

https://dspace.org/

Organisational culture and deterrence in a university information security environment

Sibande, Xolile

2021
https://hdl.handle.net/10539/33122

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

Organisational culture and deterrence in a university information security environment

A

Research Report

by

Xolile Sibande

(2057505)

In
Partial fulfilment of the requirements for the degree

Master of Commerce in Information Systems

At the

School of Business Sciences
Faculty of Commerce, Law and Management
University of the Witwatersrand

Supervisor:

Prof Ray M Kekwaletswe

ABSTRACT

Information security has become a growing concern for many organisations as well as for individuals and societies. Universities create, process, handle and store large quantities of confidential information daily which should always be secured. There are laws that govern how institutions should treat and protect confidential information from unauthorized access. Information security experts indicate that the highest percentage of information security incidents and breaches are due to human behaviour and internal attacks. This has caused a growing concern that calls for organisations to direct more focus on information security human behaviour within their environments. There is inadequate literature addressing how deterrence and organisational culture influence information security behaviour. To this point, this research report is about the influence and the role of organisational culture and deterrence in a university information security environment.

The study analysed the role that organisational culture and deterrence play in information security through the lenses of Deterrence theory and Organisational Culture theory. A case study research strategy following an interpretivism philosophy was used to gain knowledge and understanding on how aspects such as organisational norms and values as well as techniques used for consequence management affect the handling and securing of information in a university setting. Although the study context is a university environment, students were excluded from the study since the focus is on organisational culture and deterrence. A total of nine Information Technology (IT) personnel together with information security experts, functional managers and end-users who have a key role in information security in a university information security environment were interviewed using semi-structured interviews.

The study found that organisational culture and deterrence may play a huge role in influencing behaviour in an information security environment. The significance of this study is in showing the value and importance of organisational culture and deterrence in university information security.

KEYWORDS: Behaviour, Information Security, Deterrence, Organisational Culture, University.

Declaration

I, Xolile Sibande declare that this research report is my own, unaided work. It is being submitted for the Master of Commerce in Information Systems degree at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination at any other University.

_____ _____

Name of candidate Signature of candidate

_____ day of _____ 20_____ in_____

Dedication

This study is dedicated to me for all the hard work that went into making this journey a success. I would also like to dedicate this study to all my associates, friends and family who have supported me during this worthwhile journey and hope that you will do the same during my PhD journey. Lastly, I dedicate this study to everyone who has dreams that they are chasing, keep at it.

Acknowledgements

I would like to acknowledge myself for all the hard work that went into completing this milestone. To my family, friends, and colleagues, I would like to thank you for the ongoing support that you have shown me during this exciting and challenging journey. I would like to thank all the study participants who played a great role in this journey too, I appreciate your valuable contributions. A huge thank you to my financial sponsor the SITA Aero Foundation who have made this possible for me and a financial worry-free journey.

Lastly, I thank my research Supervisor Professor RM Kekwaletswe for the ongoing guidance during this journey.

Table of Contents

ABSTRACT 2

Dedication 4

Acknowledgements 4

List of Tables 9

List of Abbreviations and Acronyms 10

CHAPTER 1 11

1.1 Background to the field of study 11

1.2 Background to the research problem 14

1.2.1 The Location and Context of the Study 14

1.2.2 Information Security Challenges and Issues Observed 16

1.2.3 Identified Knowledge Gaps 16

1.2.4 Problem Statement 18

1.3 Study Purpose and Goal 19

1.4 Study Delineation 20

1.5 Study Contributions 20

1.6 Summary of the chapter 20

CHAPTER 2 22

SURVEY OF SCHOLARSHIP AND THEORETICAL FOUNDATIONS 22

2.1 Search Strategy 22

2.1.1 Information Security 22

2.1.2 Organisational Culture 24

2.1.2.1 Culture 26

2.1.3 Information Security Culture 28

2.1.4 Deterrence 30

2.1.5 Related Studies 33

2.1.6 Organisational Culture Theory 35

2.1.7 Deterrence Theory 37

2.2 Conceptual Research Framework 39

2.3 Summary of the Chapter 41

CHAPTER 3 42

RESEARCH METHODOLOGY 42

3.1 Research Paradigm 42

3.2 Research Approach 45

3.3 Research Strategy 47

3.4 Research Design 49
3.4.1 Unit of Analysis 49
3.4.2 Study Population 49
3.4.3 Sampling Technique 50
3.4.4 Sample Frame 50
3.4.5 Data Collection Method 51
3.4.6 Data Analysis Method 53
3.5 Validity and Reliability of Qualitative Research 53
3.5.1 Trustworthiness 54
3.5.2 Transferability 54
3.5.3 Credibility 54
3.5.4 Dependability 55
3.5.5 Conformability 55
3.6 Ethical Considerations 55
3.7 Summary of the Chapter 56
DATA ANALYSIS AND DISCUSSION OF FINDINGS 57
4.1 Analysis of Qualitative Data Collected 57
4.1.1 THEME A (study objective one): To analyse and describe how organisational culture influences information security behaviour in a university environment. 57
4.1.2 THEME B (study objective two): To analyse and describe how deterrence influences information security behaviour in a university environment 65
4.1.3 THEME C (study objective three): To analyse and describe how awareness influences information security behaviour in a university environment 71
4.2 Summary of the Chapter 79
4.2.1 Overview of Study Findings 79
CHAPTER 5 82
INTERPRETATION OF THE FINDINGS AND RECOMMENDATIONS 82
5.1.1 Interpretation of how organisational culture influences information security behaviour in a university environment 82
Recommendations from Theme A: 84
5.1.2 Interpretation of how deterrence influences information security behaviour in a university environment 84
Recommendations from Theme B: 86
5.1.3 Interpretation of how awareness influences information security behaviour in a university environment 86
Recommendations from Theme C: 88
CHAPTER 6 89

EVALUATION OF THE RESEARCH AND THE CONTRIBUTIONS 89
6.1 Overview of Chapters 89
6.1.1 Chapter 1 89
6.1.2 Chapter 2 89
6.1.3 Chapter 3 90
6.1.4 Chapter 4 90
6.1.5 Chapter 5 90
6.1.6 Chapter 6 90
6.2 Research Goal and Objectives 90
6.2.1 Primary Research Question 91
6.2.2 Secondary Research Questions 91
6.3 Summary of findings and how the study objectives were met 91
6.3.1 Research objective 1: To analyse and describe how organisational culture influences information security behaviour in a university environment. 91
6.3.2 Research objective 2: To analyse and describe how deterrence influences information security behaviour in a university environment. 92
6.3.3 Research objective 3: To analyse and describe how awareness influence information security behaviour in a university environment. 92
6.4 Evaluation of the Research Methodology 93
6.4.1 Appropriateness of the Data Collection Techniques 93
6.4.2 Why A Case Study Was Relevant for This Research 93
6.4.3 What Was the Research Theme? Is It Relevant to Information Security? 93
6.5 The Relevance of the Combination of Organisational Theory and Deterrence Theory 93
6.6 Contributions of the Study 94
6.6.1 Theoretical Contribution 94
6.6.2 Methodological Contribution 94
6.6.3 Practical Contribution 95
6.6.4 Contextual Contribution 95
6.7 The Study Limitations 95
6.8 Future Research 96
6.8.1 Conclusion 96
7 REFERENCES 98
8 APPENDIXES 104
Appendix A: Ethics Clearance 104
Appendix A: Ethics Clearance…continued 105
Appendix B: Participant Information Letter 106
Appendix C: Participation Consent Form 107

Appendix D: Interview Guide 108
Appendix D: Interview Guide…continued 109

List of Tables

Table 1: Differing Perspectives of Organisation Culture and Subculture Types (Kendra & Taplin, 2004:36) 26
Table 2: Highlights of Common Criminological Theories (Hu, et al., 2011) 32
Table 3: Related Studies 33
Table 4: A Summary of the Differences Among Research Paradigms (Guba & Lincoln, 1994) 44
Table 5: Quality of Positivist and Interpretive Research (Oates, 2006) 44
Table 6: A Summary of Ways to Collect Data for Each Research Paradigm (Guba & Lincoln, 1994) 45
Table 7: Difference between Quantitative and Qualitative Approach (Johnson & Christensen, 2008:34; Lichtman, 2006: 7-8) 46
Table 8: Participant Sample Frame 51

List of Figures

Figure 1: The CIA Triad (Qadir & Quadri, 2016) 23
Figure 2: The different levels of organisational culture (Waisfisz, 2015) 25
Figure 3: The visible and invisible attributes of culture (Richardson, 2014) 27
Figure 4: Levels of Culture (Van Niekerk & Von Solms, 2010) 30
Figure 5: Organisational Culture Model (Schein, 1986) 35
Figure 6: Deterrence theory (Ugrin & Pearson, 2013) 38
Figure 7: The Conceptual Research Framework 40

List of Abbreviations and Acronyms

Abbreviation	Definition
CIA	Confidentiality, Integrity, Availability
HR	Human Resources
IT	Information Technology
IS	Information Systems
VPN	Virtual Private Network

CHAPTER 1

INTRODUCTION AND BACKGROUND

This research report is about information security, organisational culture, and deterrence in a university information security environment. The security of information is a growing concern for many organisations as well as for individuals and societies (D'Arcy & Herath, 2011). Over 95% of information security incidents and breaches are due to human behaviour, insider attacks or as a cause of disgruntled employee attacks (The Committee on National Security Systems, 2001; D'Arcy, et al., 2009; Carroll, 2006; IT Security Team, 2015). The research report argues that this growing concern calls for organisations to direct more focus on organisational culture and deterrence as well as their roles in information security environments.

The first chapter of this report provides a background to the field being studied and the background to the research problem. The study location and study context are discussed. This is followed by the problem statement, study goal, study objectives, and the research questions (both primary and secondary). This chapter ends with the study contributions and delimitations.

1.1 Background to the field of study

This section gives the background to the field studied by reviewing and discussing the keywords making up the research topic. This is done to give the reader a common understanding of the context and area studied.

Information security is a top management concern and a critical issue for all organisations (van de Haar & von Solms, 1993). For an organisation such as a university, information is regarded as a critical asset and thus issues of information security and safeguarding thereof are of utmost importance (Amini, et al., 2020). A university requires information for research, teaching, and learning, gain a competitive advantage, make critical decisions, sustain operations and many other reasons. According to Katz (2005: 44), Universities in nature deal with substantial confidential information relating to clients as well as the business itself which places

them at the crux of information security threats. Katz (2005: 44) further states that the common threats often faced by such institutions include factors such as “compromises to intellectual property; deliberate acts of theft; deliberate acts of information extortion; deliberate acts of sabotage and vandalism; and deliberate acts of espionage and trespass’’.

There has been an increase in cyber-attacks which may mislead the information systems users to reveal information such as academic records, login credentials, confidential identification data, and personal information that they would not reveal under normal circumstances (Amini, et al., 2020). Therefore, the study was undertaken to observe whether organisational culture and deterrence influence behaviour in a university information security environment.

1.1.1 Information Security

Information security is defined as the protection of information in any format (physical or electronic) and information systems from any unauthorised access, modification, use, manipulation, destruction, and storage, to ensure that confidentiality, integrity, and availability of information are maintained (Da Veiga & Martins, 2015). In this study, information security is the protection of information assets, confidentiality, integrity, and availability either in processing, storage, or transmission (Whitman & Mattord, 2012).

1.1.2 Information Security Awareness

In the study, information security awareness entails ensuring that employees understand information security policies, guidelines and rules, the importance thereof and their requirements to behave in line with the policies, guidelines, and rules (McCormac, et al., 2017). Information security is achievable through technology, education of people, raising awareness on the subject, training, or enforcement of policies (D’Arcy, et al., 2009).

Information security awareness is important for everyone in organisations. This is because human behaviour contributes to over 90% of information security incidents

and breaches (Mimecast, 2020). Information security awareness can improve employee attitudes and behaviour, which can result in improved information security behaviour and management (Wiley, et al., 2020). While the expectation is for employees to display behaviour of informedness with regards to security in handling information, employers need to recognise the need to train staff on acceptable information handling and security procedures (Katz, 2005).

Education is said to be a tool that can enable the employees to understand the risk associated with the handling of information, implement adequate controls to protect the information as well as being accountable for their actions (Da Veiga & Martins, 2015). A well-implemented information security awareness program promotes organisational culture and how things are done in an organisation (Wiley, et al., 2020).

1.1.3 Organisational Culture

Organisational culture is defined as the behaviour, norms, and values within an organisation that direct how an individual or a group within an organisation conduct themselves (Knein, et al., 2019). Organisational culture gives rise to an organisation's general norms and behaviour that employees will adopt for example how they talk, dress, and behave (Du Plessis & Hoole, 2006). It is believed that organisational culture has an extent of influence on how individuals behave in an organisation (Cheung, et al., 2011).

While organisational culture can be defined collectively, the concept can also be used to refer to individual characteristics such as the individuals' attitudes, behaviour, expectations, and assumptions within an organisation (Ahmady, et al., 2016). Organisational culture is a powerful resource that provides common identity, feelings, and guidelines (Ahmady, et al., 2016). Where there are no written policies or laws, individuals in an organisation are guided by the organisational culture (Ahmady, et al., 2016). Organisational culture can potentially assist in facilitating change and stabilizing the newly implemented changes in an organisation (Kendra & Taplin, 2004).

1.1.4 Information Security Culture

An information security culture is defined as an employee's behaviour, attitudes, beliefs and knowledge towards the organisation's information assets and property at any given time (Da Veiga & Eloff, 2010). An information security culture in an organisation sets direction on how things are done concerning information security and it influences the behaviour of employees when handling an organisation's information assets that are on information systems (AlHogail & Mirza, 2014).

1.1.5 Deterrence

In this study, deterrence is defined as a psychological process that involves deterring individuals from committing any criminal activity by showing them the dire consequences of their actions (Williams & Hawkins, 1986).

It is believed that if people are told what to do, they are more likely to do exactly what they are told and if they are told not to do something, they are more likely not to do it. That is, people need deterrence to refrain from doing what is not right (Ugrin & Pearson, 2010). For example, if employees are told that they will be fired and reported to law enforcement if they are found to be performing illegal activities, there is a high probability that employees will not engage in any illegal activity.

1.2 Background to the research problem

This section provides the background to the research problem. The section discusses the study location and context, the challenges and issues observed in a university information security environment, and the knowledge gaps.

1.2.1 The Location and Context of the Study

The context for and location of the study is a South African university's information security environment; that is, how organisational culture and deterrence manifest relative to information security in a university setting. In South Africa, there are 26 universities, these universities are classified into three categories namely traditional universities, comprehensive universities, and universities of technology. A university

is an institution that offers undergraduate and postgraduate academic qualifications in various fields.

Universities create, process, handle and store large quantities of confidential information daily, which should always be secured as there are laws that govern how institutions should treat and protect confidential information from unauthorized access. Examples of laws that govern how information should be treated include the (Protection of Personal Information Act, 2013). In a university environment, there are students, academic and non-academic employees, third party stakeholders and all these people either create process, handle, or store information for different reasons.

Users, such as those stated above, use the information for making informed decisions, performing their daily tasks, staying informed on what is required to optimally support the organisation, conducting research, and sharing knowledge.

The Covid-19 pandemic has limited the face-to-face administration and support of university activities, meaning that most employees resort to virtual communication and working remotely, which often results, among other things, in people having access to otherwise confidential information. The anxiety of the new and changing ways of working, administration, and support may lead to information security breaches and information misbehaving. This could also lead to the University's confidential information ending up in the hands of unauthorized persons who could use it maliciously.

Continuous changes in the information security sphere and in the traditional way of how universities function call for a change in the information security approach. Studies have shown that 8 out of 10 information security breaches are due to human behaviour, meaning that more efforts must be directed to addressing these issues which involve individuals (Safa, et al., 2019). For example, downloading malicious software that was embedded in an email that seemed legitimate, whereas it was from a cybercriminal tricking an individual into downloading the software to enable them to gain unauthorised access to the university's information security environment. Information is very critical for universities and therefore, adequate control needs to be applied to ensure that integrity and confidentiality are maintained.

1.2.2 Information Security Challenges and Issues Observed

Academic records, operational records and any other records in a university's information system must have adequate information security controls. A few examples of security concerns in a typical university include but not limited to, (1) Illegal manipulation of marks by academic or support staff or third parties, (2) Students cheating while taking examinations remotely using online learning management systems (3) Employees disclosing and sharing confidential information such as financial and medical details kept and sourced from various university systems, and (4) theft of university secrets such as cutting-edge research data.

A university information security environment is a complex phenomenon. This is because there are different processes which include creation, use, update, retention, and storage of information. The access and authentication of those who require and use the information are critical in preserving information security.

Individuals in a university environment tend to create, process, store and handle a lot of confidential information without being fully aware of the implications of not maintaining information security best practice. Furthermore, individuals may not be aware of the consequences of information leakages and breaches, and the impact that it may have on the university. This study argues that information security should be part of the organisational culture and employees should be treating information at their disposal with utmost care.

Information security should form part of the employees' daily activities and become second nature in their behaviour which will make it easier for the integration of information security and organisational culture (Thomson, et al., 2006). There is a possibility that the employees are not fully aware of issues of information privacy and security and what impact it has on them and the university at large.

1.2.3 Identified Knowledge Gaps

Additional to the above challenges, this section discusses the knowledge gaps which were identified in motivation for the study. The knowledge gaps are discussed in four folds namely theoretical, methodological, practical, and contextual.

1.2.3.1 Theoretical Gap

The goal of the study was to determine the role of organisational culture and deterrence in a university information security environment. The review of the literature shows that many studies about culture in organisations are using the organisational culture theory as a lens. The organisational culture theory is used to assess the behaviour, norms, and values of an organisation.

From the review of literature, no known information security related study has used a combination of the organisational culture and the deterrence theories as lenses, notably in the context of a university information security environment. The outcome of the study may assist in gaining and extended knowledge and understanding of how organisational culture and deterrence influence information security behaviour in the context of a university.

1.2.3.2 Methodological Gap

The review of the literature has highlighted some knowledge gap concerning research methodology. Most studies on organisational culture used a survey method as their research strategy, and often following a positivism philosophy stance. The same can be said about the deterrence theory where most studies have been conducted using a survey method and a positivism philosophy.

The disadvantage of a survey research strategy is that it does not give the real depth of the problem being studied. In a survey strategy, questions are too closed-ended, and often fail to capture respondents' feelings or emotions. There is a need, therefore, to use a case study research strategy to analyse the role of organisational culture and deterrence in a university information security environment. A case study allowed more flexibility while gathering empirical data through observation, individual participant's views, opinions, and experiences about a university information security environment.

1.2.3.3 Practical Gap

The practical knowledge gap is in how human interaction and behaviour influence information security, notably in a university. This study was envisaged to bridge that practical gap by analysing the role of organisational culture and deterrence. That is, the analysis is envisaged to practically help in addressing the information security issues and challenges, in a university information security environment. The research argument is that information security is a social phenomenon that is largely dependent on human interaction and behaviour.

1.2.3.4 Contextual Gap

Universities offer a unique and different context to that of corporate organisations. Many studies have been conducted with the aim to analyse the influence of either organisational culture or deterrence in a particular environment, mostly financial institutions but a study of this nature has not been conducted in a South African university environment context. The observation, from the review of related studies on information security, has been conducted mostly within financial institutions particularly the banking sector, over the past few years. To this point, the contextual knowledge gap lies in the lack of studies done within a university context.

1.2.4 Problem Statement

Although information security is a well-researched area, the problem is that literature inadequately addresses how organisational culture and deterrence influence information security behaviour. That is, there is a lack of studies that unravel how deterrence and culture manifest and how the two together play a role in information security behaviour. This has left the preceding theoretical, contextual, methodological, and practical knowledge gaps concerning the know-how and know-what of the role that organisational culture and deterrence play in information security, notably in a university environment. This research report sought to bridge that knowledge gap.

Studies have shown that 8 out of 10 information security breaches are due to human behaviour, meaning that more efforts must be directed to addressing these issues which involve individuals (Safa, et al., 2019). According to Katz (2005: 44), Universities in nature deal with substantial confidential information relating to clients as well as the business itself which places them at the crux of information security threats. Katz (2005: 44) further states that the common threats often faced by such institutions include factors such as “compromises to intellectual property; deliberate acts of theft; deliberate acts of information extortion; deliberate acts of sabotage and vandalism; and deliberate acts of espionage and trespass’’.

1.3 Study Purpose and Goal

1.3.1 Study Purpose

The purpose of the study was to describe how organisational culture and deterrence influence behaviour in a university information security environment.

1.3.2 Study Goal

The goal of the study was to determine the role of organisational culture and deterrence in a university information security environment.

1.3.3 Study Objectives

The objectives were as follows:

- To analyse and describe how organisational culture influence information security behaviour in a university environment.
- To analyse and describe how deterrence influence information security behaviour in a university environment.
- To analyse and describe how awareness influence information security behaviour in a university environment.

1.3.4 Research Questions

1.3.4.1 Primary Research Question

How do organisational culture and deterrence play a role in a university information security environment?

1.3.4.2 Secondary Research Questions

The following were the secondary research questions:

1. How does organisational culture influence information security behaviour in a university environment?
2. How does deterrence influence information security behaviour in a university environment?
3. How does awareness influence information security behaviour in a university environment?

1.4 Study Delineation

The goal of the study was to determine the role of organisational culture and deterrence through the individuals' views, opinions, and experiences in a university information security environment. The study was not about analysing information security technologies, tools, and processes. Additionally, the study focused on individuals who have experience and/or are familiar with information security in the context of a university; that is, the study was not about learners but professionals familiar with the phenomenon.

1.5 Study Contributions

The study makes theoretical, methodological, practical, and contextual contributions, which are discussed in chapter 6 of this research report.

1.6 Summary of the chapter

This chapter provided a background to the field being studied and the background to the research problem. The study location and study context were discussed. This was

followed by the problem statement, study goal, study objectives, and the research questions. The chapter ended with the study delimitations and the layout of the research report.

The layout of the research report

The rest of the report is structured as follows:

Chapter 2: This chapter surveys the scholarship and theoretical foundations of the study. The chapter also discusses the theories underpinning the study and then provides the conceptual research framework which guided the study.

Chapter 3: Research Methodology. This chapter describes the research methodology that was followed in the study.

Chapter 4: Data Analysis and Results. In this chapter, data is analysed, and the findings are discussed.

Chapter 5: Interpretation of the Findings. This chapter interprets the study findings.

Chapter 6: Evaluation of the research and Recommendations. This chapter evaluates the research and ascertains whether the research objectives were met and whether the primary and secondary research questions were answered. The chapter also discusses the limitations of the study and makes recommendations for further research.

CHAPTER 2

SURVEY OF SCHOLARSHIP AND THEORETICAL FOUNDATIONS

The previous chapter introduced the research report by giving the background to the field studied, research problem, study goal, objective, and the research questions. This chapter surveys the existing scholarship by reviewing literature that gives the theoretical foundations of the study. The chapter discusses the two theories underpinning the study, and then it provides the conceptual research framework which guided the study.

2.1 Search Strategy

This section surveys scholarship by reviewing literature and concepts which informed the study.

2.1.1 Information Security

The primary objective of information security is to maintain information confidentiality, integrity, availability, authenticity, and accountability (Zhang, et al., 2017). Information integrity is about “safeguarding the accuracy and completeness of the information. Information availability ensures that information and vital services are available when required. Information authenticity refers to the legitimacy of data involved in transactions, communications, and documentation. Information accountability suggests that all actions compromising information security can be traced back to the responsible party” (Zhang, et al., 2017: 1179).



Figure 1: The CIA Triad (Qadir & Quadri, 2016)

Figure 1, above, presents the Confidentiality, Integrity, Availability (CIA) model of information security which illustrates the dependence of information security on confidentiality, integrity, and availability.

Information security is the preservation of information confidentiality, integrity, and availability to ensure that incidents and their impacts are minimised, and that information is always available for business needs (Von Solms & Van Niekerk, 2013). Scholars and researchers state that information security is about making sure that information and information systems are safeguarded to preserve their authenticity and ensuring that only authorized people have access to them (AlHogail & Mirza, 2014; Da Veiga & Martins, 2015; Van Niekerk & Von Solms, 2010).

Information security is a very complex phenomenon and one of the most important tools in protecting an organisations information system from any threats, whether internal or external (Amini, et al., 2020). Information security must be regarded as an enabler that affords an institution the ability to provide services while achieving confidentiality, integrity, and accessibility of information (Szczepaniuk, et al., 2020).

2.1.2 Organisational Culture

Organisational culture is defined as the principles that direct behaviour and activities such as beliefs, values or norms which are shared by individuals within an organisation (Van Niekerk & Von Solms, 2010). Organisational culture assists individuals in an organisation to distinguish between what is important as well as what is not, and this is achieved through ongoing communication (Ahmady, et al., 2016). Organisational culture influences how individuals in an organisation behave as it guides how things are done in an organisation makes clear what is acceptable and not acceptable (Agnantounkpatin & Zhang, 2011). Organisational culture also has a strong influence on the organisation's security environment, policies, and procedures (Ruighaver, et al., 2007).

Organisational culture is comprised of multiple subcultures of the different individuals in an organisation (Kendra & Taplin, 2004). Organisational culture is “a pattern of shared basic assumptions learned by a group as it solved its problems through external adaption and internal integration, which has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems” (Önday, 2016: 39005). Organisational culture “influences what employees can do and how they view, define, analyse and resolve problems” (Agnantounkpatin & Zhang, 2011: 52). Organisational culture values influence how individuals within an organisation behave themselves (Knein, et al., 2019).

The following are the characteristics of organisational culture:

- Learning.
- Control/Discipline.
- Conflict tolerance.
- Interpersonal Relationships.
- Open communication.
- Interdependence (Du Plessis & Hoole, 2006).

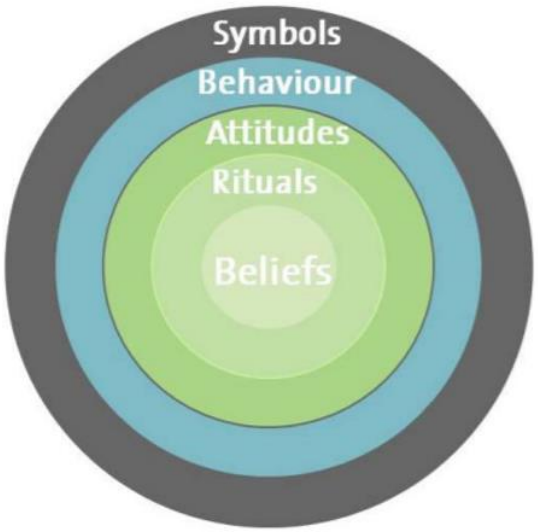

Figure 2: The different levels of organisational culture (Waisfisz, 2015)

Figure 2, above, is an onion visualising the different levels of organisational culture. The outer ring represents symbols that can be changed the easiest where else the inner rings (behaviour, attitudes, rituals, and beliefs) require much more efforts to change (Waisfisz, 2015).

Table 1: Differing Perspectives of Organisation Culture and Subculture Types (Kendra & Taplin, 2004:36)

PERSPECTIVES	TYPE(S)	AUTHORS
Corporate culture is defined by the values, heroes, rites and rituals, and the communication networks.	Tough-guy, macho culture, work hard/play hard culture, bet-your-company, and process culture	Deal and Kennedy (1982)
The framework is based on 39 indicators of organizational effectiveness. The vertical dimensions differentiate organizational flexibility and discretion from stability and control. The horizontal dimension differentiates based on an organization orientation of internal harmony from external rivalry.	Clan, adhocracy, hierarchy, market	Quinn and Cameron (1983)
Culture resides in one's subconscious and is formed from past experiences from one's upbringing, education system, language, environment, previous actions, and personal memories.	Organization	Hall (1989)
Individuals' interpretations of manifestations. The patterns or configurations of these interpretations, and the ways they are enacted, constitute culture.	Organization	Martin (1992)
Comprised of multiple subcultures that are derived from individual experiences and educational backgrounds, and are developed by an individual's occupational community (professions).	Operator, engineering, executive	Schein (1996)
A system of shared assumptions, ideas, beliefs, and related patterns of behavior learned by people over time.	National, corporate, and work culture	Baba, Falkenburg, and Hill (1996)
Holistic based on history, rituals and symbols, socially constructed and preserved by the group.	Organization and national cultures	Hofstede (1997)
Part of the overall organization design that is comprised of four design factors: core activity system, structural system, measurement system, and human resource system to enable information flow throughout the organization.	Organization	Cummings and Worley (1997)
Organization cultures that exist in technology companies based on the relationships that exist between management and employees.	Paternalistic, highly individualized, teams	Frohman (1998)
Four types of culture derived from management ideologies that form an organization culture profile	Power-oriented, role-oriented, achievement-oriented, and support-oriented	Harrison and Stokes (1997)

Table 1, above, is a summary of the differing perspectives of organisational culture and subculture types. The table shows that indeed, culture is seen from varied perspectives and levels.

2.1.2.1 Culture

According to Hofstede (1980), culture is the embedded belief system in humans - which differs from one group to another - and it influences human feelings, way of thinking and how they react to certain situations. Culture can also be defined as the shared mental programming of individuals which influences how they respond to

certain situations and environment (Richardson, 2014). “Human behaviour is largely determined by culture, which affects interactions in everyday social and work environments” (Wiley, et al., 2020: 101640).

Culture can be the result of constant patterns and behaviour in a certain setting (Winkler & Gomes, 2017). Culture reforms as people interact with each other; however, it is shaped by their behaviour (Schein, 2016). Culture is what gives individuals and groups their identity and is formed by their communication framework such as actions, gestures, the way they handle situations and defend themselves (Kendra & Taplin, 2004). Studies on organisational culture (for example, Warrick, 2017) provide evidence that culture can have a significant influence on employee attitudes, behaviour, performance, and work environment.

The following are the characteristics of culture:

- It is shared.
- It is largely invisible.
- Has a powerful influence on behaviour.
- It is learned and enduring.
- It is systematic and organized.
- It can be tight or loose (Richardson, 2014).

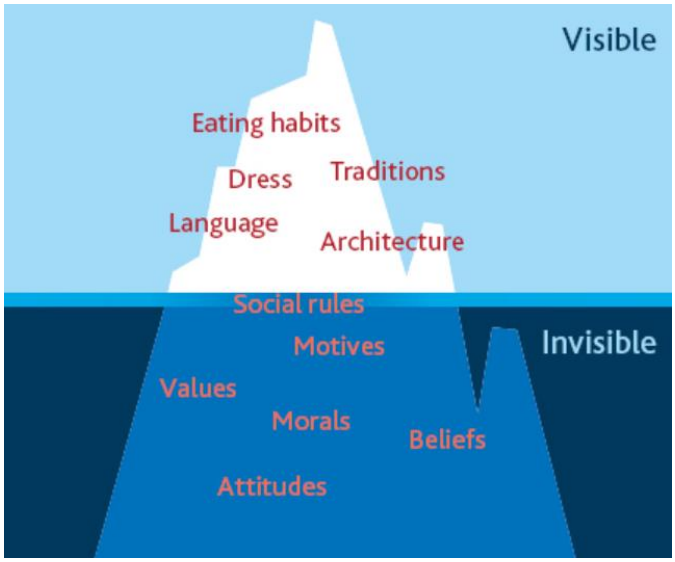

Figure 3: The visible and invisible attributes of culture (Richardson, 2014)

Figure 3, above, shows the attributes of culture. Above the waterline are the visible attributes such as traditions, dress code, eating habits and so forth. However, the attributes that cannot be easily visible such as beliefs, morals, values, and social rules are below the waterline. The invisible attributes of culture are what drives the increased complexity factors for behaviour.

2.1.3 Information Security Culture

In the context of information security, culture is the shared behaviour of individuals when they engage with sensitive activities; that is, it guides how an individual will treat sensitive information at their disposal (Winkler & Gomes, 2017). Culture is the greatest assets that an organisation possesses and should be treated as such (Warrick, 2017). Information security culture is also defined as the group's behaviour in an organisation towards information security (Winkler & Gomes, 2017). Culture is the assumptions that employees share within an organisation about information security (Solomon & Brown, 2020).

Employees may often be the weakest link in information security as they may unknowingly disclose sensitive information that they should not; therefore, information security culture is needed to assist with mitigating the risks associated with human behaviour in protecting information assets and maintain the privacy thereof (Thomson & van Niekerk, 2012). An information security culture is vital in improving behaviour towards compliance and protecting an organisation information asset (Solomon & Brown, 2020). An organisation must play its part in ensuring that employees are trained, guided, and informed of information security requirements (Katz, 2005).

It is believed that employees are the greatest threat to information security, whether intentionally or erroneously, and in most cases, it is due to lack of knowledge (Committee on National Security Systems, 2001). This cause for concern calls for the establishment or improvement of an information security culture in organisations to manage the human factor element in information security (Van Niekerk & Von Solms, 2010). “Employees are more likely to adhere to information security policies within organisations where the dominant culture has a strong focus on adherence to policies and procedures; thus, facilitating the formation of an information security subculture.” (Solomon & Brown, 2020: 2).

Individual's behaviour has a great contribution to the incidents that take place in an information security environment (AlHogail & Mirza, 2014). Information security culture changes over time as trends, behaviour, and beliefs change (IT Security Team, 2015). According to the IT Security Team (2015), organisational culture influences the information security culture of an organisation as it is part of how things are done in an organisation. People are an integral part of information security culture and their roles and responsibilities must be clearly defined to improve information security behaviour in any given context (Futcher, et al., 2010).

A strong information security culture can assist organisations in curbing human threats to information security and ultimately assist in the reduction of information leakages, incidents, and data breaches (Da Veiga, et al., 2020). Information security culture is effective in promoting ethical and secure behaviour in any environment, and to manage information security risks (Nasir, et al., 2019).

Figure 4, below, is an illustration of the different levels of a culture where corporate culture consists of artifacts, espoused values, and shared tacit assumptions. The same levels can be seen in information security culture with the addition of knowledge.

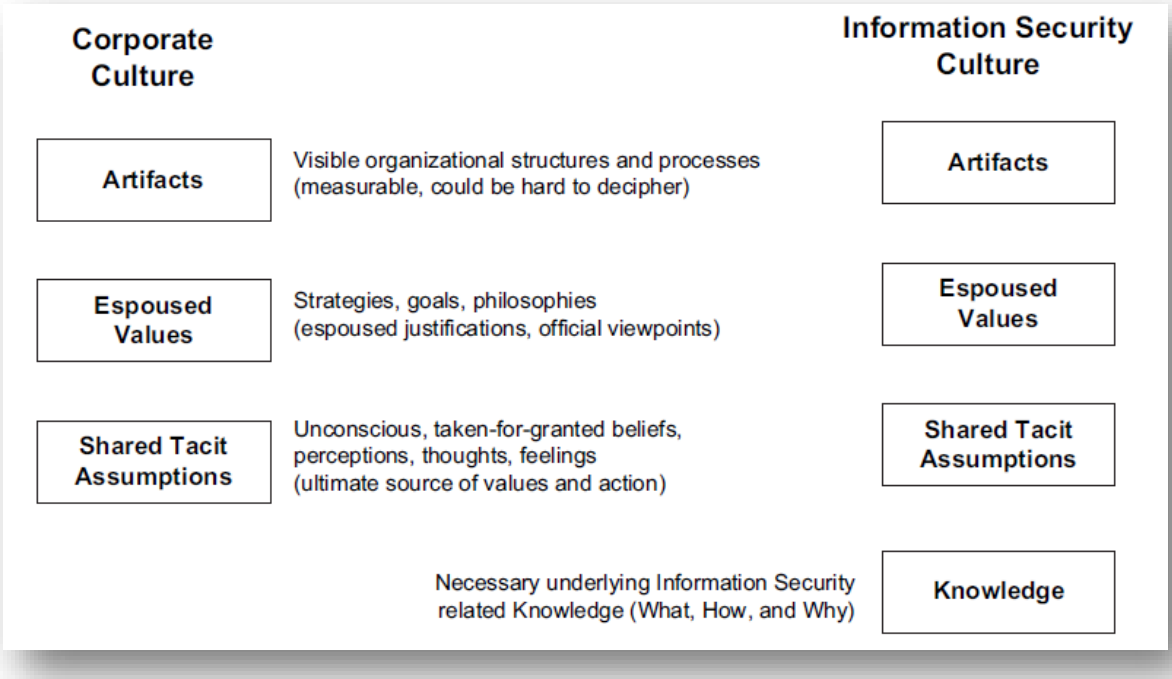

Figure 4: Levels of Culture (Van Niekerk & Von Solms, 2010)

A well-established information security culture is necessary in an organisation where the protection of information, maintaining confidentiality, privacy and integrity is mandatory (Da Veiga & Martins, 2015). In an organisation where there is an information security aware culture, there is more likely reduced risks that are associated with employee's misconduct when interacting with information assets and sensitive information (Da Veiga & Eloff, 2010). Information security culture is considered to be very key in protecting an organisation's information and security environment (Dhillon, et al., 2016).

2.1.4 Deterrence

Deterrence is distinguished between general deterrence and specific deterrence (Bhattacherjee & Shrivastava, 2018). General deterrence refers to the threat of legal action or punishment for the greater public while specific deterrence refers to an individual's exposure to detection, punishment, loss, prosecution, and the effects that it has on future crimes (Bhattacherjee & Shrivastava, 2018). "Individuals are less likely to commit criminal acts if the perceived certainty, severity, and celerity of sanction against the acts are greater" (Hu, et al. 2011: 56).

Deterrence is useful in situations where the aim is to curb any illegal activities from taking place rather than in instances where the illegal activities have already taken place and you are now seeking to punish the act (Bhattacherjee & Shrivastava, 2018). Deterrence mechanisms can involve the threat of dismissal, jail time, fines and naming and shaming of perpetrators (Safa, et al., 2019). For example, "specific deterrence dictates that, if an armed robber receives a harsh sentence of eight years in prison, he will be less likely to commit armed robbery again when he eventually gets out" (Champlin & Oldham, 2017).

For this study, "specific deterrence" was the scope as the study focused on an individual's behaviour and not the public.

2.1.4.1 Deterrence in Information Security

Deterrence can reduce risks associated with insider threats in an organisation's information security environment (Safa, et al., 2019). If people are aware of the consequences of their unethical actions and behaviour, they are more likely to refrain from instituting those actions (Hu, et al., 2011). Deterrence emphasizes three factors; firstly, deterrence implies the legal theory of behaviour control which is about the legal implications and sanctions on criminal activities (Williams & Hawkins, 1986).

Secondly, deterrence stems from the fear of the punishment rather than the actual punishment; for example, an employee refrains from disclosing confidential information for fear of losing their jobs. Thirdly, deterrence implies the illegal activities as an outcome of the cost versus reward analysis whereby the employee will first weigh what the reward is for maintaining information security as opposed to the cost of not doing so. Examples of deterrence factors include arrest, disciplinary action, sentencing, and hefty penalties. Organisations introduce information security awareness to make their policies clear to all their stakeholders and to ensure that deterrence is in place (Rezgui & Marks, 2008).

Policies define and govern the actions and behaviours of people within an organisation and the consequences thereof are a deterrent to information security breaches and leakages (Carroll, 2006). For example, "if personnel believe that he or she will be prosecuted if the information is compromised due to actions performed, intentionally or unintentionally by them then they are less likely to break the policy and breach security" (Carroll, 2006: 157).

If employees are aware that their actions are visible to others, the likelihood of them following the rules tend to increase (Shrivastava & Bhattacherjee, 2015). Individuals are more likely to maintain information security and respect the information that they have access to if they are deterred (DiIulio, 1959). Table 2 below highlights some of the criminology theories and their descriptions in relation to behaviour.

Table 2: Highlights of Common Criminological Theories (Hu, et al., 2011)

Theory	Type(s)	Description	Author(s)
Deterrence	Behavioural Theory	• Human beings are fundamentally rational in their behaviour and choose crime only when it pays. • Individuals are less likely to commit criminal acts if the perceived certainty, severity, and celerity of sanction against the acts are greater.	(Gibbs, 1975) (Tittle, 1980)
Rational Choice	Behavioural Theory	• Individuals are sensitive to the consequences of their actions and make reasoned judgments based on the cost-benefit analysis of the intended acts. • The decision to engage in criminal behaviour is a function of the perceived costs and benefits of the criminal act.	(Bekker, 1968) (Cornish & Clarke, 1986) (Paternoster & Simpson, 1996)
Self-Control	Behavioural Theory	• All human beings have the potential of committing crimes, but not everyone does because of differences in the ability of self-control. • Self-control is established early and remains relatively stable throughout an individual's lifetime. • Individuals with low self-control have a tendency to respond to tangible stimuli in the immediate environment and are more likely to be seduced by the thrill and excitement of criminal acts.	(Gettfredson & Hirschi, 1990)
Shame	Behavioural Modifier	• Shame is the experience of temporary loss of self-esteem in an internal evaluation of the self by an individual. • Shame has a deterrence effect on various criminal acts through three mechanisms: self-imposed shame (or shame), socially imposed embarrassment, and state-imposed legal sanctions.	(Lewis, 1992) (Piquero & Tibbetts, 1996)
Moral Beliefs	Behavioural Modifier	• Moral beliefs are individual judgment of right and wrong about a specific behaviour. • Moral beliefs against committing criminal acts increase the degree of perceived sanctions and the shame associated with the acts. • Moral beliefs also have a negative effect on the perceived pleasure from deviant behaviour.	(Bachman, et al., 1992) (Piquero & Tibbetts, 1996)

The theories described in the table above have been used to analyse and study criminal activities and deterrence. The next section discusses studies which are related to the present study.

2.1.5 Related Studies

This next section discusses studies which are related to the present study. The table below shows studies previously undertaken and are related to this present study. The studies brought out during the systematic literature review also assisted in identifying the existing knowledge gaps that motivated the present study. The studies below mostly focused on human behaviour in information security.

Table 3: Related Studies

Study Title	Author(s)	Study Aim/Purpose	Findings
Information security education in South Africa	Futcher, et al. (2010)	The purpose of this paper was to argue that information security should be regarded as a critical cross-field outcome (CCFO). This could assist in narrowing the evident "information security gap" that currently exists in undergraduate information technology/information systems/computer science (IT/IS/CS) curricula at South African universities.	Education in information security has matured much more rapidly in postgraduate than in undergraduate programmes at South African universities.
Combating information security apathy by encouraging pro-social organisational behaviour	Thomson & van Niekerk, (2012)	The purpose of this paper was to show how employee apathy towards information security can be addressed through the use of existing theory from the social sciences.	The work in the paper is primarily conceptual. However, the authors believe that encouraging such pro-social behaviour could contribute towards an organizational culture of information security.

The influence of organisational culture and information security culture on employee compliance behaviour	Solomon & Brown, (2020)	The purpose of this paper was to explain the nature of the combined influence of organisational culture and information security culture on employee information security compliance. This study also aims to explain the influence of organisational culture on information security culture.	Organisational culture and information security culture have significant, yet similar influences on employee compliance. In addition, organisational culture has a strong causal influence on information security culture.
Deterrence and Prevention-based Model to Mitigate Information Security Insider Threats in Organisations	Safa, et al., (2019)		The output of the data analysis also showed that subjective norms, perceived behavioural control and attitude influence individuals' intentions, and, ultimately, their behaviour towards avoiding information security misbehaviour.

The above table is a summary of related studies conducted relative to information security, either using deterrence theory or organisational culture theory. The fact that none of the studies are underpinned by the two theories together shows the relevance of the present study, which triangulates both.

Theoretical Frameworks (Underpinning theories)

The goal of the study was to determine the role of organisational culture and deterrence in a university information security environment. The theoretical frameworks underpinning a study assist in improving the ability to make better analysis and achieve an understanding of what is being studied (Hambrick, 2007). This study was underpinned by two theories namely Organisational culture and Deterrence theories. The two are discussed in this section.

2.1.6 Organisational Culture Theory

Organisational culture theory was introduced to make known the definitions and implications of organisational culture to managers and why people in an organisation behave the way they do (Schein, 1986).

Figure 5 below is an illustration of the Organisational culture model. The model suggests that organisational culture can be divided into three levels, which are behaviour and artefacts, espoused beliefs and values, and basic assumptions.

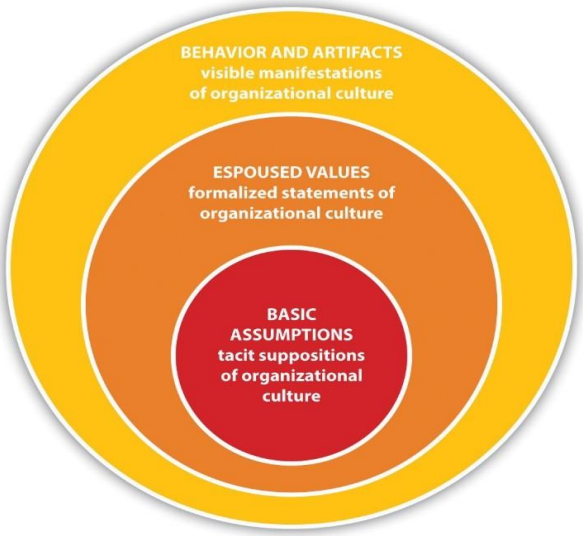

Figure 5: Organisational Culture Model (Schein, 1986)

Organisational culture exists on three levels: first are artefacts, then beneath them lies espoused values, and lastly underlying assumptions (Schein, 1986). “Assumptions represent beliefs about reality and human nature that are often taken for granted. Values are social principles, philosophies, goals, and standards considered to have intrinsic worth. Artefacts are the physical, intangible, audible results of activity grounded in values and assumptions” (Hatch, 1993: 659).

The three levels of Organisational Culture are discussed as follows:

2.1.6.1 Behaviour and Artefacts

The first level of the organisational culture theory is represented by behaviour and artefacts, these are the surface of the culture in an organisation and analysing them is easy for an outsider (Dimitrov, 2013). Behaviour and Artefacts are identifiable through the dress code, the architecture, office design arrangements, and modes of speaking (Kukreja, 2019). Although behaviour and artefacts are visible to everyone, although it does not mean that they can be understood by everyone as they are easy to be misinterpreted, they can be confusing for an outsider or observer who wants to make readily available labels upon identifying them (Kukreja, 2019).

Behaviour and Artefacts are the tangible and visible manifestations of organisational culture and they make a first impression on an outsider (Hattangadi, 2017). “Artefacts are the physical, tangible, audible results of activity grounded in values and assumptions” (Hatch, 1993: 659).

2.1.6.2 Espoused Beliefs and Values

The second level is espoused beliefs and values, and these are often championed by the leaders of an organisation (Cheung, et al., 2011). This level is echoed through the organisation’s structures, vision, mission, company policies and goals as pursued by the leaders. If beliefs and values in an organisation are consistent and can be shared with other underlying assumptions then issues of integration amongst group members would be easy to resolve (Schein, 1986). Espoused beliefs and values can assist an organisation to determine how the organisation should be run, how the employees can be managed effectively, and how the customers should be treated (Cheung, et al., 2011).

Espoused beliefs and values are how employees represent their organisation in terms of their behaviour, beliefs, and values (Hattangadi, 2017). “Values are social principles, philosophies, goals, and standards considered to have intrinsic worth” (Hatch, 1993: 659). Espoused beliefs and values are of higher value than basic assumptions and form part of an organisation’s mission, vision, and goals (Kukreja, 2019).

2.1.6.3 Basic Assumptions

The third level is basic assumptions, and these represent attributes that are not visible to the human eye and are unconsciously taken for granted; such as people's feelings, beliefs, thoughts, and perceptions (Dimitrov, 2013). These attributes are the main sources of the underlying values and their supporting activities in an organisation. Attributes and cultural elements that are deemed as unacceptable in an organisation are found or classified at this level (Cheng, et al., 2014).

Basic assumptions are what shape values in an organisation and values shape the behaviour and practices which are a visible part of organisational culture (Kukreja, 2019). Basic assumptions are the key to influencing, understanding, and even changing the culture (Schein, 1986).

2.1.7 Deterrence Theory

Deterrence theory was developed to minimise the extent to which people may engage in illegal behaviour; the view is that human behaviour is largely influenced by some form of incentives, whether good or bad (Ugrin & Pearson, 2010). It is believed that people tend to behave differently when they know that there are consequences for their unacceptable actions (Cheng, et al., 2014).

Deterrence theory is a criminology theory that is based on the implementation of regulatory models that guides employee behaviour and actions in an organisation through the threat of disciplinary action (Ugrin & Pearson, 2013). The theory suggests that the threat of disciplinary action can influence employee behaviour and actions especially when the consequences are greater than the benefits. People are likely to refrain from performing activities that are of unacceptable behaviour, unethical and illegal when they realize and know that the punishment of their actions outweighs the benefits of their wrongful behaviour (Williams & Hawkins, 1986).

The fundamentals of Deterrence theory are that people decide whether to obey or disobey the law after calculating whether the gains outweigh the consequences or not (DiIulio, 1959). It could therefore be said that an employee would be deterred from committing any illegal activities because of the unpleasant experience that they may

suffer if they lose their job or are arrested for their actions (Williams & Hawkins, 1986). Deterrence can have more effects on how people behave when they know what is at risk and the consequences thereof (Ugrin & Pearson, 2013). The deterrence model is presented below, in Figure 6, which shows the components that are believed to influence behaviour; sanction, detection, and enforcement (Ugrin & Pearson, 2013).

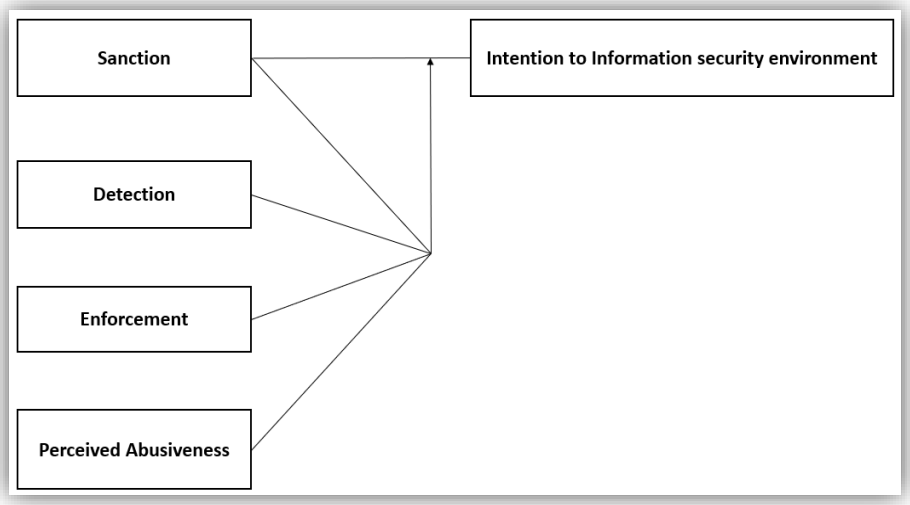

Figure 6: Deterrence theory (Ugrin & Pearson, 2013)

The Elements of Deterrence theory are discussed as follows:

2.1.7.1 Detection

Detection refers to the belief that the authorities may detect any illegal activities or behaviour (Safa, et al., 2019). Detection is the means of monitoring individuals' activities to find any misconduct, causing them to deter if their behaviour was going to result in unacceptable practices (Ugrin & Pearson, 2010). Making individuals aware of detection mechanisms that are in place may cause them to behave differently and consider the consequences of their misconduct (Ugrin & Pearson, 2010).

2.1.7.2 Sanction

Sanction refers to the belief that authorities might consider instituting punishment such as disciplinary action, jail or even dismissal for illegal activities or behaviour (Safa, et al., 2019). "Sanctions are effective to the extent they are deemed to be severe" (Ugrin & Pearson, 2013: 813). Employees are expected to be less likely to

breach information security policies if the potential sanctions are perceived as severe (D'Arcy & Herath, 2011).

2.1.7.3 Enforcement

Enforcement refers to the process of ensuring compliance with policies, laws, and regulations (D'Arcy & Herath, 2011). Deterrence theory views enforcement as a means of sanctions for unethical behaviour.

2.1.7.4 Perceived Abusiveness

Perceived abusiveness refers to the behavioural control and attitude that influence individuals' intentions, and ultimately, their behaviour towards avoiding information security misbehaviour (Safa, et al., 2019: 10).

Now that the theories underpinning the study have been discussed, the next section provides the conceptual research framework.

2.2 Conceptual Research Framework

The following section discusses the conceptual research framework, informed by the two underpinning theories and literature. The purpose of the present study was to describe how organisational culture and deterrence influence behaviour in a university information security environment. The conceptual research framework assisted in analysing the influence of organisational culture and deterrence in a university information security environment. In the study, deterrence was viewed as a behaviour driver in as much as organisational culture determines how an individual behaves in an information security environment. The figure below is a representation of the conceptual research framework.

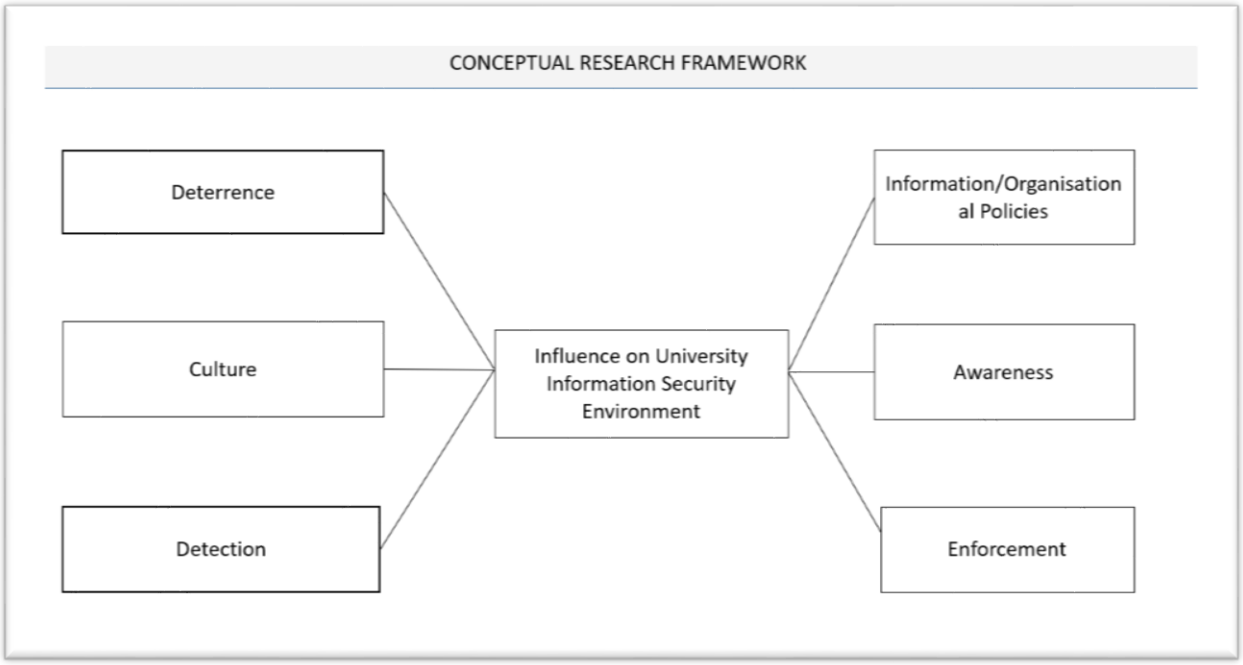

Figure 7: The Conceptual Research Framework

The conceptual research framework in figure 7 above is based on the organisational culture framework (Schein, 2016) and deterrence theory (Ugrin & Pearson, 2013).

2.2.1 Discussion of the Conceptual Research Framework Elements

- **Awareness** - this element is related to the level at which individuals in a University's information security environment are aware of deterrence initiatives and policies that govern their behaviour when dealing with information and its security.
- **Deterrence** - this element considers how deterrence can play a role in influencing the behaviour of individuals in a university information security environment.
- **Detection** - this element focuses on measures that are in place to detect any unacceptable actions or behaviour of individuals in a university information security environment.
- **Enforcement** - this element is related to how organisational and information security policies are enforced in a university information security environment.
- **Organisational and Information security policies** - this element looks at whether policies are defined and whether they are clear relative to how

information security should pan out or manifest in a university information security environment.

- **Culture** - this element looks at how organisational culture manifests in a university information security environment.

2.3 Summary of the Chapter

This chapter provided a review of the existing literature related to and informing the study. From the literature that was reviewed, it is evident that there is not adequate literature that addresses the role of organisational culture and deterrence in information security, especially in a university context. The chapter also discussed the two theories underpinning this study and subsequently provided the conceptual research framework which guided the study and the collection of empirical evidence.

The next chapter describes the research methodology that was followed in the study.

CHAPTER 3

RESEARCH METHODOLOGY

The previous chapter provided the theoretical foundations and theories that informed the present study. This chapter describes the research methodology that was followed in this study. The research methodology outlines the researcher's course of action in answering the research questions. That is, a research methodology provides a framework for answering the research questions how the study is conducted to achieve the study objectives (Creswell, 2014). The chapter outlines and describes the research paradigm followed, the research approach, the research strategy, and the research design.

3.1 Research Paradigm

This section describes the research paradigm followed in the study.

A research paradigm is defined as a set of common agreements, opinions and beliefs which are shared by researchers and scientist on how problems should be viewed and addressed, and it is subject to human error (Guba & Lincoln, 1994). A research paradigm is linked to research questions that need to be answered (Corbin & Strauss, 2008).

A research paradigm is selected based on assumptions about the views, opinions, and how one views the world (Simpson, 2010). A research paradigm is also used to describe how a researcher views the world (Kivunja & Kuyini, 2017). There are three common research paradigms followed in information systems and computing research namely the critical research, interpretive research, and positivist research approach (Yen, 2011).

3.1.1 Critical Research

"Critical research in information systems and computing is concerned with identifying power relations, conflicts and contradictions, and empowering people to eliminate

them as sources of alienation and domination" (Oates, 2006: 412). This was not the purpose and goal of the present study, and therefore not chosen as appropriate.

3.1.2 Interpretive Research

"Interpretive research in IS and computing is concerned with understanding the social context of an information system: the social processes by which it is developed and construed by people and through which it influences and is influenced by its social setting" (Oates, 2006: 406). This was deemed an appropriate paradigm to follow in the present study because the purpose was to describe the role of deterrence and organisational culture in an information security environment, from the views, opinions, and experiences of individuals. Five characteristics of the interpretive paradigm (Oates, 2006) are:

- Study of people in their natural social settings.
- Multiple subjective realities.
- Dynamic, socially constructed meaning.
- Multiple interpretations.
- Qualitative data analysis.

3.1.3 Positivism Research

Positivism research is concerned with providing an explanation that enables the prediction and control of the phenomena, this can be in either a physical or human form (Guba & Lincoln, 1994). The knowledge in positivism consists of verified hypotheses that can be accepted as laws or facts. This was not the purpose of the present study, and therefore not followed.

The present study followed an interpretive research approach as the research paradigm to solicit people's views, opinions, perceptions, and experiences. The study aimed at gathering information and perceptions through qualitative methods from participates regarding a university information security environment. The interpretive paradigm gave the best way to understand the phenomena of a university information security environment.

Table 4: A Summary of the Differences Among Research Paradigms (Guba & Lincoln, 1994)

Paradigm	Explanation
Critical	Acknowledges the difference between reality and people's perception. It has both interpretive and positivist elements.
Interpretivism	Dynamic, socially constructed meaning and multiple realities.
Positivism	Single concrete reality.

Table 4 above briefly shows the differences amongst the three research paradigms.

Table 5: Quality of Positivist and Interpretive Research (Oates, 2006)

Positivism	Interpretivism
Validity	Trustworthiness
Objectivity	Confirmability
Reliability	Dependability
Internal validity	Credibility
External validity	Transferability

Table 5 above briefly identifies the various ways of measuring the quality of the positivist paradigm versus the interpretive paradigm.

Table 6: A Summary of Ways to Collect Data for Each Research Paradigm (Guba & Lincoln, 1994)

Paradigm	Method	Data Collected
Critical	Qualitative and Quantitative	Questionnaires, observation, interviews, focus groups.
Interpretivism	Qualitative	Observation, documents, interviews, and audio-visual materials.
Positivism	Quantitative	Surveys, experiments, questionnaires.

Table 6 above briefly identifies the varied relevant ways of collecting data for each research paradigm.

3.2 Research Approach

This section discusses the various research approaches often adopted for an information systems study.

3.2.1 An inductive or qualitative approach

An inductive approach is "a means for exploring and understanding the meaning individuals or groups ascribe to a social or human problem" (Creswell, 2009: 22). An inductive approach is the analysis of data such as information from the proceedings of the interview, documents, and observation (Bhattacherjee, 2012). This approach uses the language of cases and contexts to understand the concept of the phenomenon (Creswell, 2009). Five features of an inductive approach (Yin, 2011) include:

- "Studying the meaning of people's lives, under real-world conditions.
- Representing the views and perspectives of the people.
- Covering the contextual conditions within which people live.
- Contributing insights into existing or emerging concepts that may help to explain human social behaviour; and
- Striving to use multiple sources of evidence rather than relying on a single

source alone" (Yin, 2011: 8).

The inductive approach often assumes that the data format would be qualitative. And subsequently, the present study took this approach by collecting data through semi-structured interviews to solicit profound views, opinions and lived experiences of individuals. The purpose of the study was to describe how organisational culture and deterrence influence behaviour in a university information security environment.

3.2.2 A deductive or quantitative approach

A deductive approach is "a means for testing objective theories by examining the relationship among variables" (Creswell, 2009: 22). The data is often in a quantitative format. This approach was not deemed appropriate for the present study.

Table 7: Difference between Quantitative and Qualitative Approach (Johnson & Christensen, 2008:34; Lichtman, 2006: 7-8)

Criteria	Qualitative	Quantitative
Purpose	To provide understanding & social interactions are interpreted.	To test hypotheses, look at cause & effect, & make predictions.
Group Studied	Smaller & not randomly selected.	Larger & randomly selected.
Variables	Study of the whole, not variables.	Specific variables studied
Type of Data Collected	Words, images, or objects.	Numbers and statistics.
Form of Data Collected	Qualitative data such as open-ended responses, interviews, participant observations, field notes, & reflections.	Quantitative data based on precise measurements using structured & validated data-collection instruments.
Type of Data Analysis	Identify patterns, features, themes.	Identify statistical relationships.
Objectivity and Subjectivity	Subjectivity is expected.	Objectivity is critical.

Role of the Researcher	Researcher & their biases may be known to participants in the study, & participant characteristics may be known to the researcher.	Researcher & their biases are not known to participants in the study, & participant characteristics are deliberately hidden from the researcher (double-blind studies).
Results	Particular or specialized findings that are less generalizable.	Generalizable findings that can be applied to other populations.
Scientific Method	Exploratory or bottom-up: the researcher generates a new hypothesis and theory from the data collected.	Confirmatory or top-down: the researcher tests the hypothesis and theory with the data.
View of Human Behaviour	Dynamic, situational, social, & personal.	Regular & predictable.
Most Common Research Objectives	Explore, discover, & construct.	Describe, explain, & predict.
Focus	Wide-angle lens; examines the breadth & depth of phenomena.	Narrow-angle lens; tests a specific hypothesis.
Nature of Observation	Study behaviour in a natural environment.	Study behaviour under controlled conditions; isolate causal effects.
Nature of Reality	Multiple realities; subjective.	Single reality; objective.
Final Report	Narrative report with contextual description & direct quotations from research participants.	Statistical report with correlations, comparisons of means, & statistical significance of findings.

Table 7 above gives a brief overview of the difference between the Quantitative and Qualitative approaches and provides a brief understanding of what each approach entails. From the table, it is hoped that the reader would understand the justification for adopting the inductive qualitative approach in the present study.

3.3 Research Strategy

This section describes the research strategy followed in the study.

A research strategy is a plan on how the researcher goes about answering the research question (Saunders, et al., 2012). Common research strategies employed in information systems studies include experiments, surveys, case study, action

research, ground theory, ethnography, and archival research (Oates, 2006). The present study employed a case study as a research strategy, which is discussed next.

3.3.1 Case Study

A case study research is an intensive cross-sectional or longitudinal study of a phenomenon at one or more research sites for the purpose of deriving detailed, contextualized inferences and understanding the dynamic process underlying a phenomenon of interest. Case study research is unique in that it can be used in an interpretive manner to build theories or in a positivist, manner to test theories (Bhattacherjee, 2012: 116). In a case study, the researcher is neutral in a social setting rather than an active participant (Bhattacherjee, 2012).

A case study allows an investigation of a phenomenon in depth and within its real-world context (Yin, 2014). A case study provides a researcher with the ability and opportunities to analyse the different fields in informatics and it is a widely qualitative research method (Manzoor, 2017). That is, a case study research is often described as a qualitative inquiry (Creswell, 2014). A researcher can choose any of the different types of case studies namely explanatory, exploratory, descriptive, multiple, and intrinsic (Manzoor, 2017).

A case study researched strategy was selected as a suitable strategy for this study because it allowed for the gathering of empirical data through observation, individual participant's views, opinions, and lived experiences regarding a university information security environment.

3.3.1.1 Description of the Case

In this study, the case was a university information security environment from the individuals' perspective. The study focused on their views, opinions, and lived experiences with information security. The purpose was to describe how organisational culture and deterrence influence a university information security

environment. The case study allowed for a contextual understanding of how the elements of organisational culture and deterrence manifest from the perspectives of individuals within a university information security environment.

3.4 Research Design

This section describes the research design adopted in the study.

Research design considers the type of data that would be collected, which informs the nature of the research (Manzoor, 2017). The research design is a plan on how the research questions would be answered, giving clear indications of the data sources to be used, how data would be collected and analysed (Saunders, et al., 2016). Discussions of all the other issues such as ethical matters and limitations related to the study that may be encountered are included in this section.

3.4.1 Unit of Analysis

The unit of analysis describes the level at which the study is conducted, which may be a person, organisation, group, or country (Oates, 2006). The unit of analysis in the current study were individuals. That is individuals who are familiar or have a lived experience with information security within a university context.

3.4.2 Study Population

The study population is defined as a list of individuals, organisations, or items from where the sample can be drawn (Wheather & Cook, 2000). The study population consisted of users and individuals who are familiar with or have experience with information security in a university environment, it included university individual decision makers and users from functional departments such as finance, human resources, marketing, information technology units, and the library. The population number, looking at the 26 South African universities, is complex to ascertain hence the sampling frame and method described next.

3.4.3 Sampling Technique

3.4.3.1 Sampling

Sampling in research is a strategy where a researcher examines a sample of a larger population of potential participants and uses the results to draw a conclusion that applies to a broader group of the population (Salkind, 2010). The sampling technique available for drawing samples can either be probability sampling or non-probability sampling (Miller & Brewer, 2003). In selecting a sample, the researcher should ensure that it represents the full set of cases in a meaningful and justifiable manner (Saunders, et al., 2012).

3.4.3.1.1 Probability Sampling

Probability sampling is a technique that is commonly used in survey research strategies where a researcher requires to study the sample to answer the research questions or meet the research objectives (Saunders, et al., 2016). In probability sampling, each item in the population has a chance to be selected or included in the sample (Taherdoost, 2016).

3.4.3.1.2 Non-probability Sampling

Non-probability sampling is a technique where some units of the population have no chance of being selected, the probability of selection cannot be guaranteed or predetermined (Bhattacherjee, 2012). Non-probability sampling is more popular in case study research design and where qualitative data is being collected (Taherdoost, 2016). Non-probability sampling allows a researcher the ability to use selective judgement in selecting the research sample (Saunders, et al., 2016).

3.4.4 Sample Frame

Purposive sampling is a strategy in which a sample is intentionally selected to provide the information that is being studied that cannot be obtained from other choices

(Maxwell, 1996). The non-probability technique referred to as purposive sampling was used for this study and was deemed the most suitable because a sample frame was predetermined. The sample frame consisted of individual decision makers and users who are familiar with or have lived experience in a university information security environment. The individual did not have to be working for a particular university. Notwithstanding this, the study intended to have a sample frame that covers typical roles or positions within a university.

The final number of participants was determined by the point of saturation. The table below shows the number of study participants.

Table 8: Participant Sample Frame

Description of participant's role/position	Number of participants
IT Managers	1
Security Experts	1
Functional Managers	1
End users	2
Software Tester	1
Lecturer	1
Systems Administrator	2
TOTAL number of participants	9

3.4.5 Data Collection Method

Data collection is seen as a system of interrelated activities meant for gathering information to answer the research questions (Creswell, 2014). For a case study research strategy, there are six different methods of data collection which include interviews, documentation, archive records, direct observations, participant

observation and artefacts. The present study employed an interview data collection method.

3.4.5.1 Interview

An interview is defined as a planned conversation between people. This conversation does not occur by chance; that is, there is a purpose for the interview, usually from the person who requested it (Oates, 2006). An interview has an agenda that details the issues that the interviewer wants to find out about and this interviewer will often steer the conversation in the direction of the topic of interest (Oates, 2006). Interviews are a personalised form of data collection and can be conducted face-to-face, telephonically, or in a focus group (Bhattacherjee, 2012) and virtual, especially looking at the current Covid-19 circumstances. Interviews are categorised as either structured, semi-structured or unstructured interviews (Saunders, et al., 2016).

3.4.5.1.1 Structured interviews

Structured interviews are conducted to collect quantifiable data and make use of questionnaires based on a pre-determined set of questions which are administered by the interviewer. In a structured interview set up, the interviewer reads out each question to the interviewee and records their response on a standardised schedule such as pre-coded answers. This was deemed not appropriate for the present study.

3.4.5.1.2 Unstructured interviews

Unstructured interviews are informal in nature and are conducted when a researcher wants to gain an in-depth understanding of the area of interest. There is no list of pre-defined questions in an unstructured interview; however, the interviewer needs to have clear objectives for conducting the interview. The interviewer can allow the interviewee to freely discuss their beliefs, events and behaviour about the topic of interest without restrictions.

3.4.5.1.3 Semi-structured interviews

Semi-structured interviews are conducted to collect qualitative data where the interviewer usually has a list of themes and key questions that they want to cover during the interview. Semi-structured interviews contain a list of themes, questions to be covered and the interview schedule. In semi-structured interviews, the interviewer can have follow-up questions, comments, and open discussions with the interviewee. That is, the interviewer is at liberty to explore and follow leads during the interview or discussion. This data collection method was deemed appropriate for the present study, looking at the purpose and goal of the study.

The study conducted semi-structured interviews with individuals who are familiar with or have a lived experience of a university information security environment. All interviews were conducted online and recorded via Microsoft Teams. The interview sessions began with an explanation of the purpose of the study, allowing for informed consent and permission to digitally record the session. The interview sessions took an average of 35 minutes.

3.4.6 Data Analysis Method

Data analysis is the process of cleaning, transforming, modelling data to discover useful and understandable information, and identifying the main themes that come from descriptions given by the participants in answering questions (Oates, 2006). In this study, a thematic analysis technique was used to analyse the data collected. Thematic analysis is defined as a method for detection, analysis and reporting the themes in the data (Javadi & Zarea, 2016). This study was inductive and thus thematic analysis method was deemed appropriate. An inductive approach categorises the data being analysed. The data analysis assisted in understanding the participant's views and opinions that were discussed during the semi-structured interviews.

3.5 Validity and Reliability of Qualitative Research

This section discusses the validity and reliability of this study.

Qualitative validity means “that the researcher checks for the accuracy of the findings by employing certain procedures, while qualitative reliability indicates that the researcher’s approach is consistent across different researchers and different projects” (Creswell, 2009: 176). Reliability focuses on the possibility of participants responding to the same questions in the same manner as they did previously (Oates, 2006).

For the research findings to be considered reliable and valid, they need to have these characteristics which are trustworthiness, credibility, transferability, dependability, and conformability (Anney, 2015). All these validity and reliability characteristics of research findings are briefly discussed below in relation to this qualitative study.

3.5.1 Trustworthiness

The concept of trustworthiness in qualitative research is defined as the ability to ensure that the study is carried out in a manner that addresses credibility, allows transferability, meets dependability and lastly, achieves conformability (Shenton, 2004). The trustworthiness of the data was confirmed by the similarity of the responses received from the interviewees.

3.5.2 Transferability

Transferability of this study was ensured by making sure that the findings from this study can be applied to another situation or the varied university contexts.

3.5.3 Credibility

This study ensured credibility by studying only what it was intended to be studied and by analysing the data accurately. This was also achieved by keeping the audio recordings and proceedings of the semi-structured interviews.

3.5.4 Dependability

This study ensured dependability by doing real interviews with participants, recording the proceedings, and keeping them safe on cloud storage.

3.5.5 Conformability

This study ensured conformability by conducting a data audit of the actual interviews, examining the data collection process and data analysis. Thus, making it possible that the findings can be confirmed by other researchers who may conduct a similar study.

3.6 Ethical Considerations

This section describes the research ethics that were followed in conducting the present study.

Ethics refers to the researcher's behaviour in relation to that of the participants, putting into consideration their rights, privacy, and involvement in the research (Saunders, et al., 2016). All the data that was collected during the study remains confidential to ensure that the participant's anonymity; that is identity, interest and future well-being are protected. The data will not be used for any other purposes besides analysing the influence of organisational culture and deterrence in a university information security environment.

Informed consent was obtained from participants by discussing the purpose and the goal of the study. Participants were also informed that their participation, although invaluable, is done voluntarily and that they may withdraw at any time. Their participation also remains anonymous to protect their right to privacy. No emotional and physical harm was envisaged. The study was conducted in a manner that adhered to the rules and guidelines of the Human Research Ethics Committee (Non-Medical) at the University of Witwatersrand. The ethics clearance certificate protocol number is H20/08/40.

3.7 Summary of the Chapter

Chapter 3 described and justified the research methodological choices followed for the study. Firstly, the research paradigm was discussed followed by the research approach, research strategy and lastly the research design. The chapter that follows analyses the data collected and discusses the findings thereof.

CHAPTER 4

DATA ANALYSIS AND DISCUSSION OF FINDINGS

In this chapter, data are analysed, and the findings are discussed. Thematic data analysis is done to determine the role of organisational culture and deterrence in a university information security environment.

4.1 Analysis of Qualitative Data Collected

The process of data analysis and discussion of findings follows three themes and subthemes. The themes were predetermined and are synonymous with study objectives. For each theme and subtheme, the interview question is posed, this is followed by the participants' responses in italics. A brief discussion is then given.

4.1.1 THEME A (study objective one): To analyse and describe how organisational culture influences information security behaviour in a university environment.

Interview question: Please discuss your role and familiarity with information security in the context of a university environment?

> *"...In my role, I have access to students' and lecturers' information that is stored on the system that I administer. Information security is about me protecting this information that I have access to and not share it with anyone who is not supposed to see the information".*

> *"... I have access to a lot of sensitive information and my role compels me to protect the information and make sure that I follow the processes that are in place when I need to disclose it".*

> *"... In the University, my role gives me access to student and my staffs' information, salaries, departmental budgets etc. I am aware that I should maintain information*

security and not share the information that my role allows me to access to anyone else".

The information security role entails handling confidential information and the understanding is that protecting this information is vital in preserving stakeholders' privacy.

"... I draft a lot of policies and share confidential information; in my employment contract, some clauses speak to how we should behave and deal with the information at my disposal".

"... In my daily duties, information security is about making sure that I keep the information safe and do not endanger those that I interact with or have access to their information".

University information security policies govern how individuals handle sensitive information in a workplace. Therefore, policies are used as a deterrence mechanism.

Finding

The participants' roles in a university information security environment vary, showing that the phenomenon is a complex social activity system that comprises of various actors interacting with each other.

Interview question: Please share your understanding of information security.

"... It is the secure collection, storing, use and distribution of private information whether it is student's information, personal or financial information which is used, stored and processed securely. Having policies in place to direct how information is to be accessed and used. Restrictions are in place in terms of what access I have and which resources I can access. If information wrongfully leaves the system, it can jeopardize the students, lecturers, and the whole University, it can have operational and reputational damage for the institution".

"... Ensuring that you do not give out valuable information that might put you in danger. Ensuring safety online and from hackers".

"… Preserving of private information such as names, addresses, Identity Numbers, email addresses and more. Protecting any information that can be used against you".

Information security and the awareness thereof are critical in a university information security environment and that there is a need for the phenomenon to be well understood to ensure that information is always secured, and privacy is maintained.

"… Securing of information that entails everything about the University, how things work, how they should work, securing passwords, and the network".

"… Keeping all information private and secure. Ensuring that the University has the best systems to achieve securing information. Making sure that data subjects know-how information should be managed".

"… Taking cognizant of all the information available and all the measures in place within the University and act accordingly".

Individuals' day to day activity entails protecting and preserving confidentiality and that is important in a university information security environment.

Finding

The participants show a fair understanding of what information security is and what it entails. Their understanding of this phenomenon is key to information security in a university context.

Interview question: Please describe what organisational culture means to you?

"… Organisational culture drive how I must safeguard the information that I have access to protect the reputation of the University and prevent financial loss. It enforces how each department should handle information and making them aware of how not safeguarding thereof could mean for the University".

"… Keeping us updated in terms of the latest threats, phishing, and any other information security trends".

Organisational culture's importance is embedded in how individuals perform their duties which involves guiding how they behave when handling information.

> *"… It relates to how we behave as an organisation, how we give out information, protect it, and how we share it amongst ourselves. Making sure that we follow strict guidelines when sharing or disclosing information while maintaining privacy and copyright".*

> *"… The way that the University and I conduct ourselves with information security".*

> *"… Securing password, anyone who is not part of the University's network should not have access to it".*

Organisational culture guides behaviour, how confidential information is safeguarded by individuals in a university information security environment.

> *"… Information security is part of the organisational culture; it guides how I treat information. The values of the University are aligned to the confidentiality of information".*

> *"… Each organisation has its own, the University must ensure that there is safety for everyone who identifies with the University. It is how I protect all the information in my possession and not use it carelessly".*

Finding

Organisational culture may have a different meaning for each participant; however, it shapes how they treat, safeguard, and preserve information security and privacy.

Interview question: Is information security part of the organisational culture in the university?

"… Yes, it is. People are made aware of their responsibilities with information security. There are access control mechanisms in place to ensure that you only have access to information that is required to perform your role and no more than that".

"… Yes, departments like HR and IT have employee information and it is protected from unauthorized access. Information in the University is not shared with external parties without consent".

"… Yes, it is evident even for students, during the first-year students' seminars the IT department has information security seminars for students".

Information security being part of organisational culture could mean that there are more efforts directed towards improving individual's behaviour which could influence how they handle confidential information accessible to them.

"… Not entirely. The only time that I am aware of any information security issues and initiatives is when there is IT communication sent out. It is not information that is everywhere you go around campus, it is not part of the organisational culture".

There is a need for the universities to incorporate information security into the organisation's culture. That effort can aid in promoting a good information security culture and organisational culture, which may result in good information security behaviour amongst individuals.

"… Yes. Information security initiatives are visible. Information security is part of the organisational culture. There is a lot of information security communication that is done".

"… Yes. Each day when you walk into campus there are banners on the main entrance that talk about information security. When you log into your computer there is a notice about preserving privacy and confidentiality".

"… Yes. It is one of the pillars of the University. It follows a top-down approach, communicated from the vice-chancellor level".

Finding

From the participant's responses, it seems like information security is not entirely part of the organisational culture, a lot of efforts need to take place to improve this. Some of the participants indicated that information security is part of the organisational culture to a satisfactory level.

Interview question: In your opinion, what could be done to make sure that information security is part of the organisational culture in the university?

> *"…More visibility of policies that guide how people should manage information security. Departmental meetings should have information security on their agenda. Make policies easier accessible or available to everyone and in a simple language".*

> *"… Making attendance of information security awareness sessions compulsory for all employees. Raising awareness of rules and regulations that govern information security and making that a priority".*

Individuals' need to be constantly reminded of acceptable information security practices and how thing are done in the university. This can be achieved in many ways such as training, staff engagements, meetings, and workshops.

> *"… I believe that it is already part of the organisational culture".*

> *"… Maybe have a lot more security measures implemented to protect student information".*

> *"… It is part of the organisational culture as the values of the organisations to tie to information privacy, security, and confidentiality".*

> *"… Consistent awareness training that will talk about the importance of securing information, the consequences of leaking information and ethical considerations".*

Finding

Evidently, not everyone is not sure of what could be done to make sure that information security is part of the organisational culture in the University. Some individuals recommend that there be more awareness of information security and its importance.

Interview question: If organisational culture influenced your behaviour towards information security, describe how your behaviour has been influenced?

> "*I know how I need to behave when I am handling confidential students and lecturer's information and what could happen if I am negligent. It is part of the culture in the University, we are trained and made aware"*.
>
> *"… The organisational culture is that we treat the information that we have access to with respect so when I handle someone's information, I know how I should behave".*
>
> *"… When I am working on a public computer, I am more cautious and make sure that I log out when I am done with my session. If I am browsing and the website looks doggy, I immediately log out"*.
>
> *"… I know what is right and wrong when dealing with private and confidential information at my disposal".*
>
> *"… Yes. As I had mentioned previously that information security is part of the organisational culture and it is included in our employment contract, so it does direct how I handle information".*

A well-implemented or adopted organisational culture may strongly influence how individuals interact with information security regardless of whether someone is watching them or not. The individuals are guided by the organisation's culture and therefore behave in accordance with the principles of the university.

> *"… Not entirely, I know what is expected from me and I act right and ethically".*

"… Like I mentioned earlier that there is no visibility of what the organisational culture is in terms of information security in the University. I am guided by my ethical behaviour in terms of how I handle information security".

There are instances where individuals know what is deemed as ethical behaviour and not, that knowledge guides their behaviour when handling sensitive or confidential information. Individuals must preserve information security and the image of the university when performing their duties.

Finding

The majority of the individuals' behaviour has been influenced by organisational culture. There are however a few of the participants that are influenced by their ethical behaviour.

4.1.1.1 Findings for Theme A (study objective one): To Analyse and describe how organisational culture influences information security behaviour in a university environment.

This summarizes the findings for Theme A as per the responses from the participants.

- Participants are fully aware of what information security is and what it entails in their role at the University.
- The understanding of the role of organisational culture in information security does not seem clear for some of the participants.
- Some participants indicated that information security does not seem to be part of the organisational culture.
- Participants believe that organisational culture can influence how they behave with information security.
- Some of the participants were not sure of what could be done to make sure that information security is part of the organisational culture.

4.1.2 THEME B (study objective two): To analyse and describe how deterrence influences information security behaviour in a university environment.

Interview question: What is your view on how deterrence should be dealt with in a university environment?

> *"… It should be included in organisational policies; our contracts and we should have constant reminders".*

> *"… There should be deterrence initiatives and notifications that we receive from time to time. I should be made to fear the thought of stealing any company information, abusing the internet etc.".*

> *"… Policies and guidelines in the work environment should deter us from any unethical behaviour".*

The importance of information security policies, rules and regulations must be made known to individuals working in a university information security environment so that they behave accordingly and do not disclose sensitive information that they are not supposed to.

> *"… We should be told about it to know what we cannot do in the work environment as well as know what is considered as an unacceptable/ acceptable behaviour".*

> *"… There should be visibility of what we can do and what we cannot do when dealing with information security. There should be someone that constantly tells us what is illegal over and above having it on policies. There must be deterrence clauses on employee contracts".*

> *"… Penalties of non-compliance should be visible. Employees should be made aware of all deterrence factors".*

> *"… As part of policies, it should be stated that an employee will be held liable for unethical behaviour, and disciplinary action could be taken".*

Penalties for non-adherence to information security policies must be imposed for individuals working in a university information security environment. This may assist in deterring individuals from breaking laws and not complying to set policies.

> *"… Consistent awareness training where the importance of information security is discussed, the consequences of sharing confidential information are shared".*

> *"… Give individuals access to policies and guidelines as well as training to ensure that they are fully aware of their function, responsibility, and expectations. This will also help in making sure that we do not endanger the University or bring it into disrepute".*

Finding

The majority of the participants are of the view that deterrence should be part of organisational policies and must be included in their employment contracts. Some participants alluded that there must be more initiatives or means to make them aware of deterrence factors and what is considered ethical or unethical behaviour in information security.

Interview question: In your view, would you say that deterrence can improve information security or not?

> *"… Yes. You are more likely to behave better, take care of yourself and the information that you are entrusted with. There is better decision making in terms of handling information".*

> *"… Yes. Employees would be more conscious of how they handle confidential information, and the behaviour would be different. Right now, information security is not a priority but if I were constantly reminded or deterred then I would behave differently".*

"… Yes, because it is about knowing and being informed on what procedures to follow. Once you know then you behave accordingly".

"…Yes, students would be prompted to be more aware and vigilant. I would practice more information security".

"… Yes, if you are deterred you are more likely to comply and treat information security better".

If individuals are made aware of information security policies and how they need to handle sensitive information, the university is more likely to improve its information security environment and preserve privacy. An informed workforce is more likely to behave better when handling sensitive information.

"… Yes, if people are deterred, they are behaviour is much better. They fear doing wrong".

"… Yes, if I know the consequences of my behaviour I will act accordingly and respect the information. If I am not deterred, I will behave however I want.

"… Yes, when you know the law and the consequences thereof you become afraid or rather your behaviour is more on the compliance side. You treat information better as a context of what I can and cannot do is created".

"… Yes, no one wants to dent their image because they did not preserve information security. Deterrence is one way to endure that people comply".

Finding

Individuals believe that deterrence can improve a university information security environment and someone's behaviour when dealing with private and confidential information. They are also of the view that deterrence may influence how they behave when handling sensitive information.

Interview question: Is deterrence communicated in the university? What could the implications thereof be?

> *"… Yes. Handlers of information need to know how to behave when handling University information. Deterrence can shape behaviour and help protect the reputation of the University and any financial losses that may be a result of negligence with information*".

> *"… Yes. It might help if all employees are made aware of deterrence and information security as at some point they deal with confidential information and we must know how to treat the sensitive information and what will happen if we do not behave according to the policies".*

> *"… Yes, each environment has its own rules, policies and regulations, therefore, people must know what they are and what they entail. People must be guided and deterred".*

It is important to communicate information security policies to employees, this enables them to be more knowledgeable in terms of what is considered acceptable behaviour and not in the university. The communication of policies may also play a role in deterring wrongful doing and unethical behaviour, which may result in an improved university information security environment.

> *"… it is already part of the communications and organisational culture in the University. The implications are improved behaviour in the handling of information".*

> *"… Yes. It can change attitudes. People will take their work more seriously and not share any information that they are not supposed to. Information security would be more respected".*

> *"… It should. It can change how people treat confidential information".*

Deterrence may influence how individuals handle sensitive information in a university information security environment. It may also assist in changing behaviour, carelessness and aid in individuals handling information better or differently.

"… Yes, especially considering how the way we used to work has changed. It can help to remind us what is acceptable and not when dealing with information security".

Finding

Individuals are of the view that information security deterrence factors should be communicated more. They believe that it could influence how people behave when handing information.

Interview question: Relating to the handling of information, kindly share your experiences on how deterrence can influence one's behaviour.

"… My understanding of the implications of what could happen to me, my career if I do not comply with information security policies and guidelines make me want to constantly comply. Also, I know how it can impact the University if I do not behave accordingly. The education thereof has helped in guiding me".

"… If there is no deterrence and guidelines you will behave as you please. Knowing the consequences of my behaviour help me behave in line with policies as I am bound to act accordingly. It teaches me discipline".

"…I know that I cannot share students' marks, employee salaries or any confidential information, I need to uphold policies. I am ethical and of integrity. I do not want to lose my job. I am fair and have learned what is acceptable and not".

Deterrence may influence how individuals behave in a university information security environment and how they handle information. It may lead to individuals' maintaining information confidentiality and preserving its integrity.

"… It puts me in check. It is something that prevents me from misbehaving, doing wrong or even leaking information".

"… When you have access to confidential information you are supposed to be a

custodian, a role model, do the right things and uphold integrity. Knowing what could happen to me for disclosing confidential information plays a role in how I handle information as no one wants to be punished for such mistakes".

Finding

Individuals indicate that knowing the consequences of non-compliance influences how they behave when handling confidential information.

Interview question: Do the university policies and regulation deter certain behaviours?

"… Yes, but there is room for more in terms of more guidelines and creating awareness of the policies. Notice boards should have deterrence rules and guidelines for everyone to know".

"… There are more than enough policies in place however they are not known or communicated".

"… I am not sure, as far as I understand each faculty has policies to guide behaviour but most employees either do not know them or have not read them".

"… Yes, we know that there are policies, but they are not communicated to us".

Information security policies are necessary to deter behaviour however it is of utmost importance for individuals to be made aware of the policies. For individuals to be deterred from wrongful behaviour, they must know what the policies entail and what the consequences of non-compliance are.

"… Yes, we have more than enough policies such as brand policy, information security policy, social media policies and more but people do not read them because they are too lengthy".

"… Yes, but more can be done as the environment that we operate in has changed and keeps changing rapidly. Policies must evolve and speak to the things that we are experiencing currently e.g., working online because of COVID19".

Finding

Most of the individuals are of the view that there are adequate policies to deter employees however they are not well communicated and some of them are too long to read.

4.1.2.1 Findings for Theme B (study objective two): To analyse and describe how deterrence influences information security behaviour in a university environment.

This summarizes the findings for Theme B as per the responses from the participants.

- Deterrence factors should be communicated with everyone, participants believe that if they are made aware then they will know what can and cannot be done in a university information security environment.
- Deterrence does play a role in how some participants handle the University's confidential information.
- Deterrence initiatives should be communicated more often as they provide guidance and direction on one's behaviour.
- There are enough policies to guide or influence behaviour however they are too lengthy for employees to read and familiarize themselves with them.
- Policies need to be summarized and communicated to employees on an ongoing basis.

4.1.3 THEME C (study objective three): To analyse and describe how awareness influences information security behaviour in a university environment.

Interview question: How are information security initiatives managed in the university and would you say that it plays a role in how you handle information?

"… Phishing simulations are sent out to the University community. There are regular email notices. There are also webinars on information security topics. It does play a role but there is more to be done to make people more aware".

"… There are webinars, seminars, and email communications on information security. For me, it does not play a role as I had mentioned earlier that I am guided by my ethical behaviour. I have no bad intentions or desires to harm the University, but it has nothing to do with the information security awareness initiatives".

"… We have workshops, talks and email communications on the importance of information security. It does play a role because I know that there are processes to follow in the University, I must protect the information that I have access to, and it helps in maintaining confidentiality".

Individuals working in a university information security environment must be trained on matters of information security, confidentiality and privacy. When they are in the know, they are more like to handle information better and prevent unauthorised access and disclosure of sensitive information.

"… We are sent email communications, it does play a role because now I am more cautious about how I deal with information security".

"… We have HR and IT monthly information security awareness training, new employees are taken through an induction process where they are informed of the information security policies. They do play a role as from time to time I am reminded on how to handle private and confidential information and maintain information security".

"… There are posters and banners around the campus, and we also have webinars. They do because I am aware, I behave better than someone who is not".

Information security awareness should be an ongoing activity as individuals might be faced with different challenges from time to time. Additionally, the information security

landscape changes rapidly therefore the individuals' must know how to behave when handling information security issues in a university information security environment.

> *"… We are informed through communication, campaigns, and surveys. Yes, it does because I am made aware of how I should behave".*

> *… There are poster and HR training, yes as they reiterate my responsibility regarding information security.*

> *"… We have training on how to handle information, passwords, and online learning platforms, meetings are conducted to address any concerns. The initiatives do influence how I handle information and maintain information security, they also help to guard information".*

Finding

Information security awareness initiatives seem to influence how most of the participants handle information.

Interview question: In your opinion, what would you say are the reasons information security awareness is done?

> *"… To make everyone who handles information have a high level of information security and understand its importance".*

> *"… To make people more knowledgeable. With awareness comes a change in behaviour and with a behaviour change comes a more secure information security environment in the University".*

> *"… For us to be informed on information security matters. To gain knowledge and know what is expected from us (understanding and wisdom). To ensure that we make better decisions and not make mistakes in information security".*

Constant information security awareness may influence the behaviour of individuals as well as promote a culture of informedness in a university information security environment. Information security awareness may also act as a reminder of policies, regulation and acceptable practice in a university.

> *"… To avoid information leakages, to protect people from scammers, to protect the image of the University, to protect everyone that is involved and their private information from unauthorized disclosure".*

> *"… To change attitudes, to be directed on how we should behave, to minimize confusion and to ensure that people are more knowledgeable".*

> *"… To remind staff of policies that govern information security and what they entail''*.

Finding

Individuals are of the view that awareness is done to make people more knowledgeable and give guidance on how to handle information.

Interview question: Based on your experience, how should employees be made aware of policies that govern information security, current laws, and regulations in the University?

> *"… Workshop attendances should be made compulsory".*

> *"… More awareness but not on email as I do not think that it is effective. Consider screen pop up messages, posters in the lifts and notices around the University".*

> *"… Continuous initiatives and awareness such as themed communication in line with what the month resembles in South Africa. For example, heritage month, women's more and so forth".*

There are numerous ways that a university can raise awareness on information security policies, laws and regulation. It is important that the awareness training is

customised for each target audience and is relevant to the type of information that they handle so that they know how to behave.

> *"… Through workshops, fun drives on Friday for students and give away prices to make it fun. Also, social media posts for the larger community including fun facts".*

> *"… Summarize policies, have more information security initiatives, more engaging exercises".*

> *"… A campaign from line managers to employees, graphical posters in bullet points and office flyers".*

> *"… TV screen popup messages, one-liner messages from time to time, social media posts".*

> *"… Email notifications, sessions, and training".*

Finding

Most of the individuals agree that communication and awareness are the keys to staying informed.

Interview question: Please share with me an experience of what unawareness of information security has led to?

> *"… Leaked examination papers that led to investigations and people losing their jobs".*

> *"… It has led to making a lot of mistakes when you do something that is not permitted but because I was unaware I did it either way".*

> *"… Being scammed, valuable information ending up in the wrong hands, job losses because of negligence".*

Unawareness of information security policies and principles may sometimes lead to a lot of mistakes, individuals may erroneously share or mishandling sensitive information that they would not if they were aware of the information security policies that guide behaviour in a university.

> *"… People disclosing information that they were not supposed to".*

> *"… I know of a colleague who did not follow information security procedures who ended up being fired".*

Finding

Unauthorized disclosure of information and job loss seemed to be what most of the individuals have experienced.

Interview question: What do you think could be done to improve such (previous question)?

> *"… Let people be aware of policies and disciplinary actions in an event where they do not conduct themselves the way they should".*

> *"… To be taught on information security but subject matter experts but also the person that is being taught must be available and willing to learn".*

Ongoing information security awareness education or training may be a tool that a university can use to influence behaviour and better handling of confidential information.

> *"… Awareness initiatives can help with avoiding such".*

> *"… Reiterate staff responsibilities regarding information security".*

> *"… Refresher training and constant information security discussions in meetings".*

Finding

Individuals' in a university information security environment must be made aware of the policies and regulations that they should abide by. Training and education should be conducted on an ongoing basis to foster behaviour change.

Interview question: In an event where you or a fellow worker is unaware of a particular aspect of information security, what do you do?

> *"… I read up on the subject or topic, google or even ask the information security colleagues for more information and insight".*

> *"… I enrol for courses, go search on Google, ask around or check videos online".*

> *"… I ask around and do a bit of research on the subject*.

Individuals working in a university information security environment must be encouraged to empower themselves with knowledge either through attending courses, reading up on topics of interest on the internet or by asking information security experts for more clarity where required.

> *"… I use Google, YouTube, and social media*".

> *"… I ask around especially people in the information security environment".*

> *"… I read on the subject, books, and the internet".*

> *"… I look for information all around, read books, the internet and I ask friends or colleagues. We also have an email address that we can write to when we are in doubt and a hotline number to call".*

Finding

Individuals' do ask around or consult books and online resources to stay informed and knowledgeable of information security trends and topics.

Interview question: In your opinion, how could the information security environment be improved in the university if it needs to be?

> *"… Have mandatory information security workshops. Design a policy pack for new employees so that they are aware of how they should conduct themselves in the University's information security environment. Have policy refresher sessions for existing employees and thereafter they should be sent copies of the policies where they must sign to acknowledge that they have read and understood what behaviour is expected from them".*

> *"… Make attendance of information security sessions compulsory and employees would be more informed or knowledgeable. Include policies and awareness in induction sessions".*

> *"… Through communication. Policies governing information security should be communicated with everyone through emails, pamphlets, workshops, and talks".*

> *"… What I had mentioned earlier such as workshops, fun drives on Friday for students and give away prices to make it fun. Also, social media posts for the larger community including fun facts".*

> *"… A lot of technical security measures such as biometrics, improved access controls, protection of information".*

Individuals must be reminded of information security policies, this can be part of staff meeting agendas, emails sent out when there are updates on the policy. The importance of information security must be reiterated.

> *"… Ongoing information security campaigns, policy drives, roadshows, and poster around the campus to remind employees on how to behave with information security".*

> *"… Discuss the consequences of non-adherence to information security policies. Monthly awareness sessions and newsletters".*

> *"… Educate people on the subject and technology. Create awareness so that it*

becomes part of the organisational culture and operations. Educate employees of any new trends in a language that is understandable and not using IT jargons".

Finding

Ongoing communication, awareness and compulsory workshop attendance could lead to an improved information security environment.

4.1.3.1 Findings for Theme C (study objective three): To analyse and describe how awareness influences information security behaviour in a university environment.

This summarizes the findings for Theme C as per the responses from the participants.

- Awareness of information security is important in influencing how to handle private and confidential information.
- Unawareness of information security policies and guidelines can lead to unauthorized disclosure of information, job losses, and reputational damage.
- Policies must be summarized for employees and be communicated on an ongoing basis.
- Information security information resources must be made available and easily accessible.
- Awareness initiatives must keep up with the times, be relevant and informative.

4.2 Summary of the Chapter

Chapter four presented data analysis of the participant's responses to the semi-structured interviews that were conducted during data collection. The analysis of data was done thematically, the study objectives were themed as informed by elements of organisational culture, deterrence, and awareness of information security.

4.2.1 Overview of Study Findings

The findings are summarized per theme as follows:

Theme A: How organisational culture influence information security behaviour in a university environment.

- Participants are fully aware of what information security is and what it entails in their role at the University.
- The understanding of the role of organisational culture in information security does not seem clear for some of the participants.
- Some participants indicated that information security does not seem to be part of the organisational culture.
- Participants believe that organisational culture can influence how they behave with information security.
- Some of the participants were not sure of what could be done to make sure that information security is part of the organisational culture.

Theme B: How deterrence influence information security behaviour in a university environment.

- Deterrence factors should be communicated with everyone, participants believe that if they are made aware then they will know what can and cannot be done in a university information security environment.
- Deterrence does play a role in how some participants handle the University's confidential information.
- Deterrence initiatives should be communicated more often as they provide guidance and direction on one's behaviour.
- There are enough policies to guide or influence behaviour however they are too lengthy for employees to read and familiarize themselves with them.
- Policies need to be summarized and communicated to employees on an ongoing basis.

Theme C: How awareness influences information security behaviour in a university environment.

- Awareness of information security is important in influencing how to handle private and confidential information.

- Unawareness of information security policies and guidelines can lead to unauthorized disclosure of information, job losses, and reputational damage.
- Policies must be summarized for employees and be communicated on an ongoing basis.
- Information security information resources must be made available and easily accessible.
- Awareness initiatives must keep up with the times, be relevant and informative.

The next chapter will interpret the findings detailed above.

CHAPTER 5

INTERPRETATION OF THE FINDINGS AND RECOMMENDATIONS

This chapter interprets the study findings against existing literature to determine the role of organisational culture and deterrence in a university information security environment. The interpretation of findings is also done per theme, synonymous with study objectives. A recommendation, informed by the interpretation is then given.

5.1.1 Interpretation of how organisational culture influences information security behaviour in a university environment

This section interprets how organisational culture influences information security behaviour in a university environment.

Van Niekerk and Von Solms (2010) maintain that organisational culture is the principles that direct behaviour and activities within an organisation, it could be beliefs, values or norms which are shared by individuals. The study participants mentioned that…

… Organisational culture drive how I must safeguard the information that I have access to protect the reputation of the University and prevent financial loss. It enforces how each department should handle information and making them aware of how not safeguarding thereof could mean for the University.

Another participant noted.

… It relates to how we behave as an organisation, how we give out information, protect it, and how we share it amongst ourselves. Making sure that we follow strict guidelines when sharing or disclosing information while maintaining privacy and copyright.

The responses above give an indication that some of the participants are aware of what organisational culture is and the role it plays in a University information security

environment. It is also evident that organisational culture does to a certain degree influence the participants behaviour when handling information security matters.

Organisational culture assists individuals in an organisation to distinguish between what is important and what is not important (Ahmady, et al., 2016). Organisational culture gives rise to the organisation's general norms and behaviour that employees will adopt for example, how they talk, dress, and behave (Du Plessis & Hoole, 2006). The participants mentioned that…

… organisational culture relates to how we behave as an organisation, how we give out information, protect it, and how we share it amongst ourselves. Making sure that we follow strict guidelines when sharing or disclosing information while maintaining privacy and copyright.

…The way that the University and I conduct ourselves with information security.

… departments like HR and IT have employee information and it is protected from unauthorized access. Information in the University is not shared with external parties without consent.

It is evident that understanding the role that organisational culture plays in handling information security. It helps them realise the importance of following procedures and guidelines when disclosing information. Where there are no written policies or laws individuals in an organisation are guided by the organisational culture (Ahmady, et al., 2016). One participant mentioned that…

… Information security is part of the organisational culture; it guides how I treat information. The values of the University are aligned to the confidentiality of information.

The response above indicates that organisational culture guides how individuals in a University treat information security. Even in the absence of policies and laws, the participants indicated that organisational culture influences their behaviour.

Recommendations from Theme A:

In the present study, like in literature, organisational culture was found to influence information security behaviour, notably in the handling of confidential information and maintaining security thereof. It is therefore recommended that more awareness initiatives should be undertaken to communicate the importance of organisational culture and how it could be used as a tool to improve information security behaviour in a University.

It is also recommended that ongoing workshops should be conducted with the University's community as a constant reminder of what acceptable behaviour is and how they should conduct themselves with information security.

5.1.2 Interpretation of how deterrence influences information security behaviour in a university environment

This section interprets how deterrence influences information security behaviour in a university environment.

Deterrence is a psychological process that involves deterring individuals from committing any criminal activity by showing them the dire consequences of their actions (Williams & Hawkins, 1986). The participants remarked that…

… It might help if all employees are made aware of deterrence and information security as at some point they deal with confidential information and we must know how to treat the sensitive information and what will happen if we do not behave according to the policies.

… Handlers of information need to know how to behave when handling University information. Deterrence can shape behaviour and help protect the reputation of the University and any financial losses that may be a result of negligence with information.

Deterrence is important in information security, it makes individuals aware of what the consequences of their actions are therefore allowing them to weigh their options beforehand. The participants' responses above indicate that the participants believe that it is important to deter individuals to influence their behaviour with information security. The participants also indicated that deterrence is efficient and can shape one behaviour with information security.

Deterrence is useful in situations where the aim is to curb any illegal activities from taking place rather than in instances where the illegal activities have already taken place and you are now seeking to punish the act (Bhattacherjee & Shrivastava, 2018). The participants mentioned that …

… deterrence can change attitudes. People will take their work more seriously and not share any information that they are not supposed to. Information security would be more respected.

… deterrence can help to remind us what is acceptable and not when dealing with information security.

It is human nature that people will behave differently and as they wish, however when they are deterred from committing certain actions, they tend to calculate their options and consequences of their actions. The participants' responses above indicate that if they are deterred, they are more likely to behave differently, they can refrain from sharing confidential information that they are not supposed to and secure information at their disposal.

If people are aware of the consequences of their actions, they are more likely to refrain from instituting those actions (Hu, et al., 2011). The participants remarked that…

… deterrence can change how people treat confidential information.

... The implications of deterrence are improved behaviour in the handling of information.

Based on the responses above it is evident that individuals are of the view that deterrence can influence their behaviour and make them compliant to policies and laws that guide how they should treat information security.

Recommendations from Theme B:

Individuals understand what deterrence entails and the role it plays in an information security environment. They also understand that deterrence can assist in curbing behaviour.

The University should make sure that individuals in a university information security environment are deterred from wrongful doing and are aware of the consequences of their behaviour.

To influence behaviour individuals should be deterred from any wrongful, illegal, and unethical behaviour on an ongoing basis.

It is also recommended that the University publish notices, send out emails communications and have posters or banners with messages of deterrence.

5.1.3 Interpretation of how awareness influences information security behaviour in a university environment

This section interprets the findings from studying how awareness influences information security behaviour in a university environment.

Information security can be achieved through technology, education of people, raising awareness on the subject, training, or enforcement of policies (D'Arcy, et al., 2009). The participants mentioned that…

…" We have HR and IT monthly information security awareness training, new employees are taken through an induction process where they are informed of the information security policies. They do play a role as from time to time I am reminded on how to handle private and confidential information and maintain information security".

…" *With awareness comes a change in behaviour and with a behaviour change comes a more secure information security environment in the University.*

…" We are sent email communications, it does play a role because now I am more cautious about how I deal with information security".

Information security awareness can assist in shaping individual behaviour and influence how they handle confidential information. The participants' responses above indicate that information security awareness has influenced their information security behaviour. Some of them have indicated that awareness has made them more cautious when dealing with information security.

Information security awareness can influence employees' attitudes and behaviour which can result in improved information security behaviour (Wiley, et al., 2020). The participants said…

… "We have training on how to handle information, passwords, and online learning platforms, meetings are conducted to address any concerns. The initiatives do influence how I handle information and maintain information security, they also help to guard information".

…" We have workshops, talks and email communications on the importance of information security. It does play a role because I know that there are processes to follow in the University, I must protect the information that I have access to, and it helps in maintaining confidentiality".

Information security awareness plays a critical role in preventing incidents such as information leakages, unauthorized discloser of information and information theft. The responses above from the participants indicate that information security awareness has improved their attitudes and behaviour towards information security.

Recommendations from Theme C:

It is recommended that the University should conduct ongoing information security awareness training to ensure that everyone is aware of what the policies, guidelines and laws that govern information security behaviour are.

Information security policies should be written in a manner that is easy to read and understand. They should be simplified and summarised for the University stakeholders.

Information security awareness information resources must be made available and easily accessible to everyone.

It is also recommended that information security awareness training sessions should be made a compulsory requirement.

CHAPTER 6

EVALUATION OF THE RESEARCH AND THE CONTRIBUTIONS

This chapter presents an overview of the research and ascertains whether the research objectives were met, and the primary and secondary research questions were answered through this study. The study sought to understand the role of organisational culture and deterrence in a university information security environment. The chapter also discusses the limitations of the study and makes recommendations for further research.

6.1 Overview of Chapters

The dissertation was structured into seven chapters and what each chapter represents is outlined in the following subsections.

6.1.1 Chapter 1

The first chapter introduced the field being studied by providing a background to the research problem. The study location and study context were explained, research problem, research goals and objectives, followed by research questions (both primary and secondary) were also discussed. Lastly, this chapter touched on the study contributions including its delimitations.

6.1.2 Chapter 2

This chapter gave a detailed survey of scholarship used in the study. This chapter surveyed the scholarship by reviewing existing works available on the different databases about information security in the context of South African universities. The chapter reviews literature and concepts that inform the study such as information security, culture, and deterrence.

6.1.3 Chapter 3

This chapter covered the theoretical underpinnings and its elements on which this study was based on. A conceptual research framework was developed using organisational culture and deterrence theory as a theoretical base to understand the role of organisational culture and deterrence in a university information security environment.

6.1.4 Chapter 4

This chapter discussed the research process undertaken in the study, including the research methodology used. These included the research paradigm, research approach, research strategy, research design, research instrument, data collection methods, data analysis and ethical considerations. The study also justified why the research methodology was used for this research.

6.1.5 Chapter 5

This chapter discussed the interview process, the findings that were analysed and reviewed. It also discusses the data analysis was done in themes.

6.1.6 Chapter 6

This chapter interpreted the findings against existing literature.

6.2 Research Goal and Objectives

The goal of this study was to determine the role of organisational culture and deterrence in a university information security environment.

This goal was achieved through the following objectives:

- To analyse and describe how organisational culture influences information security behaviour in a university environment.

- To analyse and describe how deterrence influences information security behaviour in a university environment.
- To analyse how awareness influences information security behaviour in a university environment.

The following questions were derived to ensure that the above objectives were met:

6.2.1 Primary Research Question

The primary research question of this study is "*How do organisational culture and deterrence play a role in a university information security environment?*"

6.2.2 Secondary Research Questions

- How does organisational culture influence information security behaviour in a university environment?
- How does deterrence influence information security behaviour in a university environment?
- How does awareness influence information security behaviour in a university environment?

6.3 Summary of findings and how the study objectives were met

The following sub-section summaries the findings per each study objectives

6.3.1 Research objective 1: To analyse and describe how organisational culture influences information security behaviour in a university environment.

The following finding from literature and empirical evidence was drawn.

- Participants are fully aware of what information security is and what it entails in their role at the university.
- The understanding of the role of organisational culture in information security does not seem clear for some of the participants.

- Some participants indicated that information security does not seem to be part of the organisational culture.
- Participants believe that organisational culture can influence how they behave with information security.
- Some of the participants were not sure of what could be done to make sure that information security is part of the organisational culture.

6.3.2 Research objective 2: To analyse and describe how deterrence influences information security behaviour in a university environment.

The following findings from literature and empirical evidence were drawn:

- Deterrence factors should be communicated with everyone, participants believe that if they are made aware then they will know what can and cannot be done in a University's information security environment.
- Deterrence does play a role in how some participants handle the University's confidential information.
- Deterrence initiatives should be communicated more often as they provide guidance and direction on one's behaviour.
- There are enough policies to guide or influence behaviour however they are too lengthy for employees to read and familiarize themselves with them.
- Policies need to be summarized and communicated to employees on an ongoing basis.

6.3.3 Research objective 3: To analyse and describe how awareness influence information security behaviour in a university environment.

The following findings from literature and empirical evidence were drawn:

- Awareness of information security is important in influencing how to handle private and confidential information.
- Unawareness of information security policies and guidelines can lead to unauthorized disclosure of information, job losses, and reputational damage.
- Policies must be summarized for employees and be communicated on an ongoing basis.

- Information security information resources must be made available and easily accessible.
- Awareness initiatives must keep up with the times, be relevant and informative.

6.4 Evaluation of the Research Methodology

6.4.1 Appropriateness of the Data Collection Techniques

The findings of the study were derived from qualitative data gotten through semi-structured interviews. This gave empirical data through individual participant's views, opinions, and experiences in a university information security environment.

6.4.2 Why A Case Study Was Relevant for This Research

The case study was considered to be suitable for this study. The case study gave profound empirical data through individual participant's views, opinions, and experiences in a university information security environment.

6.4.3 What Was the Research Theme? Is It Relevant to Information Security?

Information security in a university environment is a complex process and it involves users at different levels and is relevant to information security scholarship. This research sought to understand the role of organisational culture and deterrence in a university information security environment. A case study strategy was appropriate to understand the role of organisational culture and deterrence in a university information security environment.

6.5 The Relevance of the Combination of Organisational Theory and Deterrence Theory

The study is underpinned by organisational culture theory and deterrence theory as research lenses in a university setting to analyse the role of organisational culture and deterrence in an information security environment. The triangulation of the two theories was deemed appropriate given the complexity of the security environment

in the context of a university environment. One theory would not be sufficient as the lens to fully understand how organisational culture and deterrence can influence behaviour in a university information security environment.

6.6 Contributions of the Study

6.6.1 Theoretical Contribution

This study contributed theoretically to how organisational culture influences information security in the context of a university. An additional theoretical contribution was how deterrence influences the information security phenomenon in the sampled university context. The contribution is also in showing how the two theories underpinning the study helps unravel the dynamics manifesting in a university information security environment.

6.6.2 Methodological Contribution

The review of the literature has highlighted some knowledge gap concerning the research methodology. Most studies on organisational culture applied the survey method as their research strategy, following a positivism philosophy stance. The same can be said about the deterrence theory where most studies have been conducted using a survey method and a positivism philosophy. Therefore, the methodological contribution of this study was in using a case study method and an interpretivism philosophy to give an alternative way of understanding organisational culture and deterrence in a university information security environment.

The case study gave a real perspective on organisational culture and deterrence in a university information security environment. The case study method allowed a collection of detailed empirical data and the data is of great depth. The case study allowed contextual and real meanings to be analysed. The interpretivism philosophy brings out more of the lived subjectivity than the generalised objectivity.

6.6.3 Practical Contribution

The practical knowledge gap was in how human interaction and behaviour influence information security, notably in a University environment. This study conceptualised how organisational culture and deterrence influence and manifest in a university information security environment. Thus, the practical contribution of this study is the conceptualization of how organisational culture and deterrence influence and manifest in a university information security environment. That is, the framework is envisaged to help in addressing the practical information security issues and challenges, in a university environment.

6.6.4 Contextual Contribution

Universities offer a unique and different context to that of corporate organisations. Many studies have been conducted to analyse the influence of either organisational culture or deterrence in a particular environment, but a study of this nature has not been conducted in a South African University environment. The observation is that the focus has been on financial institutions information security environment particularly the banking sector over the past few years. This study made a contextual contribution by conducting the study in a university information security environment. By so doing, contributes to the literature of future research in information security.

6.7 The Study Limitations

The first limitation was the unit of analysis of this study. The unit of analysis of the study was the individuals who have lived experience in a university information security environment. The findings from this study, therefore, are only applicable to a typical South African university's information security environment.

The second limitation is the contextual limitation because the study was conducted in South Africa, which is a developing country. It might well be that some of the challenges that universities face in South Africa are unique to developing countries and not universities in the developed world.

The last limitation is that the interviews were mostly done with individuals who reside and work in universities in Gauteng and there is a possibility that other individuals from universities in other provinces or countries might have a different view on how organisational culture and deterrence influence and manifest in a university information security environment.

6.8 Future Research

There is an opportunity to do the same research using an organisation as the unit of analysis, instead of individuals. Research can also be conducted outside the borders of South Africa to investigate the role of organisational culture and deterrence in the university information security environment in those countries. Future research can also be undertaken with the goal of determining ways to improve the information security environment and mitigate information security incidents.

The following future research can be conducted:

- The role of organisational culture and deterrence in shaping behaviour in a university information security environment.
- How organisational culture and deterrence can influence good behaviour in a university information security environment.
- The influence of organisational culture and deterrence in improving behaviour in a university information security environment.
- Further research on university information security is necessary to provide insight on any other factors that may influence information security behaviour.

6.8.1 Conclusion

This study was conducted with the goal of determining the role and influence of organisational culture and deterrence in a university information security environment. It is one of the first attempts to determine the role and influence of organisational culture and deterrence in a university information security environment mediated by information security awareness. It is evident that organisational culture and deterrence do influence behaviour and have a role in how individuals in a university setting handle information. The study has shown that organisational culture

and deterrence are important in influencing individual behaviour and that there is a strong connection between organisational culture and information security culture.

However, there is still a long way to go before individuals realize the importance of information security and protection of information. Organisation culture, deterrence and information security culture can be used in a university information security environment to influence and improve behaviour. It was evident that educating users on the importance of information security may assist in influencing behaviour and reducing risks associated with insider threats. Communicating information security policies and the consequences of non-compliance to promote compliance and behaviour change is important.

Information security in the context of a university is an under-investigated research area and, therefore, further research is necessary to provide insight on any other factors that may influence information security behaviour.

7 REFERENCES

Agnantounkpatin, A. R. & Zhang, L. Y., 2011. *A framework for culture management in sino-African international construction projects.* Shenzhen, China, Institute of Electrical and Electronics Engineers (IEEE).

Ahmady, G. A., Nikooravesh, A. & Mehrpour, M., 2016. *Effect of organizational culture on knowledge management based on Denison model.* Dubai, AUE, Procedia - Social and Behavioral Sciences, p. 387 – 395.

AlHogail, A. & Mirza, A., 2014. Information Security Culture. *A Definition and A Literature Review,* pp. 1-7.

Amini, M., Vakilimofrad, H. & Saberi, M. K., 2020. Human factors affecting information security in libraries. *Human factors affecting information security,* 34(1), pp. 45-67.

Anney, V. N., 2015. Ensuring the Quality of the Findings of Qualitative Research: Looking at Trustworthiness Criteria. *Journal of Emerging Trends in Educational Research and Policy Studies,* 5(2), pp. 272-281.

Bachman, R., Paternoster, R. & Ward, S., 1992. The rationality of sexual offending: Testing a deterrence/rational choice conception of sexual assault. *Law & Society Review ,* 26(2), p. 343−372.

Bekker, G., 1968. Crime and punishment: An economic approach. *Journal of Political Economy,* Volume 76, pp. 169-217.

Bhattacherjee, A., 2012. *Social Science Research: Principles, Methods, and Practices.* South Florida: Textbooks Collection.

Bhattacherjee, A. & Shrivastava, U., 2018. The effects of ICT use and ICT Laws on corruption: A general deterrence theory perspective. *Government Information Quarterly,* Volume 35, pp. 703-712.

Carroll, M. D., 2006. *Information Security: Examining and Managing the insider Threat.* Kennesaw, InfoSecCD '06.

Champlin, K. & Oldham, C., 2017. *Legal Dictionary The Law Dictionary for Everyone.* [Online] Available at: https://legaldictionary.net
[Accessed 21 January 2021].

Cheng, L., Li , W., Zhai, Q. & Smyth, R., 2014. Understanding personal use of the Internet at work: An integrated model of neutralization techniques and general deterrence theory. *Computers in Human Behavior,* 38(1), pp. 220-228.

Cheung, S. O., Wong, P. S. & Wu, A. W., 2011. Towards an organizational culture framework in construction. *International Journal of Project Management,* Volume 29, pp. 33-44.

Committee on National Security Systems, 2001. *Committee on National Security Systems.* [Online] Available at: www.snss.gov
[Accessed 27 March 2020].

Corbin, J. M. & Strauss, A. L., 2008. *Basics of qualitative research.* California: Sage Publications.

Cornish, D. B. & Clarke, R. V., 1986. *The Reasoning Criminal: Rational Choice Perspectives on Offending.* New York: Springer-Verlag.

Creswell, J. W., 2009. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches.* 3rd ed. Thousand Oaks, California: SAGE Publications.

Creswell, J. W., 2014. *Research Design: Qualitative, Quantitative and Mixed Methods Approaches.* 4th ed. California: Sage.

D'Arcy, J. & Herath, T., 2011. A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems,* Volume 20, p. 643–658.

D'Arcy, J., Hovav, A. & Galletta, D., 2009. User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research,* 20(1), p. 79–98.

Da Veiga, A., Astakhova, L. V., Botha, A. & Herselman, M., 2020. Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security,* Volume 92, pp. 1-23.

Da Veiga, A. & Eloff, J. H. P., 2010. A framework and assessment instrument for information security culture. *comp u t e r s & s e c u r i t y,* Volume 29, pp. 196-207.

Da Veiga, A. & Martins, N., 2015. Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Security Review,* Volume 31, pp. 243-256.

De Silva Kanakaratne, M., Bray, J. & Robson , J., 2020. The influence of national culture and industry structure on grocery retail customer loyalty. *Journal of Retailing and Consumer Services,* Volume 54, pp. 102-113.

Dhillon, G., Syed, R. & Pedron, C., 2016. Interpreting information security culture: An organizational transformation case study. *Computers & Security,* Volume 56, pp. 63-69.

DiIulio, J. J., 1959. *Deterrence Theory.* s.l.:s.n.

Dimitrov, K., 2013. EDGAR SCHEIN'S MODEL OF ORGANIZATIONAL CULTURE LEVELS AS A HOLOGRAM. *Икономически изследвания Economic studies,* Volume 4, pp. 1-35.

Du Plessis, Y. & Hoole, C., 2006. An Operational Project Management Culture Framework (Part 1). *SA Journal of Human Resource Management,* 4(1), pp. 36-43.

Futcher, L., Schroder, C. & von Solms, R., 2010. Information security education in South Africa. *Information Management & Computer Security,* 18(5), pp. 366-374.

Gettfredson, M. & Hirschi, T., 1990. *A General Theory of Crime,* Stanford, CA: Stanford University Press.

Gibbs, J. P., 1975. *Crime, Punishment, and Deterrence.* New York: Elsevier.

Guba, E. G. & Lincoln, Y. S., 1994. *Competing Paradigms in Qualitative Research In: N. Denzin & S. Lincon, eds. Handbook of qualitative research.* London New Delhi: Thousand Oaks, CA, Sage.

Hambrick, D., 2007. The field of management's devotion to theory. Too much of a good thing. pp. 1346-1352.

Hatch , M. J., 1993. The Dynamics of Organizational Culture. *Academy of Management Review,* 18(4), pp. 657-693.

Hattangadi, V., 2017. *Dr Vidya Hattangadi.* [Online]
Available at: http://drvidyahattangadi.com
[Accessed 19 October 2020].

Hofstede, G., 1980. *Culture's Consequences: International Differences in Work-Related Values.* Beverly Hills: Sage Publications.

Hofstede, G., Hofstede, G. J. & Minkov, M., 2010. *Cultures and Organizations: Software of the Mind.* 3rd ed. s.l.: McGraw Hill.

House, R., Javidan, M., Hanges, P. & Dorfman, P., 2002. Understanding cultures and implicit leadership theories across the globe: An introduction to project GLOBE. *Journal of World Business,* 37(1), pp. 3-10.

Hu, Q., Xu, Z., Dinev, T. & Ling, H., 2011. Does Deterrence Work in Reducing Information Security Policy Abuse by Employees?. *Communications of the acm,* 54(6), pp. 54-60.

IT Security Team, 2015. *Trends in IT Security,* s.l.: CompTIA.org.

Javadi, M. & Zarea, K., 2016. Understanding thematic analysis and its pitfall. *Journal of Client Care,* 1(1), pp. 34-40.

Johnson, B. & Christensen, L., 2008. *Educational research: Quantitative, qualitative, and mixed approaches.* Thousand Oaks: CA: Sage Publications.

Katz, F. H., 2005. *The Effect of a University Information Security Survey on Instruction Methods in Information Security.* New York, Association for Computing Machinery.

Kendra, K. & Taplin, L. J., 2004. PROJECT SUCCESS: A CULTURAL FRAMEWORK. *Project Management Journal,* 35(1), pp. 30-45.

Kivunja, C. & Kuyini, A. B., 2017. Understanding and Applying Research Paradigms in Educational Contexts. *International Journal of Higher Education,* 6(5), pp. 26-41.

Knein, E., Greven, A., Bendig, D. & Brettel, M., 2019. Culture and cross-functional coopetition: The interplay of organizational and national culture. *Journal of International Management,* 25(4), pp. 1-20.

Kukreja, S., 2019. *Management Study HQ.* [Online]
Available at: https://www.managementstudyhq.com
[Accessed 19 October 2020].

Lewis, M., 1992. *Shame: The Exposed Self,* New York: Macmillan.

Lichtman, M., 2006. *Qualitative research in education: A user's guide.* Thousand Oaks: CA: Sage Publications.

Manzoor, M., 2017. *A review of case study approaches and techniques in studies on big data in online markets.* Shanghai, IEEE.

Maple, C. & Azad, M. A., 2019. Deterrence and Prevention-based Model to Mitigate Information Security Insider Threats in Organisations. *Future Generation Computer Systems,* Volume 97, pp. 1-21.

Maxwell, J. A., 1996. *Qualitative Research Design: An Interactive Approach London, Applied Social Research Methods Series.* 1st ed. s.l.:SAGE Publications Inc.

McCormac, A. et al., 2017. Individual differences and Information Security Awareness. *Computers in Human Behavior,* Volume 69, pp. 151-156.

Miller, R. L. & Brewer, J. D., 2003. *The A-Z of Social Science Research: A Dictionary of Key Social Science Research Concepts.* s.l.:Sage Publications.

Mimecast, 2020. *Mimecast.* [Online]
Available at: https://www.mimecast.com
[Accessed 23 December 2020].

Nasir, A., Arshah, R. A., Ab Hamid, M. R. & Fahmy, S., 2019. An analysis on the dimensions of information security culture concept: A review. *Journal of Information Security and Applications,* Volume 44, pp. 12-22.

Oates, B. J., 2006. *Researching Information Systems and Computing.* 1st ed. London, Thousand Oak, New Delhi: SAGE Publications.

Önday, Ö., 2016. Organization Culture Theory: From Organizational Culture of Schein to Appreciative Inquiry of Cooperrider & Whitney. *Elixir International Journal,* Volume 92, pp. 39002-39008.

Paternoster, R. & Simpson, S., 1996. Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law & Society Review,* 30(3), p. 549−583.

Petersen, A. J., Kushwaha, T. & Kumar, V., 2015. Marketing Communication Strategies and Consumer Financial Decision Making: The Role of National Culture. *J. Mark,* 79(1), pp. 44-63.

Piquero, A. & Tibbetts, S., 1996. Specifying the direct and indirect effects of low self-control and situational factors in offenders' decision making: Toward a more complete model of rational offending. *Justice Quarterly,* 13(3), p. 481−510.

Prince, N. R., Prince, B. J. & Kabst, R., 2020. National culture and incentives: Are incentive practices always good?. *Journal of World Business,* Volume 55.

Protection of Personal Information Act (2013) Government Gazette, No. 37067 .

Qadir, S. & Quadri, S. M., 2016. Information Availability: An Insight into the Most Important Attribute of Information Security. *Journal of Information Security,* Volume 7, pp. 185-194.

Rezgui, Y. & Marks, A., 2008. Information security awareness in higher education: An exploratory study. *Computers & Security,* Volume 27, pp. 241-253.

Richardson, B., 2014. *Culture-Induced Complexity: What Every Project and Program Manager Needs to Know.* [Online]
Available at: https://www.pmi.org
[Accessed 18 October 2020].

Rowley, J., 2002. Using Case Studies in Research. *Management Research News,* 25(1), pp. 16-27.

Ruighaver, A. B., Maynard, S. B. & Chang, S., 2007. Organisational security culture: Extending the end-user perspective. *Computers & Security ,* Volume 26, pp. 56-62.

Safa, N. S. et al., 2019. Deterrence and prevention-based model to mitigate information security insider threats in organisations. *Future Generation Computer Systems,* Volume 97, pp. 587-597.

Salkind, N. J., 2010. *Encyclopedia of research design.* Thousand Oaks: SAGE Publications.

Saunders, M., Lewis, P. & Thornhill, A., 2012. *Research Methods for Business Students.* 6th ed. Harlow: Pearson.

Saunders, M., Lewis, P. & Thornhill, A., 2016. *Research Methods for Business Students.* 7th ed. Harlow: Pearson Education.

Schein, E. H., 1986. *Organizational Culture and Leadership.* 1st ed. San Francisco: Jossey-Bass.

Schein, E. H., 2016. *Organizational Culture and Leadership.* 5th ed. San Francisco: Jossey-Bass.

Shenton, A. K., 2004. Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information,* 22(2), pp. 63-75.

Shrivastava, U. & Bhattacherjee, A., 2015. *ICT as a Corruption Deterrent: A Research Note.* New York, Association for Computing Machinery.

Simpson, B., 2010. Pragmatism, Mead and the Practice Turn. *Organization Studies,* 30(12), pp. 1329-1347.

Solomon, G. & Brown, I., 2020. The influence of organisational culture and information security culture on employee compliance behaviour. *Journal of Enterprise Information Management.*

Szczepaniuk, E. K., Szczepaniuk, H., Rokicki, T. & Klepacki, B., 2020. Information security assessment in public administration. *Computer & Security,* Volume 90, pp. 1-11.

Taherdoost, T., 2016. Sampling Methods in Research Methodology; How to Choose a Sampling Technique for Research. *International Journal of Academic Research in Management (IJARM),* 5(2), pp. 18-27.

Thomson, K. & van Niekerk, J., 2012. Combating information security apathy by encouraging prosocial organisational behaviour. *Information Management & Computer Security,* 20(1), pp. 39-46.

Thomson, K.-L., von Solms, R. & Louw, L., 2006. Cultivating an organizational information security culture. *Computer Fraud & Security,* pp. 7-11.

Tittle, C. R., 1980. *Sanctions and Social Deviance: The Question of Deterrence.* New York: Praeger.

Ugrin, J. C. & Pearson, J. M., 2010. *UNDERSTANDING THE EFFECT OF DETERRENCE MECHANISMS ONCYBERLOAFING: EXPLORING A GENERAL DETERRENCE MODEL WITH A SOCIAL PERSPECTIVE.* St. Louis, International Conference on Information Systems (ICIS) at AIS Electronic Library (AISeL).

Ugrin, J. C. & Pearson, J. M., 2013. The effects of sanctions and stigmas on cyberloafing. *Computers in Human Behavior,* Volume 29, pp. 812-820.

van de Haar, H. & von Solms, R., 1993. A Tool for Information Security Management. *Information Management & Computer Security,* 1(1), pp. 4-10.

Van Niekerk, J. F. & Von Solms, R., 2010. Information security culture: A management perspective. *Comp u t e r s & S e c u r i t y,* 29(1), p. 476–486.

Von Solms, R. & Van Niekerk, J., 2013. From information security to cyber security. *comp u t e r s & s e c u r i t y,* Volume 38, pp. 97-102.

Waisfisz, B., 2015. *An organisational cultural perspective,* Netherlands: ITIM International.

Warrick, D. D., 2017. What leaders need to know about organizational culture. *Business Horizons,* Volume 60, pp. 395-404.

Wheather, C. P. & Cook, P. A., 2000. *Using Statistics to Understand the Environment.* New York: Routledge Publishing.

Whitman, M. E. & Mattord, H. J., 2012. *Principles of Information Security.* 4th ed. Boston: Cengage Learning.

Wiley, A., McCormac, A. & Calic, D., 2020. More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security,* Volume 88, p. 101640.

Williams, K. R. & Hawkins, R., 1986. Perceptual Research on General Deterrence: A Critical Review. *Journal of the Law and Society Association,* 20(4), pp. 545-572.

Winkler, I. & Gomes, A. T., 2017. *Advanced Persistent Security.* s.l.:Elsevier Inc.

Yen, C. L., 2011. A Discussion of Paradigms and Research Methods. *The Journal of WuFeng University,* Volume 19, pp. 357-368.

Yin, R. K., 2011. *Qualitative Research From Start to Finish.* First Edition ed. New York: Guilford Press.

Yin, R. K., 2014. *Case Study Research Design and Methods.* 5th ed. California: Sage.

Zhang, X. J., Li, Z. & Deng, H., 2017. Information security behaviors of smartphone users in China: an empirical analysis. *Information security behaviors,* 35(6), pp. 1178-1190.

8 APPENDIXES

Appendix A: Ethics Clearance

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG

Research Office

HUMAN RESEARCH ETHICS COMMITTEE (NON-MEDICAL)
R14/49 Sibande

CLEARANCE CERTIFICATE	**PROTOCOL NUMBER: H20/08/40**
PROJECT TITLE	An analysis of organizational culture and deterrence in a university information security environment
INVESTIGATOR(S)	Ms X Sibande
SCHOOL/DEPARTMENT	School of Business Sciences/
DATE CONSIDERED	21 August 2020
DECISION OF THE COMMITTEE	Approved Risk Level: Low
EXPIRY DATE	21 September 2023

DATE 22 September 2020 **CHAIRPERSON** _____
(Professor J Knight)

cc: Supervisor : Professor R Kekwaletswe

DECLARATION OF INVESTIGATOR(S)

To be completed in duplicate and **ONE COPY** returned to the Secretary at Room 10004, 10th Floor, Senate House, University. Unreported changes to the application may invalidate the clearance given by the HREC (Non-Medical)

I/We fully understand the conditions under which I am/we are authorized to carry out the abovementioned research and I/we 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. **I agree to completion of a yearly progress report.**

_____ 23 / 09 / 2020
Signature **Date**

PLEASE QUOTE THE PROTOCOL NUMBER ON ALL ENQUIRIES

Appendix A: Ethics Clearance…continued

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG

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

CLEARANCE CERTIFICATE	**PROTOCOL NUMBER: CBUSE/1622**
PROJECT TITLE	An Analysis Of Organizational Culture And Deterrence In A University Information Security Environment.
INVESTIGATOR	Ms Xolile Sibande
SCHOOL/DEPARTMENT OF INVESTIGATOR	School of Business Sciences
DATE CONSIDERED	8 September 2020
DECISION OF THE COMMITTEE	Approved unconditionally
RISK LEVEL	MINIMAL RISK
EXPIRY DATE	31 December 2020

ISSUE DATE OF CERTIFICATE 8 September 2020 **CHAIRPERSON** _____
(Neetu Ramsaroop)

cc: Supervisor: Prof Ray Mompoloki Kekwaletswe

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.

xsibande _____ 06 / 10 / 2020
Signature **Date**

PLEASE QUOTE THE PROTOCOL NUMBER ON ALL ENQUIRIES

Appendix B: Participant Information Letter

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG

Date: 18 October 2020
Study Topic: Organizational culture and deterrence in a university information security environment
Ethics protocol number: H20/08/40

Good day,

My name is Xolile Sibande and I am a Master's student in Information Systems at the University of the Witwatersrand, Johannesburg. As part of my studies, I have to undertake a research project, and I am investigating organizational culture and deterrence in a university information security environment under the supervision of Prof Ray Kekwaletswe. This research project aims to find out the role of organizational culture and deterrence in a university information security environment.

As part of this project, I would like to invite you to participate in the study through a semi-structured interview. The interview or conversation will be done as an online meeting and it is anticipated to take around 45 minutes. With your permission, the interview will be recorded digitally to allow the conversation to flow.

There will be no personal costs to you if you participate in this project, you will not receive any direct benefits for your participation but there are no disadvantages or penalties if you do not choose to participate or if you withdraw from the study. You may withdraw at any time or not answer any question if you do not want to. The interview will be completely confidential and anonymous as I will not be asking for your name or any personally identifiable information, and the information you give to me will be held securely and not disclosed to anyone else. I will be using a pseudonym (false name) to represent your participation in my final research report.

If you have any questions during or afterward about this research, feel free to contact me on the details listed below. This study will be written up as a research report which will be available online through the university library website. If you wish to receive a summary of the report, I will be happy to send it to you. The data collected from this research project will be stored in a password-protected computer and will be kept for 2 years. If you have any concerns or complaints regarding the ethical procedures of this study, you are welcome to contact the University Human Research Ethics Committee (Non-Medical), telephone +27(0) 11 717 1408, email hrecnon-medical@wits.ac.za

Yours sincerely,
Xolile

Researcher:
Xolile Sibande, [redacted]

Appendix C: Participation Consent Form

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG

An analysis of organizational culture and deterrence in a university information security environment

Xolile Sibande (2057505)

I, [redacted], agree to participate in this research project. The research has been explained to me and I understand what my participation will involve. I agree with the following:

(Please circle the relevant options below).

I agree that my participation will remain anonymous	YES x	NO
I agree that the researcher may use anonymous quotes in her research report	YES x	NO
I agree that the interview may be audio recorded	YES x	NO
I agree that the information I provide may be used anonymously after this project has ended, for academic purposes by other researchers, subject to their own ethics clearance being obtained.	YES x	NO

..... (signature)
[redacted] name of participant)
21 October 2020 (date)

..... (signature)
Xolile Sibande ..... (name of the person seeking consent)
18/10/2020 ..... (date)

Appendix D: Interview Guide

RESEARCH INSTRUMENT/INTERVIEW GUIDE

ORGANISATIONAL CULTURE AND DETERRENCE IN A UNIVERSITY INFORMATION SECURITY ENVIRONMENT

Purpose: The purpose of this study is to describe how organisational culture and deterrence influence behaviour in a university information security environment. The main aim of this study is to determine the role of organisational culture and deterrence in a university information security environment and to achieve the research purpose.

A. Introduction section

1. Please discuss your role and familiarity with information security in the context of a university's environment.
2. Please share your understanding of information security.

B. Objective 1: Analyse and describe how organisational culture influences information security behaviour in a university environment.

1. Describe what organisational culture means to you.
2. Is information security part of the organisational culture in the university?
3. In your opinion, what could be done to make sure that information security is part of the organisational culture in the university?
4. If organisational culture influenced your behaviour towards information security, describe how your behaviour has been influenced?

C. Objective 2: Analyse and describe how deterrence influences information security behaviour in a university environment.

1. Describe your understanding of deterrence.
2. How can deterrence influence behaviour in an organisation?
3. What is your view on how deterrence should be dealt with in a university environment?
4. In your opinion, would you say that deterrence can improve information security or not?
5. Is deterrence communicated in the university? What could the implications thereof be?
6. Relating to the handling of information, kindly share your experiences on how deterrence can influence one's behaviour.

Appendix D: Interview Guide…continued

7. Do the university policies and regulation deter certain behaviours?
8. Based on your experience, how should employees be made aware of **policies** that govern information security, current laws, and regulations in the university

D. Objective 3: Analyse how awareness can improve information security behaviour in a university environment.

1. How are information security initiatives managed in the university and would you say that it plays a role in how you handle information?
2. In your opinion, what would you say are the reasons information security awareness is done?
3. Please share with me an experience of what unawareness of information security has led to.
4. What do you think could be done to improve such (previous question)?
5. In an event where a student or fellow worker is unaware of a particular aspect of information security, what do you do?
6. In your opinion how could the information security environment be improved in university if it needs to be?