to how an organisation manages its processes of attracting/selecting and retaining its human resources

4.3.3 *Observations*

The availability of leadership and a structure dedicated to the implementation of the cybersecurity strategy, though acknowledged, is still considered as another functional unit that provides oversight to the rest of the organisation. It is these sentiments by the participants that give the impression that cybersecurity is about technology and processes and not about people and the way they conduct their operations.

4.3.4 *Conclusion for research question 2*

The design components of the strategic orientation framework provide a systemic approach to analysing the role of leadership in creating alignment and a climate that is conducive to the creation of a cybersecurity culture. There is a significant acknowledgement of these components by the participants, though, from a biased view, that leads them to say “that is not my responsibility”.

4.4 Summary of the findings

This chapter presents results from the initial analysis of the data collected during the in-depth semi-structured interviews and observations. The findings were discussed in light of the two propositions under consideration and also the design components of the strategic orientation framework.

CHAPTER 5. DISCUSSION OF THE FINDINGS

5.1 Introduction

Digital transformation is imperative for businesses seeking to remain relevant to their customers driven by changing customer behaviour and the adoption of technology for improved operational efficiencies and support of new business models. The financial services sector is one of the industries that are experiencing a significant shift in digitally led operations. With this comes new challenges and risks that threaten business as they transform their operations. One of the most significant challenges is that of cyber-attacks.

No sector is immune to the threat of cyber-attacks; however, the financial services sector faces the most significant risk from them. South Africa is considered one of the top countries for cyberattacks aimed at financial institutions using advanced social engineering techniques.

Organisations within the sector are making significant technologies to protect their cyber assets and improving their compliance policies through the updated enterprise risk management frameworks. However, technology and processes alone are not sufficient mechanisms for safeguarding against cyberattacks. Consideration of the people component of the organisation is vital in the formulation of a comprehensive cybersecurity system implementation. Such factors include embedding in the employees that are part of the organisation's culture, a cybersecurity culture.

This case study explored the role of leadership in creating a cybersecurity culture in the financial services sector in South Africa. The study conducted a series of in-depth, face-to-face, semi-structured interviews and observations of senior managers with one of the big financial institutions in South Africa. In this chapter, the findings of the study are analysed and discussed.

The discussion of results follows a similar approach as in chapter 4 aligned to the themes emerging from the two research questions:

1) What type of organisational culture supports a cybersecurity culture?

2) How does leadership build and embed a cybersecurity culture in an organisation?

5.2 Discussion on Research Question 1

5.2.1 *Organisational culture*

The organisation is currently undergoing a massive transformative change in its organisational culture as part of its separation from the former parent institution and redefining its strategy for the future as a digitally-led organisation. Cummings & Worley (2009) state that any changes in the organisational policy directly lead to changes in the organisational changes which impact the corporate culture. Todnem BY (2005) argues that to effectively change organisational culture, change management processes are required to guide the process. Cultural transformation is implemented through change management initiatives, to minimise the impact of the disruption brought about by the transformation, which usually involves changing people's behaviours and habits. Change management is, therefore, the discipline of achieving the transition with minimal disruptions.

Kotter (2012) outlines the process of leading the change through an 8-step model that focuses on creating a climate for change, engaging and enabling the organisation, and implementing and sustaining the change. Figure 5 below illustrates how the steps of the model drive change through winning the heads, hearts and hands of the employees. The head of the organisation is won by creating awareness and shared understanding of the impending changes and expected behaviours. Achieved by getting the employees to embody the desired behaviours as part of their value system and the organisation's DNA. The last section, hands, are focused on turning the values into actions made visible through the organisation's shared behaviours and attitudes.

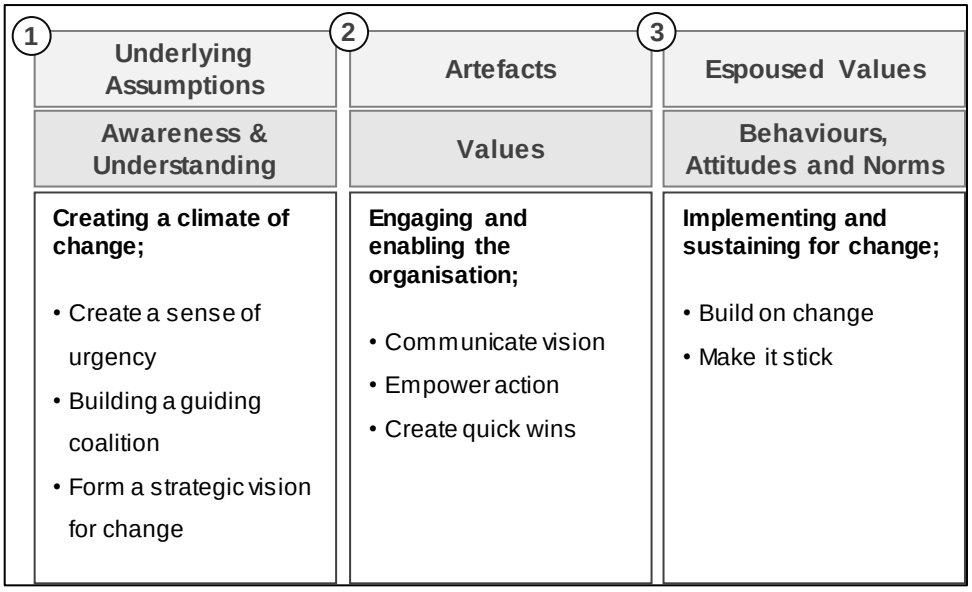


Figure 5: A modified Kotter's Organisational Change Model

Changing the culture of the organisation requires changing components of the organisation's actions and positions, Cummings & Worley (2009). The participants interviewed in this study acknowledge the transformation that the business is undergoing concerning the organisation's culture. Notably, the company has become more open with its communication, and the leadership is engaged and focused on building trust with the employees of the organisation, making it conducive for innovation.

The participants chose to describe the organisation's culture as transitioning to a more communal and collaborative culture that is open, inclusive and more tolerant. Considering the competing values framework (CVF), the collaborative, collective definition of the organisational culture fits the description of the clan and its adhocracy cultures. Cameron & Quinn (2006) describe the clan culture as one in which the people are friendly and share a lot among themselves like an extended family while considering adhocracy as being dynamic, entrepreneurial, and creative places for work. The new situation is in contrast with the former more hierarchical and market-driven culture adopted from the previous parent institution. The culture was more a matter of "command and control" with a lack of sense of accountability among employees for fear of being blamed. (Goodman et al., 2001) argues that an organisation's culture would be a combination of two of the four types of organisational cultures described by Cameron & Quinn (2006).

The clan and adhocracy cultures are ideal cultures for the organisation that is to be relevant in the future as a digitally led organisation. This new culture is developing around a new shared identity that is relatable to everyone in the bank. Concerning the transitionary state, the organisation admits the difficulty of describing the current organisational culture partly because the organisation is in the process of redefining itself.

5.2.1.1 Underlying Assumptions

Create a climate for change

The organisation operates in a highly regulated industry, and compliance is at the heart of the organisation's culture. However, the compliance culture that was previously in the organisation was responsible for creating a climate of fear and blame, resulting in people distrusting leadership with very little inter-departmental collaboration. It stifled innovation.

Transforming the culture to be more open and inclusive required creating a climate for the change. Kotter (2012) proposes the following as the initial processes of creating the environment for change: 1) creating a sense of urgency; 2) building a guiding coalition, and 3) forming a strategic vision for change. The following sections discuss how the organisation has been able to create a climate for creating a cybersecurity culture of the organisational culture.

Culture transformation is about winning the head, heart and hands of the organisation for change to stick. To align the organisation to the required for change, Kotter (2012) proposes (as a first step), that leadership has to create a sense of urgency. One of the participants noted that the leaders of the organisation communicated that the organisation needs to transform into a digitally-led organisation or risk becoming irrelevant to the market. Kotter (2012) supports that creating urgency is essential in the process of securing buy-in around a new strategy. Employee buy-in seeks the commitment of the individual for the proposed changes and notes that the unit of change is the individual employee. However, with the strategy to be digitally led come new challenges of cybersecurity risks, and these require the whole organisation to be vigilant of

associated threats. Leadership had to create a sense of urgency around the needed levels of vigilance to protect and safeguard the organisation against the emerging cybersecurity risk. Managing risk has been at the core of everyone's job, and cybersecurity is an emerging form of risk to be managed by everyone.

The education and awareness training programmes are deliberate techniques used by leadership to create a sense of urgency and communicate the desired cybersecurity behaviours and attitudes. All the interviewed participants agree that the organisation provides extensive awareness training on cybersecurity as well as the desired actions to prevent and report potential breaches. All participants were able to identify some of the potential cyber threats and their impact on the business should they be successful. Reid & Van Niekerk (2014b) argue that awareness alone is not enough to change a culture; the people would like to act out the desired behaviours. Awareness needs to convert into a common understanding that then becomes part of the shared values of the organisation for it to translate into a habit. The process of moving from awareness into practice requires the leaders to display empathy and be authentic, Reid & Van Niekerk, (2014b).

Shared understanding and language relating to cybersecurity achieved through awareness training made mandatory with no tolerance accepted for non-compliance. Coercion is used in the initial stages of culture-building as people are usually reluctant to change, Reid & Van Niekerk (2014b). Since culture takes time to create regular and consistent workshops and training reinforce the desired behaviours, and they should be very pragmatic, Bada & Sasse (2015). The leadership makes the awareness very visible through the use of various forms of media to communicate the urgency and these could include, storytelling, cite data, video, print, digital and leadership engagement through town halls with consistent and authentic messaging.

Kotter (2012) shares that the second step in the model involves the creation of a guiding coalition. Given the size of the organisation, 42 000 employees strong, the desired transformation needs to be driven from leadership. The cybersecurity function is the formal champion of the change; however, it collaborates with leaders of the other services. According to one of the participants, "I think culture

is almost passed by osmosis", therefore creating a guiding coalition of business leaders closer to staff, and trust by their people enables the spreading of the message as well as getting feedback and insights from the organisation. The collaboration may be both formal and informal and is instrumental in driving the desired change throughout the organisation.

Richardson (2008) states that the importance of leadership sponsorship of a transformation initiative to give it a high priority. The CEO of the organisation recognises the importance of cybersecurity to the success of the organisation's strategy to be digitally-led and endorsed the formation of a well-resourced cybersecurity function with a leader, chief security officer, who is part of the organisation's executive committee. The cybersecurity function is part of the chief security officer's office, charged with forming a strategic vision for the organisation's fraud and anti-money laundering, physical and cybersecurity.

5.2.1.2 Artefacts

Engage and Enable the Organisation

Engaging employees creates a connection between the leadership and employees and is critical in the development of a trust-based relationship. Kotter (2012) suggests that engagement is vital in winning the hearts of the individuals within an organisation. An engaged workforce is more productive and loyal to an organisation, Merritt (2002). The organisation utilises townhall sessions to promote open and honest communication through a platform for two-way conversations. The organisation can get the same information at the same time to ensure trust between leadership and employees. Through these engagements, the employees feel they are part of something, and their voices can be heard and can contribute to the success of the business. These are all critical aspects of the open and inclusive culture developing in the organisation.

The leadership encourages courageous conversation as a way of keeping each other honest and accountable. Courageous conversations are conversations that transcend the barriers of hierarchy and patronage, Brisson-Banks (2010). People are encouraged to make their voices heard; some speak up; however, there are

still others that do not trust the system and choose not to speak out. The previous culture of command and control could be responsible for these behaviours.

The organisation makes use of a whistleblowing hotline to encourage the reporting of behaviours not aligned to the organisational practices; it is a management system for peer-review behavioural conduct. The whistleblowing hotline is both anonymous and independently managed to ensure the protection of the whistle-blower.

People are creatures of habit and are generally reluctant to change, Todnem BY, (2005). To just start the process of transforming the employee behaviour to be more vigilant, the organisation employed technology-supported techniques for screening emails. The non-intrusive, low learning curve results in faces minimal resistance and quick users' adoption. The number of emails that employees test for suspicious content has decreased the number of phishing emails opened. The disabling of features on the end-user devices like the USB port on laptops altered the need for employees to want to use external storage devices but instead used the company sanctioned platforms. Automatic system upgrades of end-user devices remove the hurdle of having the employees consciously remember to do the updates. The use of the technology-enabled mechanism of driving desired behaviour enabled the cybersecurity function to have early wins in the culture-building process.

5.2.1.3 Espoused Values

Implementing and Sustaining for Change

Developing a culture is not a once-off event, but rather a continuous and ongoing process that requires sustained and consistent awareness training and communication around the desired behaviours. All the participants highlighted that organisations conducted mandatory awareness training at least once a year; however, during the year, they receive communication via various media on the subject. When the cybersecurity functions pick up potential threats either from the market or internally, they make use of ad-hoc communications to raise awareness so that employees become increasingly vigilant.

What gets rewarded gets repeated until it becomes a habit. The organisation recognises and celebrates individuals and departments that exhibit exemplary behaviour. The incentives serve to reinforce the desired behaviour as well as encouraging engagement among the organisation. The organisation has also won several awards for its cybersecurity function, and these awards and recognition serve as a source of pride for the organisation – a reason for employees to wish to be associated with it.

5.3 Discussion on Research Question 2

5.3.1 *Leadership*

5.3.1.1 Leadership style

The organisation's culture transformation from a command and control culture to an open and more inclusive culture, the leaders in the organisation, need to adopt an appropriate leadership style. The current leadership style in the organisation is both transactional and active transformational, McKnight (2013) states that these styles of leadership are complimentary. As the organisation operates in high compliance and regulated industry, active transactional leadership is adopted to get everyone to complete their training. Incentives and disciplinary action drive behaviour, McKnight (2013). Three of the participants reported that the consequences for non-compliance with the awareness training led to either being denied access to the organisation's systems or getting a final warning letter.

Transformational leadership style allows leaders to gain the trust of the organisation through leadership displaying exemplary behaviour. Bolden (2010) argues that leaders have to share a compelling vision that the employees can relate with to encourage the behaviour change. Transformational leadership places focus on the needs of the individual, Holten & Brenner (2015). This leadership style is vital in trust-building between the leadership and employees, with the organisation promoting openness and transparency. One participant remarked that they were reluctant to change unless provided with a compelling argument on the need to more vigilant. Intellectual stimulation, charisma,

inspirational motivation and individual considerations are the characteristics of this leadership style, Holten & Brenner (2015). Organisational commitment to change is significant for transformational leadership and results in higher adoption of the desired behaviours and attitudes, McKnight (2013). The organisation appointed as the chief security officer CSO, a security expert with significant experience and industry respect both locally and international. The chief security officer has been vital in developing a compelling vision and strategy for the organisation's security.

Leadership as change agents influence the success of the change by role modelling the desired behaviours, Cameron & Green (2009). One participant highlighted the importance of leadership walking the talk and espousing the desired values as key to how they, in turn, behaved.

The chief security officer CSO needs to influence other leaders to share the message and espouse the desired attitudes to all sections of the business. The ability to influence other leaders requires sponsorship from the CEO to ensure that there are cultural transformations and adoption of cybersecurity mindset as a common thing across the business. The leadership of the cybersecurity function, through their position at the highest level of the organisation, needs to demonstrate that the service is not another oversight role, but rather an integral part of the business.

5.3.1.2 Cybersecurity Strategy

External forces due to changing customer behaviours and expectations, coupled with the innate need for increased operational efficiencies are the fundamental driving forces behind the organisation's current strategic direction. The transformational change of strategy to be more digitally focused as well as the internal supporting structures and processes, Cummings & Worley (2009) resulted in the creation of a cybersecurity function. The cybersecurity function provides guidance and strategic direction for the organisation in managing cybersecurity risk. The development of a cybersecurity strategy and the creation of the cybersecurity function supported by the view of Batteau (2011) that

suggests that transformational change requires a change in policy and organisational design.

The cybersecurity function developed a strategy to mitigate the impact of cybersecurity risk on the business and aligned to the organisational strategy. The cybersecurity function and the corporate strategy are aligned to minimise the effect of change fatigue within the organisation, Cameron & Green (2009). The cybersecurity function is a well-resourced with a significant budget for awareness and communication, talent development and recruiting, and corporate social initiatives (CSI). The service is centralised, providing support to all the business units within the organisation. The centralisation is a result of an organisation redesign to optimise and leverage of efficiencies of having a central security function from the scarce and underutilised skills and expertise localised in the different business units.

5.3.2 *Organisational Design*

5.3.2.1 Technology

For an organisation going through a massive transition and repositioning, there is a risk of creating change fatigue among employees by introducing a lot of new things at the same time. Technology has been pivotal in driving behaviour change in how employees share and store files. Technology supported mechanisms implemented which are non-intrusive and work in the background. The removal of USB ports and quarantining of suspicious emails before opening are some of the initiatives that the bank has undertaken. Others include the restriction of access to certain services from non-standard issued company devices.

5.3.2.2 Structure

The organisation is designed based on a divisional structure as shown in figure 6 below, indicating the constituent business units of the organisation. The divisional structure is outcomes orientated, enabling each business unit to focus wholly on a particular market and product segment, Absa Group Limited (2019).

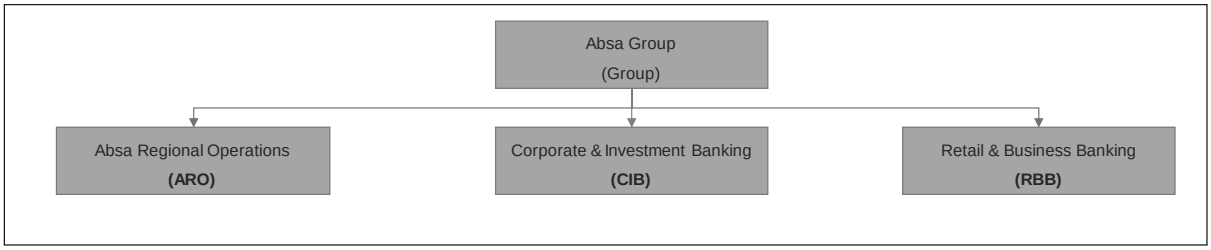


Figure 6: The Divisions of the Organisation

The individual business units, including group, are designed based on a functional structure. The functional structure enables the business units to be independent entities staffed with specialists and led by experienced leaders, Tiller, (2012). The group is a non-revenue producing business unit that provides shared services on governance and operational capability to the rest of the business units. Figure 7 below shows the functional structure of the group with the cybersecurity function as one of the functional units within the group.

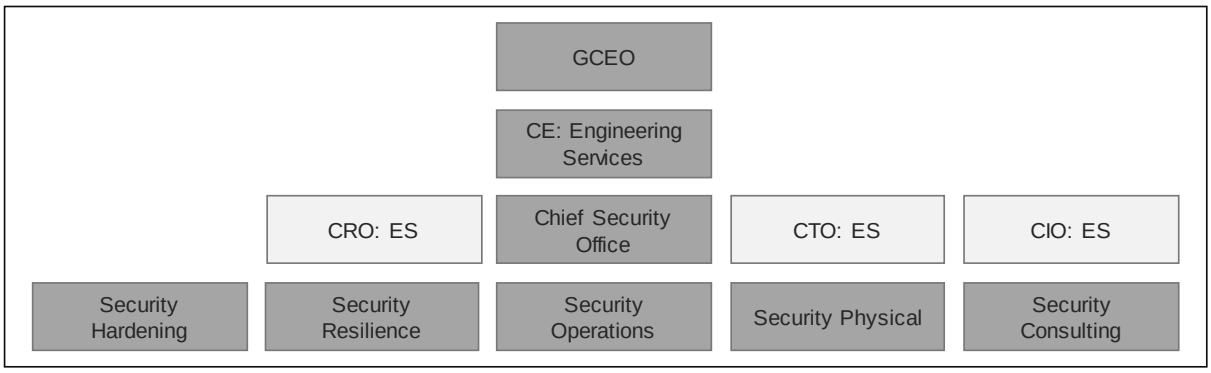


Figure 7: The Group's Security Functional Structure

The cybersecurity function was previously one of the many domains in Information Technology focused on protecting the organisation's information management systems. Based on the previous organisational design that has information security under technology, 6 of the 8 participants shared that we are not in cybersecurity. The functional structure highlights one of the disadvantages outlined by Cummings & Worley (2009) of limiting the view of the employees to the holistic organisational task.

The centralised security function responsible for fraud and anti-money laundering, cybersecurity and physical and personal security supports all the business units in the organisation. The service is headed up by a chief security officer, CSO. The CSO has a seat on the organisation's board committee on

Information Technology reporting on all matters security including mitigation and protection plans for Absa Group Limited (2019). Members of the committee include Exco members (CEO, FD, CE Engineering Services and two independent directors) and non-Exco members (CIO, CRO Engineering Services, CSO, CDO).

Security resources previously localised within the business units moved to the central function. The centralisation of resources and skills enables the organisation to reduce duplications of services and optimises the use of talent and resource allocation (Cummings & Worley, 2009; Tiller, 2012). The CSO is supported by leadership within security looking after five broad areas of security, namely, security resilience, security operations, security consulting, security hardening and security physical. The specialist nature of security and its subfunction requires that the structure is supported by specialist units, Cummings & Worley (2009). These areas are well-staffed with the appropriate skills and expertise and are well-resourced to achieve targets assigned to them. The centralised security function provides both governance and operational support to the rest of the group.

The interdependencies between the security function work and the technology and risk functions resulted in increased collaboration between the services. The functional structure supports the required degree of cooperation due to the interdependencies between the services. The CSO is responsible for protecting and mitigating the impact of internal and external risks and the screening of new technology in development, preproduction. The risk office assures the threat landscape for the live environment.

5.3.2.3 Management System

A sound management system is critical in supporting the structure to deliver on the overall organisational strategy, Tiller (2012) and laying a solid foundation for the operations of the organisation, Cummings & Worley (2009). Risk management is a management system enforced through the guidelines and frameworks outlining the Enterprise Risk Management framework used to manage and mitigate risk. Cybersecurity is a new risk, reduced through the risk

management system. The organisation's well-defined governance and control processes for managing and mitigating risks extend to managing cybersecurity risk. This is attributable to the high degree of compliance required in the highly regulated sector where the regulatory bodies conduct regular audits to ensure compliance, Absa Group Limited (2019). The enterprise risk management framework is supported by;

1. A robust and consistent governance structure
2. Well defined risk categorisation (principle risks)
3. Clear accountability for the management and oversight of risk through the implementation of three lines of the defence operating model
4. A holistic approach to evaluation, response and monitoring of risk
5. Well defined and robust risk operating model outlining roles and responsibilities of stakeholders

The governance and control function serves as risk monitoring and reporting function. It provides input to the governance committee that tracks the organisation's risk appetite and provides mitigation procedures. The governance and control based on frameworks developed from industry best practices define the processes and procedures of managing the risk. It measures compliance with the pre-defined structures. Management systems support the organisation with compliance with regulatory and legislative requirements by providing support for governance and control and reporting on performance. The governance and control functions assess the potential risk, such as cybersecurity risk, based on directives from leadership. The outcome of the assessments informs the type of remedial action required to either avoid or absorb the risk. The management systems play an essential role in communicating the desired behaviours and provide feedback to leadership on the impact of the change, Cummings & Worley (2009).

The mandatory compliance courses provide the organisational learning of the desired new behaviour and the types of threats to cybersecurity and their

implication on the business—the compliance courses delivered as computer-based training via an online portal on the organisation's intranet. Organisational learning is vital in developing a shared understanding and knowledge for improved organisational performance, Wang & Ahmed (2003). Organisational learning ensures that the organisation is prepared to adapt to changes in the environment by continually learning and adjusting accordingly, Saadat & Saadat (2016). The course material is kept up-to-date and relevant and engaging.

The learning platform is integrated with the individual performance reports, providing input to the incentive system. Failure to comply can result in disciplinary action against the individual. Some of the disciplinary actions include system lockout or final written warnings. Full compliance is celebrated and rewarded.

The whistleblowing hotline is an anonymous platform for employees to report suspicious behaviours. It's a peer control mechanism that empowers employees to have a voice they would ordinarily not use to speak up.

5.2.3.4 Human Resources Management

An engaged, motivated workforce is more productive and committed to the organisational strategy, and this is observed through the organisational performance, Cummings & Worley (2009). Employee engagement is achieved by empowering, sharing information, training and incentivising the desired behaviour, Cameron & Green (2009). These four elements are interdependent and should be addressed together for maximum output. The leadership through quarterly townhall meetings engages the organisation in two-way conversations. These promote inclusivity, openness and transparency, the core values of the new organisational culture.

5.4 Conclusion

The organisation has a compliance culture as a subculture of its organisational culture; the creation of a cybersecurity culture enhances the compliance culture. The process of culture building is slow and protracted, requiring continuous reinforcement; however, alignment to the vision is needed. The organisation

achieved alignment by creating a sense of urgency based on the need to survive in a turbulent market environment that is rapidly transforming. To ensure the whole organisation is aligned and understand the expected behaviours, structured and mandatory awareness and training programs provide continuous reinforcement. Through these initiatives, the organisation can create a shared understanding and awareness on the risk to cybersecurity and the expected actions to protect, prevent or manage the impact of successful breaches.

The increasing number of people reporting suspicious emails and events indicates that the awareness messages are taking hold in the people. Rewarding and celebrating individuals who exhibit exemplary behaviours and attitudes to cybersecurity is also instrumental in reinforcing the desired culture. The public celebration and rewarding of desired actions align with the need for greater openness and transparency.

The organisation was redesigned in alignment with the organisational strategy, to include a centralised security function responsible for security-related issues including cybersecurity. The service provides governance and operational support to the other business units within the organisation. The centralisation of the services enabled the organisation to leverage the scarce skills and expertise that were localised in the various business units while reducing duplication of systems.

Through the guidance and leadership of an experienced security expert, with vast industry experience leading organisations of similar sizes, the security function is viewed as a business priority, not a value-added service. They can influence and collaborate with other members in the leadership to drive the cybersecurity culture within the rest of the business.

Structured processes and procedures make up part of the management system supporting the creation of the cybersecurity culture. These include the enterprise risk management framework which provides guidelines on how to manage risks, including cybersecurity. The computer-based training platform offers a measurable system for which the organisation can measure and report on employee engagement with the awareness training. The system generates

certificates upon successful completion of an assessment of one's understanding of the taught concepts. These certificates have been used as an indication of the organisation's knowledge of the threats, risks, implications and required actions to prevent or mitigate the impact of cybersecurity breaches.

People are reluctant to change and require coercion for initial buy-in from everyone; hence the organisation integrates the output of the compliance training with the performance management system. The integration of the learning and performance management systems ensures full compliance with training by rewarding compliance and disciplining non-compliance.

CHAPTER 6. CONCLUSIONS & RECOMMENDATIONS

6.1 Introduction

This study set out to explore the role of leadership in cybersecurity culture in the South African financial services sector. It focused on senior managers from different functions with the organisation's group structure. The choice was made based on the role they played in strategy implementation. The managers provided insights based on their lived experience of the initiatives undertaken by the organisation's leadership in creating and sustaining a cybersecurity culture within the organisation expressed in the participant's voices. This is vital in exposing the underlying assumptions and espoused values within the business.

This chapter provides a summary of the research process, findings and the conclusions based on the discussions of the two research questions and provides recommendations and areas of future research.

6.1.1 *Summary of the research process*

The aim of the study is restated as follows;

- To explore how a behaviour-based approach to cybersecurity can be implemented and nurtured within an organisation through the creation of a cybersecurity culture. The study focused on how the approaches and methods were used by the organisation's leadership to develop and sustain the cybersecurity culture.
- To understand the lived experiences of the senior managers who had to implement the change and lead their followers in adopting the desired behaviours aligned to the organisational change.

In fulfilling the aim of the study, a problem statement is formulated on the adoption of a behaviour-based cybersecurity approach focused on changing the organisational culture. This approach is similar to the one adopted by the safety-critical sector in the adoption of a safety culture to mitigate fatalities and incidents due to human negligence. A review of the available literature on the relationship

between leadership, organisational culture and organisational change management provided insights into culture development. Two research questions were formulated to explore the problem and these were;

1. What type of organisational culture supports a cybersecurity culture?
2. How does the leadership build and embed a cybersecurity culture in an organisation?

The design of the study is based on a single case study focusing on one of the leading financial institutions in South Africa. The qualitative case study employed semi-structured interviews with a selection of eight senior managers from the institution, the primary data collection method. The interviews were conducted at the institute's premise to enable observations of non-verbal cues based on the interactions within the organisations. The observations and publicly available documentation provided a secondary source of data.

Though the interview sought to explore the role of leadership, the institution's policy prohibited top leadership from participating in interviews with students. Failure to access top leadership proved to be a challenge in that, this limited visibility into the strategy formulation process and the insights into the desired culture and its relationship to cybersecurity.

The following sections discuss the conclusions regarding the two research questions posed in this study.

6.2 Conclusions regarding research: Question 1

An organisation has a climate and a culture. The organisation's climate components include the obvious things that people may identify and are usually tangible. These include artefacts (the brand, corporate identify, etc.), behaviours and metrics found in an organisation. They are easy to change and are usually the areas of initial focus for culture transformation. The organisational climate focuses on winning the minds of the individuals in the organisation by providing awareness and understanding of the desired behaviours. Leaders' behaviours

exemplify these behaviours and should always be consistent and authentic for the employees to embody them.

The leadership has created a climate that promotes openness and encourages innovation. There are, however, some individuals within the organisation, due to the legacy culture, that distrust leadership and require coercion. The findings of this study indicate that in some instance's coercion was required to get people to comply with the cyber security related training despite leadership's effort to create an open and transparent culture that motivates individuals. The leadership style and culture dynamic is an interesting finding however, it was not the focus of this study and should be explored in further research. Misalignment between the behaviours and attitudes of participants and the climate created within the organisation. The environment allows employees to develop and grow while being exposed to leading industry's best practices. According to Schein's organisational culture model artefacts, metrics and values are easy to change, and changes in the organisational climate may change these.

The other components of organisational culture are invisible and much more difficult to change over protracted periods to take hold of in an organisation. These are intangible and often the source of the common assumptions and attitudes; they may include beliefs, values and assumptions held collectively by the organisation. These components focus on the hearts and hands of the individual within the organisation to exemplify their desired behaviours and incorporate them as part of the core value system.

The behaviours and attitudes exhibited by some of the participants may be attributed to their professional training and expectation and not as a general rule for the whole organisation. The employees rely on trust and professionalism of colleagues since the organisation empowers them to know what they have to do, and they then do it. Those with Information Technology and Internal Audit-related experiences exhibited a higher degree of caution and compliance than their counterparts. They tended to exemplify the security-inspired trust but verify mentality by not accepting things at face value, including the author's request for an interview.

The cybersecurity culture is a culture of vigilance and agility in responding to internal and external cybersecurity risks and includes a shared understanding of the course of action to take in response to and in preventing a cyberattack. It involves the shift from awareness to behaviour and attitude. However, for an organisation that operates in a highly regulated sector, compliance policies and procedures guide the way people in the organisations work. Hence, the organisation had a minimal learning curve altering the behaviour of the organisation as compliance and risk management is ingrained in their DNA.

The awareness training has enabled the creation of a shared understanding and resulted in some early wins with people reporting cases of suspicious emails and objects within the environment. The challenge is making these observed behaviours and translating awareness into action among the majority of the organisations. Instilling the “fear of God” into employees for non-compliance to training and reinforced with written warnings is considered a quick but painful process of raising awareness among employees.

Increased exemplary behaviour is required to demonstrate more of the desired actions, especially concerning cybersecurity. Leadership has been instrumental in building trust within the organisation through open and honest communication. They realised that if they are going to change the culture, they will need to win the hearts and minds of the people.

Due to the transitionary state of the organisation, the organisational culture is yet to stabilise, and once it is stable, it might be appropriate to strengthen the cybersecurity culture, hence the increased focus on awareness building. As the new organisational culture is yet to mature, so too is the cybersecurity culture. The gap between awareness and making it part of the corporate culture has not been brought close enough, in part due to the current state of the organisation.

6.3 Conclusions regarding research: Question 2

Since leadership is navigating the organisation in a new strategic direction, the leadership style adopted encourages greater collaboration and communications across departments for greater information-sharing and transparency. Leaders

engage and walk the talk, so they are perceived as authentic and believable in their messaging to build trust with the rest of the organisation. Leadership exemplifies collaboration by engaging and sharing information among the leaders from the various sections.

While the organisation has acknowledged cybersecurity as a significant emerging risk, some of the participants still view it as a technology risk that is part of information security and as such confine its responsibility to that section of the business. Cybersecurity risk is considered a technology risk that indirectly impacts individuals within the organisation addressed through technology and processes.

Due to the sensitivity of the data reporting, the organisation was unable to share this information; however, it was able to decrease incidents and increase reports from staff of suspicious activities. This reporting on cybersecurity was done at the executive committee level to inform the strategy formulation.

There appears to be no formal tracking and monitoring internally on levels of the return of investment on the awareness education in driving the behaviour over time from the period they started. Improvements in the adoption of the desired behaviour are based purely on the sentiment of the increasing identification of suspicious messages.

6.4 Recommendations

6.4.1 *Practitioners*

The adoption of technology both in the workplace and at home has created an informed and knowledgeable workforce opting to be engaged than to be coerced into behaving in a particular manner. Leaders of organisations embarking on digital transformation programs need to be deliberate in their change management processes. Employees require the organisation’s leadership to provide them with a compelling case for change to ignite the sense of urgency for the change within the organisation. The leaders need to be empathetic to the employees and authentic in their actions to build trust with their followers. Kotter’s

8-step model for change provides insights for a framework adopted for managing change.

6.4.2 *Academics*

This research contributes to the body of knowledge of organisational development, focusing on the creation of a cybersecurity culture within an organisation. It can provide a foundation for the development of their research design for further research into the development and sustainability of the cybersecurity culture in other organisations or industries.

6.5 Suggestions for further research

The rapidly changing business environment requires organisations with greater agility to respond faster to both internal and external threats. Cybersecurity risk is an example of rapidly evolving threats requiring vigilance and responsiveness in the organisational response. The alertness and agility baked into the organisation's DNA are similar to heightened levels of compliance. The participants cited the low level of both corporate and cybersecurity culture maturity. A potential area of further research would be exploring the cybersecurity maturity levels of organisations within the financial services sector.

Awareness building is vital in developing a shared understanding within an organisation of the expected behaviours and attitudes. The awareness-building process requires significant investment to create relevant and engaging content that is continuously updated. Based on the findings from this study, there is no adequately defined quantification of the effectiveness of the awareness-training on building a behaviour-based cybersecurity defence. Therefore, potential research would be to develop a model to predict the return on investment on awareness-training in the reduction of cybersecurity breaches.

The financial services sector in South Africa is one of the most regulated in the world, with several regulatory bodies providing oversight into the sector's activities. Since cybersecurity risk is another type of risk-managed through a well-defined risk management framework and controls, there is a low learning curve

in embedding a cybersecurity culture to the existing risk and compliance culture. However, the new reality that every business will at some point probably be a victim of cybercrime, a potential area of research would be how leaders in under-regulated sectors of the economy develop and nurture cybersecurity culture in their organisations.

The findings of this study indicate that in some instance's coercion was required to get people to comply with the cyber security related training despite leadership's effort to create an open and transparent culture that motivates individuals. The leadership style and culture dynamic is an interesting finding which should be explored further in in future research to provide sufficient insights into the logic of this motivation versus coercion dynamic.

6.6 Conclusion

Digital transformation promises organisations of all sizes the competitive advantage required to remain relevant to customers at a time when switching costs are low for customers. These transformations are organisation-wide and range from improvements in customer experience, operational efficiencies and business models. Along with these changes is the emergence of cybersecurity risk, while technological and process controls are available to mitigate the impact of cybersecurity breaches, the human remains the most significant attack vector for cybercriminals.

This study discovered that creating a culture of vigilance to dangers posed by cybersecurity risks is vital in developing a cybersecurity culture. Education and awareness are critical in driving the message of the desired and expected behaviour and attitudes. Numerous methods of generating awareness are employed to drill the message into the hearts of the followers. The message is compelling and inspiring to drive the adoption of the desired behaviour by the followers. Due to the high levels of regulations and compliance within the financial services sector, the organisation was moving to merge its compliance culture with the emerging cybersecurity culture.

Awareness does not translate into behaviour change; the leadership of the organisation needs to be intentional and authentic in their action by ensuring alignment with the desired action. The followers perceive the leadership's language and actions as consistent with their message leading to employee buy-in. The intentional and clearly defined change process is implemented to ensure the success of the organisational transformation.

The organisation supported their strategy by creating a well-resourced and expertly led security function to lead the cybersecurity initiatives and to report progress at the highest committee – the board's information technology committee.

Culture takes a long time to develop; the organisation is in the middle of an organisational transformation process and is laying the foundation by creating a climate aligned to the new strategy. The findings of the study illustrate that most of the changes implemented to focus on creating the right climate to foster the creation of the cybersecurity culture.

REFERENCES

Absa. (2020). *Absa | Learn more about a leading bank in Southern Africa and our values*. Absa. Retrieved from https://www.absa.co.za/about-us/absa-bank

Absa Group Limited. (2019). *Absa Group Limited 2018 Integrated Report* (p. 90). Retrieved from https://www.absa.africa/content/dam/africa/absaafrica/pdf/reports/2018/absa-group-2018-integrated-report.pdf

Absa Group Limited. (2020). *Absa Group Limited Financial results for the reporting period ended 31 December 2019* (p. 178) [Annual Report]. Retrieved from https://www.absa.africa/content/dam/africa/absaafrica/pdf/sens/2020/Results-booklet-for-the-period-ended-31-December%202019.pdf

Bada, M., & Sasse, A. M. (2015). *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?*

Barriball, K. L., & While, A. (1994). Collecting data using a semi-structured interview: A discussion paper. *Journal of Advanced Nursing*, *19*(2), 328–335. https://doi.org/10.1111/j.1365-2648.1994.tb01088.x

Bass, B. M. (1990). From transactional to transformational leadership: Learning to share the vision. *Organizational Dynamics*, *18*(3), 19–31.

Bass, B. M., & Bass, R. (2009). *The Bass Handbook of Leadership: Theory, Research, and Managerial Applications*. Simon and Schuster.

Bass, B. M., & Riggio, R. E. (2006). *Transformational Leadership*. Psychology Press.

Batteau, A. W. (2011). Creating a culture of enterprise cybersecurity. *International Journal of Business Anthropology*, *2*(2).

Bloomberg, L., & Volpe, M. (2008). *Completing Your Qualitative Dissertation: A Roadmap from Beginning to End*. SAGE Publications, Inc. https://doi.org/10.4135/9781452226613

BMI. (2017). *Banking—South Africa—Q1 2018*. Retrieved from https://0-bmo-bmiresearch-com.innopac.wits.ac.za/article/view?article=1316630&advanced_search=1&matches=8901&page=1&position=5&keyword=south%20africa%20banking%20sector

Bolden, R. (2010). *Leadership, Management and Organisational Development*. 11.

Bollinger, A. S., & Smith, R. D. (2001). Managing organizational knowledge as a strategic asset. *Journal of Knowledge Management*, *5*(1), 8–18. https://doi.org/10.1108/13673270110384365

Brisson-Banks, C. V. (2010). Managing change and transitions:a comparison of different modelsand their commonalities. *Emerald Insight*, *31*(4), 241–252. https://doi.org/10.1108/01435121011046317/full/html

Bukht, R., & Heeks, R. (2017). *Defining, Conceptualising and Measuring the Digital Economy* (SSRN Scholarly Paper ID 3431732). Social Science Research Network. https://doi.org/10.2139/ssrn.3431732

BusinessTech, S. (2019). *Barclays is pulling out of Absa: Report*. Retrieved from https://businesstech.co.za/news/banking/109371/barclays-is-pulling-out-of-absa-report/

Cacioppe, R., & Edwards, M. (2005). Seeking the Holy Grail of organisational development A synthesis of integral theory, spiral dynamics, corporate transformation and action inquiry. *Emerald Insight*, *26*(2), 20. https://doi.org/10.1108/01437730510582536/full/html

Cameron, E., & Green, M. (2009). *Making Sense of Change Management: A complete guide to the models, tools and techniques of organisational change* (2nd ed.). Kogan Page.

Cameron, K., & Quinn, R. E. (2006). *Diagnosing and Changing Organisational Culture: Based on the Competing Values Framework*. John Wiley & Sons.

CISOMAG. (2020, March 2). *Found 10% Increase in Ransomware Attacks in 2019: Trend Micro*. CISO MAG | Cyber Security Magazine. Retrieved from https://www.cisomag.com/found-10-increase-in-ransomware-attacks-in-2019-trend-micro/

Coetzee, J. (2019). Banks' branch closures point to need for new business model. *The Citizen*. Retrieved from https://citizen.co.za/business/2105664/banks-branch-closures-point-to-need-for-new-business-model/

Connelly, M. (2016). *The Kurt Lewin Model Of Change*. Change Management Coach. https://www.change-management-coach.com/kurt_lewin.html

Creswell, J. W., & Poth, C. N. (2017). *Qualitative inquiry and research design: Choosing among five approaches*. Sage publications.

Crotty, M. (1998). *The Foundations of Social Research Meaning and Perspective in the Research Process*.

Cummings, T. G., & Worley, C. G. (1989). Organisational development and change. *Ausg. St. Paul Ua: West Pub. Co*.

Cummings, T., G., & Worley, C., G. (2009). *Organisation Development & Change* (9th ed.). Cengage Learning.

Cummings, T. G., & Worley, C. G. (2014). *Organization development and change*. Cengage learning.

de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1–7.

Decisions, I. S. (2020). *Insider Threat Statistics: The seriousness of insider threats, intentional or not*. IS Decisions. Retrieved from https://www.isdecisions.com/insider-threat/statistics.htm

Denzin, N. K., & Lincoln, Y. S. (2008). Introduction: The discipline and practice of qualitative research. In *Strategies of qualitative inquiry, 3rd ed* (pp. 1–43). Sage Publications, Inc.

Dolan, P., Hallsworth, M., Halpern, D., King, D., & Vlaev, I. (2010). *MINDSPACE: Influencing behaviour for public policy* [Monograph]. Institute of Government. http://www.instituteforgovernment.org.uk/publications/

ENISA. (2018). *ENISA Threat Landscape Report 2017* [Report/Study]. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017

Esterberg, K. G. (2002). Qualitative methods in social research. *McGraw-Hill Boston, MA*.

FitchSolutions. (2020). *South Africa Banking & Financial Services Report Includes 10-year forecasts to 2029* (Market Report Q2 2020; p. 52). Fitch Solutions.

Flyvbjerg, B. (2006). Five Misunderstandings About Case-Study Research. *Qualitative Inquiry*, *12*, 219–245. https://doi.org/10.1177/1077800405284363

Gandolfi, F., & Stone, S. (2017). The emergence of leadership styles: A clarified categorization. *Review of International Comparative Management*, *18*(1).

Goodman, E. A., Zammuto, R., & Gifford, B. D. (2001). *The competing values framework: Understanding the impact of organizational culture on the quality of work life - ProQuest*. https://search.proquest.com/docview/197988769?pq-origsite=gscholar

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Externalities and the magnitude of cyber security underinvestment by private sector firms:

A modification of the Gordon-Loeb model. *Journal of Information Security*, *6*(1), 24.

Gubrium, J. F., & Holstein, J. A. (1998). *NARRATIVE PRACTICE AND THE COHERENCE OF PERSONAL STORIES | Kopernio*. https://kopernio.com/viewer?doi=10.1111%2Fj.1533-8525.1998.tb02354.x&token=WzE5OTUyMzQsIjEwLjExMTEvai4xNTMzLTg1MjUuMTk5OC50YjAyMzU0LngiXQ.4o2iinfc28TAOfZwrwj8TatzwkU

Guldenmund, F. W. (2000). The nature of safety culture: A review of theory and research. *Safety Science*, *34*(1–3), 215–257.

Hambrick, D. C., & Mason, P. A. (1984). Upper echelons: The organization as a reflection of its top managers. *Academy of Management Review*, *9*(2), 193–206.

Hartmann, P., & Henkel, J. (2020). The Rise of Corporate Science in AI: Data as a Strategic Resource. *Academy of Management Discoveries*. https://doi.org/10.5465/amd.2019.0043

Hohman, P. (2015). Managing Cyber Threats. *Canadian Underwriter*, *82*(5), 48–49.

Holten, A.-L., & Brenner, S. O. (2015). Leadership style and the process of organizational change. *Leadership & Organization Development Journal*, *36*(1), 2–16. https://doi.org/10.1108/LODJ-11-2012-0155

Intellidex. (2018). *Transformation in the banking industry 2016—2017* (p. 28). The Banking Association of South Africa. Retrieved from

https://www.banking.org.za/wp-content/uploads/2019/04/Transformation-in-Banking-Report-2016-17.pdf

Jones, S.R., Torres, V., & Arminio, J. (2011). Negotiating the complexities of qualitative research in higher education: Fundamental elements and issues. *Negotiating the Complexities of Qualitative Research in Higher Education: Fundamental Elements and Issues*, 1–213. https://doi.org/10.4324/9780203843758

Jones, Susan R. (2002). (Re)Writing the Word: Methodological Strategies and Issues in Qualitative Research. *Journal of College Student Development*, *43*(4), 461–473.

Kane, G. C., Palmer, D., Phillips, A. N., Kiron, D., & Buckley, N. (2015). Strategy, not technology, drives digital transformation. *MIT Sloan Management Review and Deloitte University Press*, *14*(1–25).

Keung, E. Z., McElroy, L. M., Ladner, D. P., & Grubbs, E. G. (2020). Defining the Study Cohort: Inclusion and Exclusion Criteria. In T. M. Pawlik & J. A. Sosa (Eds.), *Clinical Trials* (pp. 47–58). Springer International Publishing. https://doi.org/10.1007/978-3-030-35488-6_5

Kotter, J. (2012). *Leading Change* (2nd ed.).

Kumar, V., Srivastava, J., & Lazarevic, A. (2006). *Managing cyber threats: Issues, approaches, and challenges* (Vol. 5). Springer Science & Business Media.

Leech, B. L. (2002). Asking Questions: Techniques for Semistructured Interviews. *PS: Political Science & Politics*, *35*(4), 665–668. https://doi.org/10.1017/S1049096502001129

Matthews, H. (2008). Operational Risk. *Operational Risk*, *51*, 14.

McKnight, L. L. (2013). Transformational Leadership in the Context of Punctuated Change. *Journal of Leadership, Accountability and Ethics*, *10*(2), 10.

Merriam, S. B. (2002). Introduction to Qulaitative Research. In *Qualitative research in practice: Xeamples for discussion and analysis* (1st ed., p. 16). John Wiley & Sons.

Merritt, R. (2002). Cyber gurus: 'Culture of security' crucial, costly. *Electronic Engineering Times (01921541)*, *1237*, 18.

Mimecast. (2020). *The State of Email Security Report 2019* [Market Report]. Retrieved from https://cdw-prod.adobecqms.net/content/dam/cdw/on-domain-cdw/brands/mimecast/the-state-of-email-security-report-2019.pdf

Moneyweb, H. T. (2019). SA's 'big four' banks have shut down almost 700 branches this decade. *The Citizen*. Retrived from https://citizen.co.za/business/2140329/sas-big-four-banks-have-shut-down-almost-700-branches-this-decade/

Nanjundeswaraswamy, T. S., & Swamy, D. R. (2014). Leadership styles. *Advances in Management*, *7*(2), 7.

Nieva, V. F., & Sorra, J. (2003). Safety culture assessment: A tool for improving patient safety in healthcare organizations. *BMJ Quality & Safety*, *12*(suppl 2), ii17–ii23.

Patton, M. Q. (2016). Two Decades of Developments in Qualitative Inquiry: A Personal, Experiential Perspective. *Qualitative Social Work*. https://doi.org/10.1177/1473325002001003636

Phillips, R., & Tanner, B. (2019). Breaking down silos between business continuity and cyber security. *Journal of Business Continuity & Emergency Planning*, *12*(3), 224–232.

Pidgeon, N. (1998). Safety culture: Key theoretical issues. *Work & Stress*, *12*(3), 202–216.

Rahl, S. (2017). Research Design and Methods: A Systematic Review of Research Paradigms, Sampling Issues and Instruments Development. *International Journal of Economics & Management Sciences*, *6*(2), 5. https://doi.org/10.4172/2162-6359.1000403

Rana, N., Bansal, M., & Gupta, A. (2015). Organisational Development: A Paradigm. *Global Journal of Business Management*, *9*(1), 110.

Ray, J., Marshall, H., Coderre, R., De Sousa, V., Cody, E., & Jean, J. (2019). *2019 CYBER THREATSCAPE REPORT* (p. 102) [Market Report]. https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf

Reid, R., & Van Niekerk, J. (2014a). *From information security to cyber security cultures*. 1–7.

Reid, R., & Van Niekerk, J. (2014b). *Towards an Education Campaign for Fostering a Societal, Cyber Security Culture*. 174–184.

Reuters, R. (2020). *Company Profile for Absa Bank Ltd (ABSPp.J)*. IN. Retrieved from https://in.reuters.com/finance/stocks/company-profile/ABSPp.J

Richardson, K. A. (2008). Managing complex organizations: Complexity thinking and the science and art of management. *Emergence: Complexity and Organization*, *10*(2), 13–26.

Roopnarain, R. (2019). *South Africa Major Banks Analysis*. 17.

Saadat, V., & Saadat, Z. (2016). Organizational Learning as a Key Role of Organizational Success. *Procedia - Social and Behavioural Sciences*, *230*, 219–225. https://doi.org/10.1016/j.sbspro.2016.09.028

SABRIC. (2019). *SABRIC Annual Crime Stats 2018*. Retrieved form https://www.sabric.co.za/media-and-news/press-releases/sabric-annual-crime-stats-2018/

Saldaña, J. (2015). *The coding manual for qualitative researchers*. Sage.

Saunders, M. N., & Lewis, P. (2012). *Doing research in business & management: An essential guide to planning your project*. Pearson.

Schein, E. H. (2010). *Organizational culture and leadership* (Vol. 2). John Wiley & Sons.

Seidman, I. (2006). *Interviewing as qualitative research: A guide for researchers in education and the social sciences*. Teachers college press.

Shaver, E. (2014). *The Many Definitions of Leadership*. Eric Shaver. https://www.ericshaver.com/the-many-definitions-of-leadership/

Sorrell, J. M., & Redmond, G. M. (1995). Interviews in qualitative nursing research: Differing approaches for ethnographic and phenomenological studies. *Journal of Advanced Nursing*, *21*(6), 1117–1122.

Stake, R. E. (1995). *The Art of Case Study Research*. SAGE.

Strauss, A., & Corbin, J. (1998). *Basics of qualitative research: Techniques and procedures for developing grounded theory, 2nd ed* (pp. xiii, 312). Sage Publications, Inc.

Sun, N., Morris, J. G., Xu, J., Zhu, X., & Xie, M. (2014). ICARE: A framework for big data-based banking customer analytics. *IBM Journal of Research and Development*, *58*(5/6), 4: 1-4: 9.

Teoh, C. S., & Mahmood, A. K. (2017). *National cyber security strategies for digital economy*. 1–6.

The World Bank. (2020). *GDP growth (annual %)—South Africa | Data* [Market Information]. Data.Worldban.Org. Retrieved from https://data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG?contextual=default&end=2018&locations=ZA&start=2008

Tiller, S. R. (2012). Organizational Structure and Management Systems. *Leadership and Management in Engineering*, *12*(1), 20–23. https://doi.org/10.1061/(asce)lm.1943-5630.0000160

Todnem BY, R. (2005). Organisational change management: A critical review. *Journal of Change Management*, *5*(4), 369–380. https://doi.org/10.1080/14697010500359250

Treasury. (2019). *2019 Budget Review: Economic Review* (p. 14) [Budget Review]. SA Government Treasury Department.

Wang, C. L., & Ahmed, P. K. (2003). Organisational learning: A critical review. *Emerald Insight*, *10*(1), 8. https://doi.org/10.1108/09696470310457469/full/html

Yin, R. K. (2014). Case Study Research Design and Methods (5th ed.). *The Canadian Journal of Program Evaluation*, 282. https://doi.org/10.3138/cjpe.30.1.108

Zikmund, W. G., Babin, B. J., Carr, J. C., & Griffin, M. (2013). *Business Research Methods* (9th ed.). Cenage Learning.

APPENDIX (A) Participant's Information Sheet

Dear
Participant

Ref: Interview Request Letter

Mr Robert Mataruse **(Student No. 1297842**) is currently a Master of Management in Digital Business (MMDB) student, at the University of Witwatersrand's Business School. One of the core components required to graduate from this program is the completion of a research report.

Robert has chosen to perform his research in the **field of organisational culture, focusing on cybersecurity culture**. His research seeks to explore the role of leadership in building and embedding a cybersecurity culture within the South African financial services sector. Cybersecurity has become topical in recent years as companies focus on business strategies focused on transforming their organisations into digital businesses, due to the rising number of cyber-attacks and reported breaches. While technology provides a sufficient layer of defence against these attacks and breaches, human behaviour seems to be the major contributor for all successful breaches. The research will focus on understanding the process that the organisation is using to create and sustain a cybersecurity culture as a way to combat the impact of human behaviour on cybersecurity breaches.

Robert would like to explore the possibility of interviewing you for his research project. The duration of the interview would vary but is expected to take an hour on average and will not exceed an hour and a half. The discussion would be recorded on a dictaphone, then transcribed. Your position and company name would be kept anonymous to ensure confidentiality. The identity of your organisation will not be revealed in the thesis, rather it will just be representative of the sector, and none of the comments made by you or any individual will be explicitly linked to your company.

Please may you advise if Robert Mataruse may set up an interview by contacting him on the details below?

If you have any concerns, please contact my supervisor or me. Our details are provided below:

Yours
Sincerely

Robert Mataruse (Student)

+27 72 314 8100
robert.mataruse@gmail.com

Kiru Pillay (Supervisor)

+27 82 602 7261
Kiru2010@gmail.com

APPENDIX (B) Participant Agreement Form

Informed Consent Form: Participant

Robert T. Mataruse is currently completing his Master of Management in Digital Business (MMDB) at Wits Business School. One of the key components to be successfully admitted for this program is the completion of a Research Project.

Robert has chosen to perform his research in the field of Organisational Culture. His research explores the role of leadership in developing and nurturing a cybersecurity culture to mitigate incidents due to insider threats by creating new behaviours and norms in the ways of work.

The duration of the interview will vary but is expected to take an hour on average and will not exceed an hour and a half. The discussion will be recorded on a dictaphone, then transcribed. Your position and company name will be kept anonymous to ensure confidentiality. Although a list of all the functional areas represented by each interviewee will be stated in the thesis, none of the comments made by you or any individual will be linked to a specific person.

Your participation is voluntary and you may withdraw at any time without penalty.

If you have any concerns, please contact my supervisor or me. Our details are provided below:

Robert Mataruse (Student)

+27 72 314 8100
robert.mataruse@gmail.com

Kiru Pillay (Supervisor)

+27 82 602 7261
Kiru2010@gmail.com

Signature of participant: ……...Date…….

Signature of Researcher: ……..Date……..

APPENDIX (C) Instrument

Role of leadership in cybersecurity culture in the Financial Services Sector in South Africa: Interview Instrument

Introduction

- Thank you for agreeing to meet and speak with you.
- My name is Robert Mataruse (Student Number: 1297842), and I am currently a student at Wits Business School, studying for a Master of Management in the field of Digital Business. As part of the program, I am supposed to submit a research report; I chose to focus my research on:

  The role of leadership cybersecurity culture with the financial services sector in South Africa

- I would like to discuss with you to understand your lived experience as a leader within the business on how the organisation is building and nurturing a cybersecurity culture.
- Please note that your participation in this study is voluntary, and you may withdraw from the study at any point without any negative consequences.
- The estimated time for the interview is approximately 1 – 1.5 hours. Should they need to take a short break during the discussion, they are allowed.
- Would you mind if I were to record the discussion for my notes and your identity will be made anonymous in the final report.

Interview Questions

1. ***How would you define your role in the business? (Participant's self-introduction)***

   Probe:

   - What are your primary responsibilities?
   - How long have you been with the company?

2. ***How would you define the organisational culture?***

   Probe:

   - What is the dominant culture of the organisation, and how do people generally interact with each other?
   - What kind of behaviours are generally encouraged within the organisation?

3. ***How do you think the current leadership is responsible for the culture, how are they doing it?***

   Probe:

   - What type of leadership style does the organisation's leadership exemplify?
   - How would you describe the environment with the organisation that the leadership is creating?

4. ***How is the organisation sustaining that culture?***

   Probe:

   - What is the fundamental values and attributes that created a shared history for the organisation and serve as a unifying force for the organisation?

5. ***What is your organisation's stance on the issue of cybersecurity?***

   Probe:

   - Does the organisation have the right leader (cybersecurity leader)/champion?

- Is cybersecurity considered an IT-only problem or is it everyone's challenge?
- Do you know and understand the organisation's position/strategy on cybersecurity?
- Do you feel there are sufficient communication and emphasis around cybersecurity?
- Do you think there is a common understanding within the organisation on the risks associated with cybersecurity?

6. ***Do you think the organisation has a cybersecurity culture?***

   Probe:

   - Does the organisation exemplify a cybersecurity-focused mindset and culture?
   - How are these behaviours encouraged?

7. ***How is the organisation cultivating a culture of cybersecurity?***

   Probe:

   - Does the organisation provide annual or more frequent cybersecurity learning and training to your company senior executives, the board of directors, and employees?
   - Do you do simulation drills to ensure everyone knows how to react in the event of an attack? – phishing/smishing drills

8. ***In your role, to what extent do you help promote the desired behaviours of encouraging a cybersecurity culture?***

   Probe:

   - As a leader, how are you promoting the desired behaviours concerning cybersecurity to your subordinates?

9. ***If you could change anything about the current organisational culture, what would you like to see more of?***

APPENDIX (D) Qualitative Coding

Theme	Category	Codes	Quotes
Culture	Artefacts	Communication	**Participant 4:** "I think the game-changer has been the open and honest communication from leadership, that this is not just establishing a new culture is a nice thing to do, but it is a business priority. Moreover, should we not transform our culture and improve our bank will not be existing in five to ten years."
			Participant 1: "So we are constantly getting reminders about our team who has not done the training."
	Espoused Values	Culture Development	**Participant 2:** "So we have a culture team tasked with the promotion of the organisational culture. In a big organisation such as this, culture is almost passed over by osmosis. And maybe that's why I'm struggling to catch on. Because you kind of just start to understand the culture by seeing how other people operate. As part of this new rollout, we had serious rollout workshops and kick-off things that everybody or 42,000 people went to, irrespective whether it is in South Africa, or another country. From the workshops, one started to kind of get a sense of how the organisation operates. I think it is a culture that's trying to generate a kind of innovative thinking about stuff, we are on a digital journey, and we know that banking is changing. So, there is quite a lot of encouraging people to kind of behave differently."
		Organisational Learning	**Participant 8:** "One of the things that I probably left out there is that we have a massive budget – bigger than any other organisation right now in this country, I will tell you that for sure, in terms of learning and from a cyber point of view …"
			Participant 2: "We have a rigorous culture about the training in the sense that when people do not complete the training on time, we have a process of locking you out of your systems and not being able to access all systems until you do this. I guess that is how they are driving that culture of everybody having an understanding of those risks."
	Underlying Assumptions	Organisational Culture	**Participant 2:** "We are a bank that had an old entrenched culture where people did not trust each other, and people did not feel safe communicating. It is work in progress for the organisation, but it is improving, and we are not there yet."
			Participant 5: "The culture, the aspect of the culture is a very flexible culture where you have the leeway to work from wherever you wish because the business has given us the opportunity and the resources to be able to work in any office area, be it at the centre, actually even at home. It is very people-based."

Theme	Category	Codes	Quotes
			Participant 5: “It is a culture where teams are given opportunities, like employees going to study as well. From a training perspective, the bank is one of the best places to learn as there many opportunities to get significant exposure to new things. Moreover, where there is extensive help and support in terms of developing individuals.”
			Participant 8: “The culture of the bank is about people having the courage to speak out and speak up, appreciating people’s ideas, and it is about promoting transparency.”
Leadership	Leadership Process	Awareness Building	
		Cybersecurity Strategy	**Participant 4:** “So we have a cybersecurity strategy, part of the cybersecurity strategy involves awareness training. Awareness training ensures that all our stakeholders, that is, all our employees are aware of cybersecurity. We do focus on making it known that it is a joint responsibility for all staff members to be conscious of cybersecurity. Because we employ so many thousands of people, it increases our risk since one employee’s laptop could be the access point for a cybersecurity breach.”
			Participant 8: “So part of the cybersecurity strategy is a communication strategy to make sure that the importance of cybersecurity filters through the entire bank, from our, converge security office, to business to all the employees. There is upward and downward communication.”
		Change Management	
	The Leader	Cybersecurity Leadership	**Participant 1:** “At the core, there is the leader of the function, and you want to make sure that you have somebody that is not just a technical expert, but also a senior leader and executive. So that they can lead an organisation and understand what it means to be a level-five leader. In our context, we have been lucky to get somebody experienced, and that has global exposure. Furthermore, he is now bringing that to the South African context.”
			Participant 3: “We put security together such that there is no separate physical and cybersecurity; it now falls under one umbrella, one leader. It is an integrated approach to security.”
			Participant 4: “So for the cybersecurity or the converge security office is a relatively new function within Absa, it is approximately three years old. It has been made a business priority and is no longer just an ad hoc support function. Establishing an independent or separate role dedicated to converged security, the bank showed that it takes cybersecurity seriously. So our head of cybersecurity, which is our chief security officer with a budget and the mandate to protect the converged security. Since best practices consider cybersecurity integrated with physical security, and where cybersecurity and physical security converge, we are trying to reap the benefits of that as well.”

Theme	Category	Codes	Quotes
		Leadership Style	**Participant 1:** “Our leaders are very mature about being more pull and more carrot than stick so that they encourage you to volunteer to be more vigilant, rather than being told to be more attentive. Through role modelling events through rewarding and celebrating successes, that is through continuous support.”
			Participant 8: “You see that ability to work together and communicate messages is a leadership thing.”
			Participant 8: “Because it is leadership that gives direction from behaviour-wise staff members; if leadership is not able to work together, people will not be able to work together and even share information, they should completely change.”
			Participant 4: “I think that is what the job of the leadership of the security Exco to make sure other businesses are way interconnected with.”
	Technology	Active Monitoring	**Participant 3:** “You are democratizing cybersecurity by putting the power in the individual’s hands, even if it is just knowledge. In some cases, technology is placed in the hands of the colleagues, at least with email, they can secure emails themselves, and there is no need to go to the IT department.”
		Technology-enabled Security Support	**Participant 3:** “There is a whole bunch of sticks too, and those sticks range from automated sort of bots that catch instances of cybersecurity threats or breaches.”
			Participant 2: “We spend large amounts of money on the technology to prevent it even getting to us. The automatic screening of emails means a lot of suspicious emails blocked before they get through and that sort of stuff. That creates a security layer around users removing the need to rely on human beings not to click on a phishing email or that sort of stuff because generally those are blocked before they even get to them.”
		Cybersecurity Function	**Participant 4:** “In reorganizing the bank last year, we made sure that the two functional areas integrated, at least on that topic of cybersecurity management, and so we have got an end-to-end view now and once again, you know, driving this culture of cybersecurity across domains and functional areas.”
			Participant 3: “The converge security office is a relatively new function approximately three years old. It has a seat on the Exco. By having a seat in the Exco, it is no longer just an ad hoc function or ad hoc support source; it is a business priority.”

Theme	Category	Codes	Quotes
Organisational Design	Structure		**Participant 4:** “So people and our staff now see cybersecurity not as just like three years ago as a buzzword, you know, but they see it as a necessary function of the business. Like you need an accounting department to process your taxes and your financials. You need a cybersecurity department to make sure all your services are safe and protected.”
			Participant 4: “So we do extensive awareness training, we have got an awareness calendar as well. Each month we focus on different topics. So, we look at all the different factors. For example, look at all the different types of attacks.”
			Participant 4: “I was in charge of a project looking at our current awareness program, externally benchmarking it, comparing the topics and advising the head of training to say that we have this, but that it is viable for you and for us to hear a few more topics that will be more comprehensive because this is what the external market is doing.”
		Governance & Control Function	**Participant 6:** “These would have come up from the assessment that we would have done on cybersecurity to say, for us to remediate these are the things that we need to do. In some cases, there is an investment required.”
		Monitoring & tracking awareness training effectiveness	**Participant 4:** “So we have actual key performance indicators for our awareness training program? So, the awareness training tab has assessments to make sure that employees do have the basic understandings of the competence of cybersecurity. We also have targets, for example, that we need. We had 40,000 employees; we need to make sure we access at least 90%. And 100% of it always. However, we measure how much training we have implemented; how many people have passed.”
			Participant 4: “So, for example, we see that okay, since we have implemented training on phishing schemes, phishing schemes by the employees we send the training has decreased. Is there a measurable difference in our breaching incidents? It is not directly correlated because sometimes there are other factors involved, but we do try to see the return on investment. We measure the number of attacks, the impact of training and what we have invested, for example, that X amount of training X amount in a new technology X amount in new staff, how much is the reduction in attacks is due to technology, new staff or due to the training.”
			Participant 8: “We measure our people’s understanding of what these things are. We also identify those that have failed the testing and arrange that they are then sent for further education.”
			Participant 8: “If there is alignment between your awareness sessions in your culture, people responding to it.”
		Risk Management	**Participant 7:** “So you cannot just bring in a new vendor; obviously, there is a whole vendor process you have to go through to them. There are usually five committees because we are such a large organisation; there are rules and regulations in place for introducing anything into the organisation.”

Theme	Category	Codes	Quotes
			Participant 7: “Well, I think all the necessary controls are in place, concerning data privacy, and all of that sort of stuff ... we are under so much scrutiny and the SARBs who analyse what banks do with such detail.”
		Whistleblowing Hotline	**Participant 5**: “I think we have whistleblowing lines and all of that in place. The staff know about these things, and they are using it as well.”
	Human Resources Management	Cyber function Staffing & Retention	**Partner 3:** “And we make sure that the function is capacitated in terms of bums on seats and, competence level. We ensure there are no vacancies and with critical vacancies filled within a rapid timeframe, we are looking at 36 days or less a type of thing to fill critical vacancies.”
			Partner 3: “It took us 18 months to staff up our cybersecurity capability and going through the full battery of assessments and, and selection processes to make sure that we have the right profile of individuals on board.”
			Participant 4: “So we pay special attention to retaining our cyber skills, okay, and developing our cyber skills. So, we pay a large focus on making sure our cyber capabilities keep up to date with the latest training available. The latest developments in cyber technology and cybersecurity.”
			Participant 4: “So now we realize that the cost of hiring and the cost of replacing you might as well look after them now not only from a marketing point of view but from a development perspective from giving them a culture.”
			Participant 8: “In general, we are also quite very good at retaining our staff, you know, okay, we do not have a high turnover, we have an open budget for training.”
			Participant 8: “Again, every year we train about 20 students that are not even part of the bank, to bring them into the cyberspace and give them some skills and awareness, you know, I am saying. So that is leadership’s commitment of resources.”
			Participant 4: “We have also commenced many initiatives, we are actually in the fourth cohort of cybersecurity academy, where we take fresh, unemployed, unskilled school leavers. We train them on the scarce cybersecurity qualification.”
		Education and Awareness	**Participant 3:** “There has been an education and awareness campaign that kicked off last year. Furthermore, that education and awareness campaign touches all 40,000 employees.”

Theme	Category	Codes	Quotes
			Participant 4: “So we do extensive awareness training, we have got an awareness calendar as well. Each month we focus on different topics. So, we look at all the different types of attacks.”
			Participant 4: “There is a whole bouquet of topics to cover on cybersecurity, make sure that all employees have at
			least a basic knowledge of what cybersecurity awareness and threats are. For example, what we also do is that we do more detailed training for more high-risk employees.”
			Participant 2: “Banks are compliance heavy. Furthermore, we have a legal obligation to train up our people around all these risks. So we do have much training on topics that include cyber risks, fraud risks and money laundering.”
			Participant 5: “The compulsory training people would do just that there is more awareness around it, you know about phishing, and if you know, get these emails, and stuff do we have like security email addresses that you need to mail.”
			Participant 7: “So I would say the compliance training, including cyber risk training, is extensive. Moreover, every single colleague in Absa is almost sick to death of being trained on that.”
			Participant 8: “We also have like an educational portal, where people can go in and learn the mandatory courses. It is an online course, and if anyone does not complete it, their account gets disabled. So, it is a serious thing that it is measured. Everybody does it.”
		Incentives, Recognition & Rewards	**Participant 5:** “I will say that because of the initiatives that were introduced in the organisation, to make sure that we get involved and also the recognition that we get yearly from a performance rating point of view.”
			Participant 2: “So the primary measure has just been one about as I said, locking people out of the system has been the key. Previously, it was too easy to go, “I will do it next week and just get ramped up”. Okay, so until now there was no level of consequence management.”
			Participant 8: “If something is done well, you know, people are rewarded. We tell people about it, we communicate it, it becomes part of our DNA.”
		Skills Development	

APPENDIX (E) Ethics Approval

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG

SCHOOL OF GRADUATE SCHOOL OF BUSINESS ADMINISTRATION ETHICS COMMITTEE
CONSTITUTED UNDER THE UNIVERSITY HUMAN RESEARCH ETHICS COMMITTEE (NON-MEDICAL)

CLEARANCE CERTIFICATE **PROTOCOL NUMBER: WBS/BA1297842/959**

PROJECT TITLE The role of leadership in cybersecurity culture within the South African financial services sector

INVESTIGATOR	Mr Robert Mataruse
SCHOOL/DEPARTMENT OF INVESTIGATOR	MM (Digital Business)
DATE CONSIDERED	21 October 2019
DECISION OF THE COMMITTEE	Approved unconditionally
RISK LEVEL	MINIMAL RISK
EXPIRY DATE	28 FEBRUARY 2021

ISSUE DATE OF CERTIFICATE 17 February 2020 **CHAIRPERSON** __ _____
(Dr MDJ Matshabaphala)

cc: Supervisor: Dr Pillay

DECLARATION OF INVESTIGATOR

To be completed in duplicate and **ONE COPY** returned to the Chairperson of the School/Department ethics committee.

I fully understand the conditions under which I am are authorized to carry out the abovementioned research and I guarantee to ensure compliance with these conditions. Should any departure to be contemplated from the research procedure as approved I/we undertake to resubmit the protocol to the Committee.

_____ _____/_____/_____
Signature **Date**