University of Fort Hare

Together in Excellence

A Bring Your Own Device Information Security Behavioural Model

Alfred Musarurwa

2017

A Bring Your Own Device Information Security Behavioural Model

By

Alfred Musarurwa

Research Thesis

Submitted in fulfilment of the requirements for the degree

Doctor of Philosophy

In

Information Systems

In the

Faculty of Management and Commerce

Of the

University of Fort Hare

Supervisor: Professor Stephen Flowerday

Co-Supervisor: Dr Liezel Cilliers

2017

Abstract

The Bring Your Own Device (BYOD) phenomenon has become prevalent in the modern-day workplace, including the banking industry. Employees who own devices have become the unintended administrators of the organisation's information as their mobile devices often carry information belonging to the organisation. The unintended administrator is not necessarily schooled or aware of the information security risks and challenges that are associated with the BYOD. This inadvertently shifts the management of organisational information security from the information technology (IT) administrator to the unintended administrator. This shift leaves the organisation at risk of information security breaches that can permeate the organisation, which result from the behaviour that the unintended administrator displays when operating the mobile device.

This study introduces the BYOD Information Security Behavioural (BISB) model. The model constructs are a combination of individual and organisational traits of the unintended administrator. The purpose of this study is to mitigate the risks posed by the unintended administrator in organisations through the implementation this model. The risk that the unintended administrator poses in relation to the BYOD phenomenon results in chief information officers (CIOs) being unable to totally control these mobile devices. Traditional endpoint information security management tools and methods can no longer secure devices in the BYOD the way they can in the traditional network where they are confined to the organisation's IT administrator. This results in the organisation's information security becoming the responsibility of the unintended administrator. This study was conducted in the banking sector in Zimbabwe. It is noteworthy that the BYOD phenomenon has become prevalent in the banking sector among other organisational sectors like education, health or even government departments. Information security is also an important component of the banks as such and a choice was made to conduct the study in the banking industry.

The design science research paradigm was followed in this study and included a survey of 270 bank employees in Zimbabwe, which received 170 complete responses. A literature review on both employee behaviour and organisational culture was conducted, followed by a case study of a commercial bank in Zimbabwe. The literature review culminated in traits that were then classified as individual traits and organisational traits.

Six constructs –, knowledge, attitude, habit, environment, governance and training – were identified from the literature and combined to form the BYOD information security behavioural (BISB) model. Statistical calculations were conducted on the survey results which informed the reliability, validity and rigour of the model constructs. An expert review including industry experts was conducted to evaluate the BISB model.

This study concludes by recommending that organisations in Zimbabwe should make use of the BISB model to mitigate the information security risks that are posed by the unintended administrator. While there are technical solutions for managing the information security risks that come with the BYOD, this study points out that without harnessing the individual and organisational traits that make up the BYOD information security behavioural model for the unintended administrator, technical solutions alone will not be effective.

Declaration

I, Alfred Musarurwa, hereby declare that:

- ✓ The work in this dissertation is my own work.
- ✓ All sources used or referred to have been documented and recognised.
- ✓ This dissertation has not previously been submitted in full or partial fulfilment of the requirements for an equivalent or higher qualification.
- ✓ This thesis received ethical approval (**Ref: FLO061SMUS01**) from the University of Fort Hare's Research Ethics Committee (UREC).

____

Alfred Musarurwa

____

Date

Publications

Conference:

Musarurwa, A., Flowerday S.V. and Cilliers L. (2017) Individual traits that determine the Bring Your Own Device information security culture: A case study of the banking sector in Zimbabwe: The 16th Annual Security Conference Las Vegas Nevada USA.

Musarurwa, A., Flowerday S.V. and Cilliers L. (2017). An Achilles heel for Chief Information Officers: The BYOD unintended administrator. The 17th Annual Security Conference Las Vegas Nevada USA.

(Under review)

Journals:

Musarurwa, A., Flowerday S.V. and Cilliers L. (2017. Securing the Bring Your Own Device Unintended Administrator. Elsevier Computers and Security (Under review)

Musarurwa, A., Flowerday S.V. and Cilliers L. (2017). From Information Technology Administrator to the BYOD Unintended Administrator Emerald Insight Information and Computer Security (Under review)

Acknowledgements

First and foremost I would to thank the almighty God for affording me the opportunity to meet the wonderful supervisors I worked with throughout the journey. I would like to thank Professor Stephen Flowerday and Dr Liezel Cilliers for being my thesis advisors. Their tutelage and direction were instrumental in guiding me during the journey. I acknowledge the assistance of Farai Marambire and Munyaradzi Mafi with data collection. Thank you for putting up with the late nights and sometimes near impossible requests. This project would not have been such a success without your immeasurable help. I would also like to thank the rest of my IT department at MBCA who helped me out on numerous occasions by holding fort when I was away for my studies. I would like to thank my colleagues who I frequently left in charge of my duties at MBCA as I worked on this thesis, and who gave me peace of mind that my name was in good hands. I would also like to thank all my colleagues at MBCA bank who participated in the survey and were patient with me as I sent reminder after reminder. In addition, I would like to thank fellow employees, who bore with me through my extensive travel and hectic schedule to allow me to achieve this success. Finally, and most importantly, I would like to thank my wife Mirriam and my boys Rowland and Rowan, who were very understanding and supportive throughout the entire project and allowed me to get away with the late nights and hours away from home.

Table of Contents

List of Figures

List of Tables

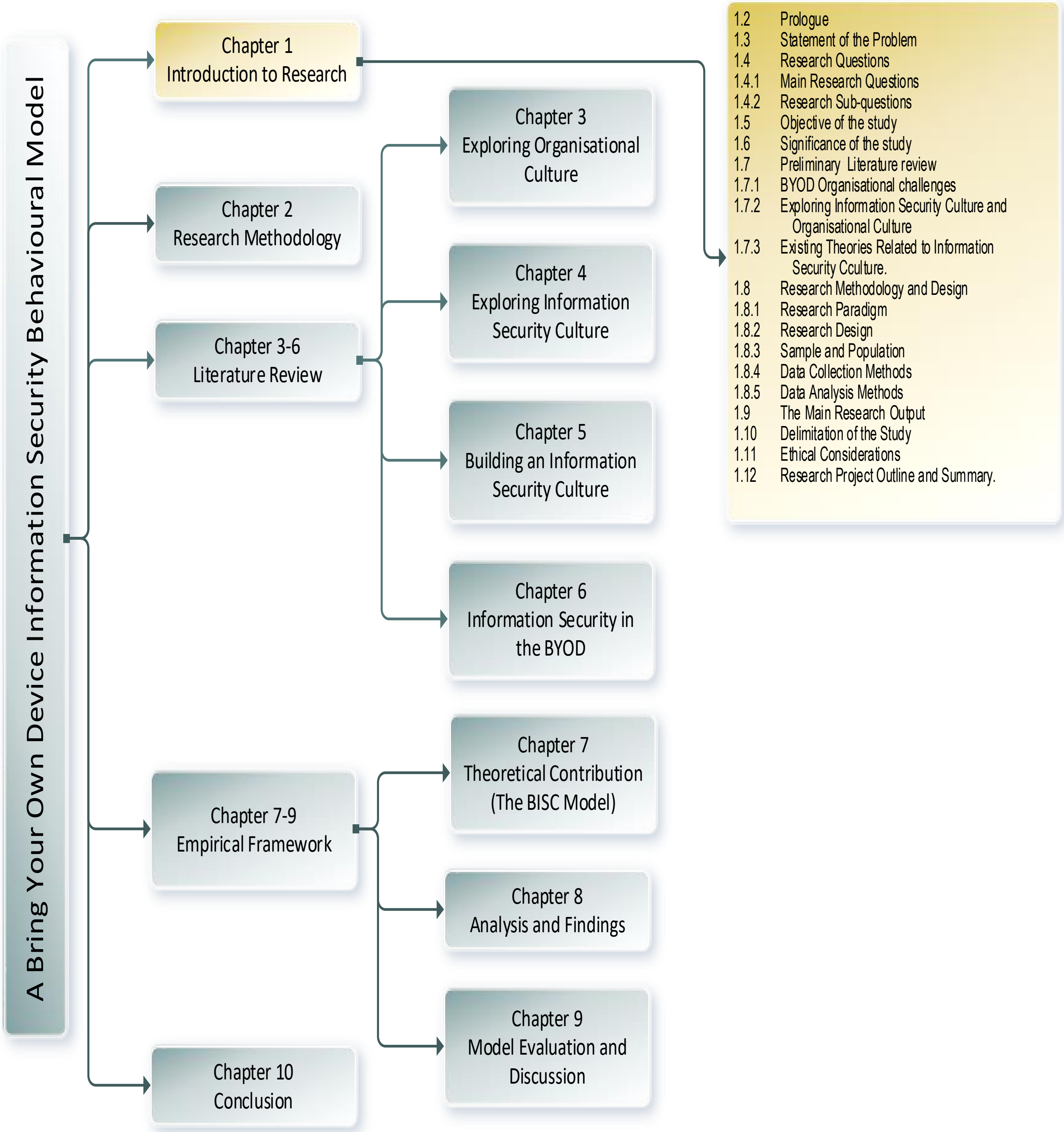
Abbreviations

ADSC	African Digital Security Culture
BISB	BYOD Information Security Behavioural
BYOA	Bring Your Own Apps
BYOD	Bring Your Own Device
BYOS	Bring Your Own Software
BYOT	Bring Your Own Technology
CAGR	Compound Annual Growth Rate
CCLM	Conscious Competence Learning Model
CIO	Chief Information Officer
CISF	Comprehensive Information Security Framework
COBO	Company Owned Business Only
COPE	Corporate Owned Personally Enabled
CYOD	Choose Your Own Device
CRM	Customer Relationship Monitoring
CVF	Competing Values Framework
EXCO	Executive Committee
GST	General Systems Theory
HYOD	Here’s Your Own Device
ICT	Information Communication Technology
IoT	Internet of Things

IS	Information Security
ISACA	Information Systems Audit and Control Association
ISC	Information Security Culture
ISO/IEC	International Organisation for Standardisation/International Electrotechnical Commission
IT	Information Technology
KCB	Kenya Commercial Bank
MISSTEV	Model for Information Security Shared Tacit Espoused Values
MKC	Modes of Knowledge Creation
OC	Organisational Culture
OCT	Organisational Culture Theory
OECD	Organisation for Economic Co-operation and Development
PDCA	Plan, Do, Check, Act-model
SPSS	Statistical Package for Social Scientists
TPB	Theory of Planned Behaviour
TRA	Theory of Reasoned Action
UREC	University Research Ethics Committee
UWYT	Use What You are Told
VPN	Virtual Private Networks

Chapter 1: Introduction to Research

The B.Y.O.D. Genie Is Out Of the Bottle – "Devil or Angel" --Singh & Phil, 2012



A Bring Your Own Device Information Security Behavioural Model
Chapter 1
Introduction to Research
Chapter 2
Research Methodology
Chapter 3-6
Literature Review
Chapter 3
Exploring Organisational Culture
Chapter 4
Exploring Information Security Culture
Chapter 5
Building an Information Security Culture
Chapter 6
Information Security in the BYOD
Chapter 7-9
Empirical Framework
Chapter 7
Theoretical Contribution (The BISC Model)
Chapter 8
Analysis and Findings
Chapter 9
Model Evaluation and Discussion
Chapter 10
Conclusion

1.2 Prologue
1.3 Statement of the Problem
1.4 Research Questions
1.4.1 Main Research Questions
1.4.2 Research Sub-questions
1.5 Objective of the study
1.6 Significance of the study
1.7 Preliminary Literature review
1.7.1 BYOD Organisational challenges
1.7.2 Exploring Information Security Culture and Organisational Culture
1.7.3 Existing Theories Related to Information Security Cculture.
1.8 Research Methodology and Design
1.8.1 Research Paradigm
1.8.2 Research Design
1.8.3 Sample and Population
1.8.4 Data Collection Methods
1.8.5 Data Analysis Methods
1.9 The Main Research Output
1.10 Delimitation of the Study
1.11 Ethical Considerations
1.12 Research Project Outline and Summary.

1.1 Prologue

The advent of mobile computing has reshaped the way companies conduct their day-to-day business as it enables flexibility in accessing work from any location where connectivity is available. Technology experts have forecast that mobile Internet penetration across the African continent will grow exponentially between 2014 and 2020, and will result in almost everyone being connected by the end of the decade (Lange & Lancaster, 2014). Traditionally, organisations supplied their employees with all information technology (IT) hardware and software, which was managed and controlled by policies from the organisation's IT framework. This policy model is referred to as "*Use what you are told (UWYT)"* (Brodin, 2016a, p. 55). In the UWYT model, information security (IS), which refers to the standards for guarding data and information against illegal access, is addressed by the organisational information and communication technology (ICT) policy (Chiu & Churchill, 2017).

Bring Your Own Device (BYOD) has permeated the information and communication management in organisations. It has emerged as a phenomenon or new business policy by management which gives employees the privilege of using their own individual mobile devices to carry out work-related tasks (Alagbe, 2016). This can also be viewed as Bring Your Own Technology (BYOT) (Ackerman & Krupp, 2012). The proliferation of mobile devices that have the ability to connect to the Internet has given impetus to the growth of this BYOD phenomenon in organisations. BYOD is mainly driven by employees' preference for different types of mobile device. Considering the different preferences that employees may have, they end up acquiring devices of their choice and consequently use them more than the company supplied devices, which may not necessarily be of their choice (Garba, Armarego, Murray, & Kenworthy, 2015; Ghosh, Gajar, & Rai, 2013).

The information security management of an organisation cannot be separated from the implementation of the BYOD phenomenon, as BYOD inadvertently affects the information security management processes. Alhogail (2015) argues that information security is a people issue as well as a technology issue. While providing clear advantages like reducing the organisational technology and software acquisition budget, BYOD opens the organisation to serious challenges with respect to securing data that is stored or displayed on the personal device using BYOD (Gessner, Girao, Karame, & Li, 2013). These devices are portable and they may be lost or misplaced, leading to private information of the organisation going public.

The BYOD phenomenon gives rise to an "unintended administrator" who has total control of the device but he/she does not necessarily understand the advantages and disadvantages of information security management. With the increase of Internet speed, as well as the spread in wireless Internet connections through such technologies like 3G, 4G, LTE, Wi-Fi and many others, mobile devices are almost always remotely connected to the organisational networks. This in turn exposes the organisation's networks to potential malicious attacks from hackers through compromised network access points. The evolution of the mobile applications and services demands some attention from corporate organisations if their operations are to maintain the integrity that is expected of them (Disterer & Kleiner, 2013). These unintended administrators have administrative access rights to their devices, giving them the access to download applications of their choice, some of which may include malicious software. Martins and Eloff (2002) state that an organisation's information security culture is developed from its employees' daily habits, characteristics and behaviour, as well as their uptake of the implemented policies and models. Applying this thinking to the BYOD phenomenon, the organisation's overall information security becomes as strong as its weakest link, which in this case is the unintended administrator (Chen, Li, Hoang, & Lou, 2013). There is a need for conscious efforts to develop positive attitudes and behaviours, and create a culture for securing the BYOD unintended administrator. Establishing an information security culture can only be effective if technology users appreciate, understand and implement the necessary precautions (Alhogail, 2015).

The success of any security system is closely related to the behaviour and ethics of the target audience and the organisational culture. Thus, considering that one of the greatest strengths of any model is also the greatest vulnerability, this research project will investigate the employee behavioural patterns when using mobile technology and the information management culture. This will then culminate in identifying the traits that will be the basis for the formulation of the BYOD information security behavioural model. The commercial banking sector is used to conduct this study because of the high controls and sensitive data associated with it, as well as the negative consequences that the bank faces when data is compromised.

This chapter begins by defining the statement of the problem followed by an overview of the research questions that guided this research study. The objective for the study will be examined, followed by an outline of the significance of this study. A brief overview of how the BYOD unintended administrator can be secured is conducted, covering pertinent components such as the BYOD challenges faced by organisations, exploring information security culture, and an overview of existing theories on information security culture. The research methodology overview will explore the research paradigm adopted, followed by the research design, sample population selected for the survey, and analysis methods employed on the selected data. The chapter will briefly introduce the BYOD Information Security Behavioural (BISB) model which is the main research output. The chapter concludes with a delimitation of the study and the ethical considerations made when conducting the study process. An outline of the research project will also be given to illustrate the way the study was conducted.

1.2 Statement of the Problem

The focus of this research is on mitigating the risks posed by the unintended administrator created by the BYOD phenomenon in the Zimbabwean commercial banking sector. The unintended administrator poses a major information security risk for organisations if not properly implemented. This problem, according to Von Solms and Van Niekerk (2013), also results in the following information security risks:

- ✓ Chief information officers (CIOs) and security experts have limited control of the mobile device that is being used under BYOD since each user has administrative rights on their own device.
- ✓ Traditional systems such as antivirus software and network monitoring tools become limited to devices within the organisational network.
- ✓ The security of the devices can no longer be the full responsibility of the organisation.

Chen et al. (2013) pointed out that “there is a need for a combination of people, processes and technology in the formulation of an Information Security solution” (p. 19). It is imperative to examine and address the security challenges that come as a result of the unintended administrator. A view on the common traits towards information security will lead to the creation of a behaviour of information security. Eschelbeck and Schwartzberg (2012) remark that “the BYOD phenomenon in the workplace is rapidly becoming a rule rather than an exception, replacing the traditional Use What You are Told policy (UWYT)” (p.2). The problem is the inherent information security weakness emanating from the unintended administrator’s level of control. This research study takes the form of a case study in Zimbabwe in which the commercial banking sector was be used to set the stage for this discussion.

1.3 Research Questions

In the case of the BYOD phenomenon, security can be effective if the unintended administrator appreciates and understands the necessary precautions. The research questions will play a vital role in providing an understanding of the development of the BISB model. In this study, the research questions are divided into two sections: the main research question and the research sub-questions as appear below.

1.3.1 Main Research Question

How can an organisation build an information security culture to mitigate the risks posed by the BYOD unintended administrator?

An information security aware culture is built from the employees' information security behaviour. Ali and Brooks (2009) point out that the study of culture is rooted in anthropology, sociology and psychology. The concept of an information security culture, which emerged in the late 1990s, refers to the patterns and behaviour in organisations when protecting information of all kinds (Connolly & Lang, 2012). The employees' interaction with the information assets and their security behaviour therefore forms the basis of the information security culture in regard to BYOD. The following four sub-questions support this main research question.

1.3.2 Research Sub-questions

The answers to the following four research sub-questions will together address the main research question.

i. What is required for organisations to build an information security culture?

An information security culture fits into the organisational culture as a sub culture. Organisational culture is defined as the way things are done in any given organisation (Cowling, 2016). In the same context, information security for the organisation would mean the way security is managed in the particular organisation. This research sub-question gives impetus for the identification of key traits in building and fostering a culture for the organisation, which will be mainly around BYOD security. A security aware organisational culture will be considered in the creation of the information security culture (Da Veiga & Eloff, 2010).

ii. How does the BYOD unintended administrator affect the organisational information security culture?

This research sub-question investigates the positive and negative effects of BYOD on the organisational information security culture. It also sets the basis for the requirements for building an information security culture around BYOD. From the problem statement it was learnt that the unintended administrator had too much control over the devices they use and this does not necessarily translate to total security to the standard of the organisation whose data they are accessing. In Chapter 5, the organisational information security culture will be explored in detail, highlighting the effect exerted by the BYOD.

iii. **How can BYOD information security behaviour mitigate the risks associated with the unintended administrator?**

BYOD is mainly driven by employee preferences. The information security culture in an organisation will thus contribute to the shaping of these preferences and behaviours. Da Veiga and Eloff (2010) suggest that the interaction that the employees have with the information assets portrays a behaviour, which forms the basis of an information security culture. Answering this research question will assist in establishing the organisational traits required in order to build an organisational information security culture for BYOD. This will in turn guide the creation of an information security behavioural model for the BYOD unintended administrator, as outlined in Chapter 7.

iv. **What roles do employees and the organisation play in building an information security culture for BYOD?**

Since organisations are composed of employees, it is important to understand their role in building an organisational information security culture. The environmental factors in an organisation play an important role in the building of an information security culture around BYOD. Training programmes and upskilling of the employees are some of the ways through which the organisation can influence the creation of an information security culture around BYOD. Chapters 3 to 6 discuss the significance of the employee contribution to the building of an information security culture in organisations. The artefact discussed in Chapter 7 is a culmination of various traits including individual employee traits for building an organisational information security culture. From the problem statement identified, the above research questions will answer the research objective in the next section.

1.4 Objective of the Study

The primary objective of this research study is to develop a model for commercial banks to build an information security culture for the BYOD unintended administrator. This model will deal with the issues of employee habits, behaviour, beliefs, attitudes and knowledge, which influence a culture with regard to information security. It will also focus on the cognitive memes of information security and use them as the basis for formulating a culture for information security around BYOD. The research study will be conducted in the banking sector where information security is a key performance indicator as well as a key result area. The model resulting from this research study builds from individual and organisational traits for fostering an information security culture. The organisational traits of governance, environment and the awareness training given to the employees influence the information security culture of the bank. The next section addresses the reason why this study is significant.

1.5 Significance of the Study

The study will introduce a BISB model for an organisation. For the purposes of this study, the discussion is based on the commercial banking sector. Banks are generally characterised by very tight selection rules when it comes to information products that could improve their headline earnings and make their working conditions manageable. King (2012) argues, "banking is no longer about somewhere you go to for a transaction, but it's more about something you can do from anywhere" (p. 3).

BYOD information security behaviour is a key imperative which needs to be positioned properly so that banks can benefit from this technological phenomenon. An important countermeasure in BYOD is to consider several controls that are not necessarily technical. Several information security model standards such as ISO/IEC 27002 can be used to manage information security around BYOD. However, some of these standards address such human components as training and awareness without addressing how to influence behaviours (Da Veiga & Eloff, 2010). This model addresses the unintended administrator's behaviour which will influence the formative aspects of the information security culture. If the model is adopted, the unintended administrator will behave more securely and thus add to the security culture of the bank. This will increase the bank's overall security and align with its low risk appetite.

The study will contribute to the body of knowledge on information security and BYOD. From the perspective of technological innovation, this study will provide valuable insights on the information security culture with regard to the BYOD phenomenon. To qualify the importance of this, Munteanu and Fotache (2015) posit that information security is a function of technology, whilst risk perception is a human characteristic. These two components are addressed in this study.

This study also enables organisations to create training and upskilling for their employees so as to maximise the benefits of the BYOD phenomenon. A 2015 report on the implications of this perspective on information security by ISACA and RSA pointed out that organisations that offer training do not seem to be reaping benefits from a corresponding reduction in attacks, as the nature of the attacks remains human dependent. Such training programmes leave these organisations in the same position as organisations without training programmes. Revisiting the organisational and employee behavioural patterns may give a practical solution for BYOD (Lanaj, Johnson, & Barnes, 2014).

1.6 Preliminary Literature Review

The BYOD phenomenon emerged from the consumerisation of ICT, which is characterised by the consumerisation of devices, solutions and services, ultimately resulting in a shift in the way ICT is managed. It brings such benefits as shortening the delivery cycle of business operations and reducing the overall ICT spend on devices (Thomson, 2012). Whilst Ackerman and Krupp (2012) view BYOD and bring your own technology (BYOT) as the same phenomenon, Woodill (2012) suggests that BYOD and BYOT are two separate phenomena. He argues that in as much as BYOD involves employees carrying their own devices to work, the type of software applications to be loaded is supplied by the organisation’s ICT. He views BYOT as an extreme form of BYOD, where the employee supplies all the computing service and devices to the organisation.

1.6.1 BYOD Organisational Challenges

Markus and Robey (1988) warn that the major security challenge to any organisation’s information security is from within. This involves careless or malicious employees who intentionally violate and compromise the organisation’s information security policies. Malware attacks may occur when the unintended administrator installs malicious applications. Therefore, the greatest strengths in BYOD, which include working from anywhere as well as an overall reduction in the ICT budget, are also the greatest vulnerabilities when it comes to the security risks that the organisation is exposes to (Chen et al., 2013). If the device containing organisational data is stolen or misplaced, this may result in information being exposed to the wrong audience. The fact that these devices operate outside the organisation’s network means that network security management systems will not be useful in managing them. For instance, sensitive organisational data like financial details, minutes, emails, or details of confidential human resources can be carried on a device that also has personal files such as photographs, social networking profiles, or even games (Shumate & Ketel, 2014).

1.6.2 Exploring Information Security Culture and Organisational Culture

Several researchers and academics share the tenet that while technology and policy are key pillars for organisational security, they require culture as another fundamental factor. Robbins, Judge, and Hasham (2009) suggests that organisational culture is the personality of the organisation, whilst Lundy and Cowling (1996) loosely define organisational culture as a way of doing things in any particular organisation. The organisational culture should be the basis for cultivating an information security culture to ensure that adequate and relevant checks and balances are identified and implemented in a successful manner (Da Veiga & Eloff, 2010). An information security culture is a sub-culture of organisational culture and, as such, it is important to understand the aspect of organisational culture in relation to information security culture (Da Veiga & Eloff, 2007).

1.6.3 Existing Theories Related to Information Security Culture

A number of theories, such as the theory of planned behaviour (TPB), Schein's organisational culture theory (OCT), which identifies three levels of organisational culture, and general systems theory (GST) have been postulated to explain information security culture. The creation of the BYOD model will revolve around people's behaviour and attitude, as well as their relation to the systems they are exposed to. The theories stated above will assist is explaining certain behaviours and phenomenon, as well as the design aspects of BYOD system, which influence its uptake and eventually the building of BYOD information security behavioural patterns. Table 1 below explains the three main theories used. Additional theories may be cited where relevant to explain certain viewpoints.

Table 1. Existing research theories and their application to this study

Theory	Main Findings of the Theory	Application to this Study
Theory of planned behaviour (TPB)	Ajzen (1988) proposed a model that can measure the way human actions are guided and at the same time predict the occurrence of a particular behaviour, as long as that behaviour is deliberate. This theory is based on the realisation that behaviour can be deliberate and intentional.	In building a culture, it is important to understand people's behaviours and intentions. The TPB provides insight on understanding the occurrence of predictable behaviours, which will be useful in identifying some phenomena in the organisational information security culture.

General systems theory (GST)	This theory states that the elements of a system are interdependent and contribute to the functionality of the whole system (Von Bertalanffy, 1950).	In this research, the GST will provide insight on how BYOD systems and culture can be interlinked. This will form the basis of the relationships between the critical success factors in building an information security culture.
Organisational culture theory (OCT)	The OCT was proposed by Schein (1988). It adopts a functionalist view and describes culture as a pattern of basic assumptions that can be classified into three levels: ✓ Level one addresses artefacts – these are the aspects that can be seen, heard and felt about an organisational culture. ✓ Level two addresses espoused values –this addresses the reasons that an organisational member can give as shaping the belief system. ✓ Level three addresses shared tacit assumptions – these are shaped as a result of certain successful strategies that have worked before.	The OCT assists in building our understanding of the organisational culture. Considering that the aim of this study is to foster an information security model, the theory provided the rigour in the model constructs. It will also assist in validating the assumptions to be made in the model.

1.7 Research Methodology and Design

Every research project is driven from some fundamental norms about what leads to useable research and which research methods lead to that valid research (Myers & Newman, 2007). Burns (2000) view methodology as a structured way of doing things, which involves structures, actions and systems, to be able to run a research process. It is important to understand what these assumptions are in order to conduct research. This section outlines the plan used to explore and construct the proposed solution to the research problem defined. The section will be broken down into four subsections which include the research paradigm, research design, data collection methods, and data analysis methods.

1.7.1 Research Paradigm

The selection of the right research paradigm is the foundation for ensuring that the research methodology satisfies the perspective behind the assumptions of the paradigm. This suggests that a research paradigm must guide every research study. Hevner, March, Park, and Ram (2004) remark that the two basic paradigms for researching information systems are behavioural research, which focuses on what is true, and design research, which deals with what is effective. Hevner et al. (2004) further highlight the design science paradigm into which they characterise much of the research in information systems. Design science seeks to expand the limitations of human and organisational abilities by creating innovative artefacts (Hevner et al., 2004). This study will employ the design science paradigm as it seeks to create an information security culture for the BYOD based on employee participation. Chapter 2 contains a detailed description of the research method employed for this study. The next section will discuss the research design.

1.7.2 Research Design

This research project will adopt design science guidelines as proposed by Hevner et al. (2004). This proposal is supported by Peffers, Tuunanen, Rothenberger, and Chatterjee (2007), who state that design science research involves "a rigorous process to design artefacts to solve observed problems, make research contributions, evaluate the designs, and communicate the results to appropriate audiences" (p. 49). All of the logical assumptions were verified using theories from the social sciences. Existing literature studies that have been proven relevant and successful in previous research, were used to create questionnaires for this study. In order to assess and validate the developed model, expert reviews were conducted. In addition, Cronbach's alpha tests were used to measure the internal consistency of the components. To ensure that valid conclusions have been reached, the seven design science guidelines were followed and observed closely in no particular order of significance. The following section addresses the sample population as the next research methodology step.

1.7.3 Sample and Population

The sample population for this study was of employees from a selected bank. Hackshaw (2009) developed the formula below to determine the size of the sample with a certain level of precision at a 95% level of confidence.

n = P (1 -P) (Z / E) 2

Where n = sample size:

- ✓ P = population size
- ✓ Z = confidence interval at 95%
- ✓ E = error margin

In this study, the target was the population for the whole bank. A total of 270 bank employees received the online questionnaire loaded in Survey Monkey. Of the population of 270, 205 employees participated, which represents a response rate of 76%. Of the 205 responses received, it was found that only 170 respondents had completed the questionnaire, resulting in a response rate of 82% (refer Appendix 2: Questionnaire). Oates (2006) states that a response rate of 30% or higher is acceptable in a research project. Considering that the response rate was well above 30%, it was deemed acceptable as it also fits within the proposed thresholds of Hackshaw's formula. The next section describes the data collection method followed.

1.7.4 Data Collection Methods

A mixed method design was employed to give a multidimensional and complete understanding of the issues under study. This study employed both qualitative and quantitative data collection methods, including the use of questionnaires and the researcher's observation notes. Myers and Newman (2007) argue that there are three types of quantitative research technique: observation, experimentation, and survey. This study applied an observation technique in identifying the constructs followed by a survey conducted on a commercial bank in Zimbabwe to bring about the scientific rigour for the components of the study. To qualify this Frechtling (2002) states that there is trade-off between breadth and depth, and between generalisability and targeting specifics, when employing quantitative and qualitative techniques.

The primary data collection method for this study was the use of a questionnaires, observations and interviews with departmental heads. The literature review constituted the secondary data collection.

The questionnaires was sent out to all of the bank's employees through an email. The employees currently make use of BYOD for their electronic mail communication and other services, depending on their job profiles. The data gleaned from the questionnaires were then discussed with the heads of departments in an interview.

1.7.5 Data Analysis Methods

Mixed methods research was used for this study since data collected from the questionnaires was both qualitative and quantitative. The Statistical Package for Social Scientists (SPSS) Version 23 was used to make relevant statistical conclusions for the quantitative data. Subsequently, multivariate statistical measures of factor analysis were used to describe the variability among the correlated variables. Other descriptive statistical computations were used to generate applicable measures such as correlation, regression, mean, median and standard deviation, where applicable. The reliability of the questions was measured by means of the Cronbach's alpha test. The validity of constructs, either internally or externally, was assured through the use of multiple sources of information. Combining various studies increases the relevance of a study through a trade-off in the strengths and weakness in either study (Pelino, Kane, Koetzle, & Voce, 2014).

1.8 The main research output

From the literature review conducted, individual traits of attitude, knowledge and habit were identified and combined with organisational traits of environment, governance and training to come up with the model.

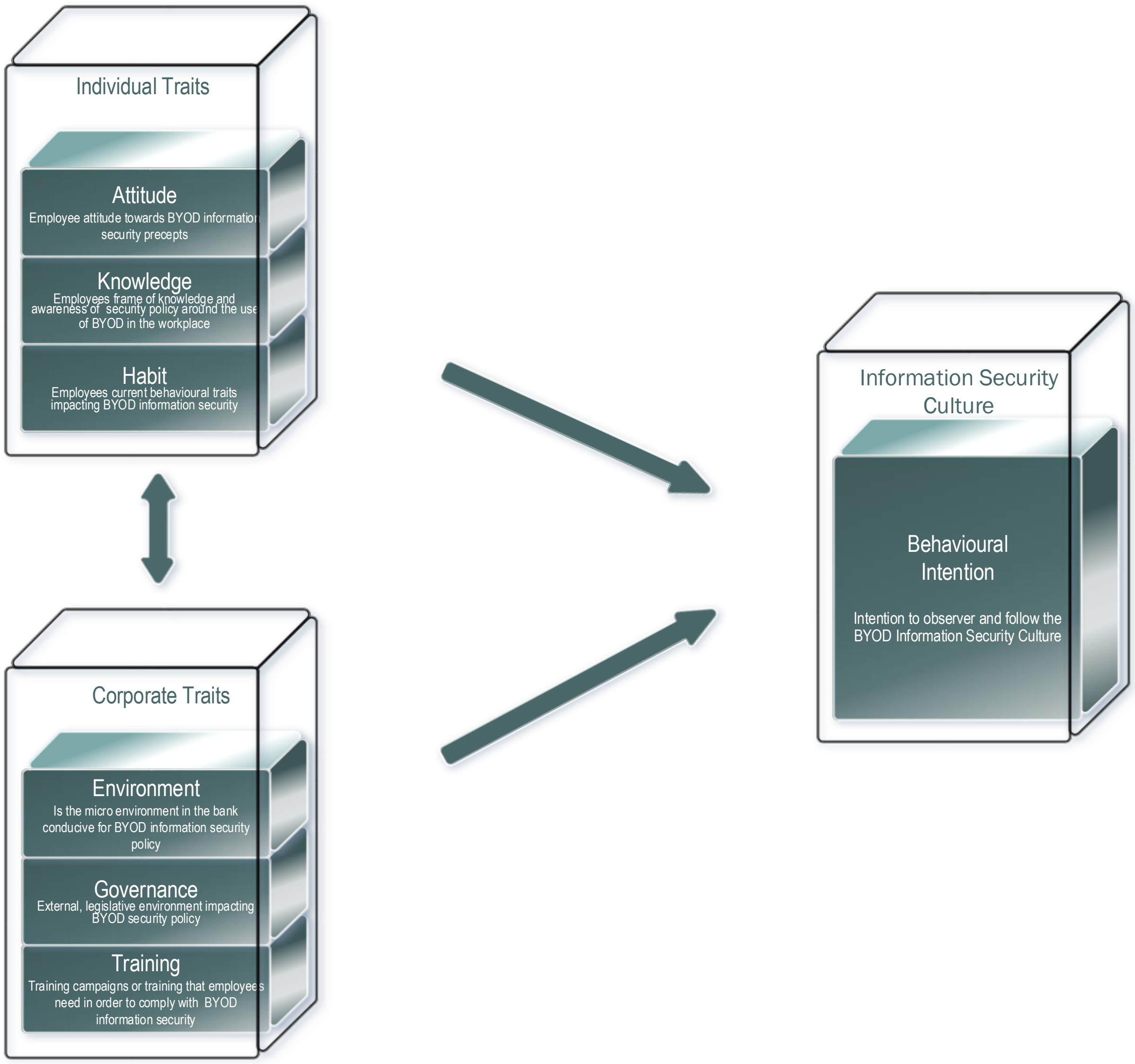

Individual Traits
Attitude
Employee attitude towards BYOD information security precepts
Knowledge
Employees frame of knowledge and awareness of security policy around the use of BYOD in the workplace
Habit
Employees current behavioural traits impacting BYOD information security
Corporate Traits
Environment
Is the micro environment in the bank conducive for BYOD information security policy
Governance
External, legislative environment impacting BYOD security policy
Training
Training campaigns or training that employees need in order to comply with BYOD information security
Information Security Culture
Behavioural Intention
Intention to observer and follow the BYOD Information Security Culture

Figure 1. Main Research Output

The model of relevance in this research is the BISB model. Chapter 7 discusses in details the research output which is the culmination of the individual and organisational traits. The next section will present the delimitation of this study. Six theoretical propositions were formulated from the six traits identified from the literature review as follows

i. **Proposition 1 (P1)**: Employee **attitude** towards information security is positively associated with the building of an information security culture for the BYOD unintended administrator.

ii. **Proposition 2 (P2)**: The **habit**s of the employee with regard to information security are positively associated with the building of an information security culture in the BYOD phenomenon.

iii. **Proposition 3 (P3)**: Employee **knowledge** is positively associated with the building of an information security culture in the BYOD phenomenon.

iv. **Proposition 4 (P4):** The **training** offered to the employee by organisations is positively associated with the building of an information security culture in the BYOD phenomenon.

v. **Proposition 5 (P5):** The **environment** is positively associated with the building of an information security culture in the BYOD phenomenon.

vi. **Proposition 6: Governance** is positively associated with the building of an information security culture in the BYOD phenomenon.

These propositions were then tested using the statistical techniques of factor analysis, regression and correlation.

1.9 Delimitation of the Study

This study was conducted in Zimbabwe, which is a developing country is Southern Africa with a population of about 14.5 million. The country has 18 banks. The target population identified for this research study was bank employees, restricted to only those employees in the selected target bank in Zimbabwe. The study concentrated on the information security around BYOD in the bank. The study also makes use of some concepts related to human behaviour and attitudes towards technology, culminating in an information security culture model for BYOD. This study also looked at employee attitudes, behaviours, and individual cultural values, among other things, towards information security. It did not include technical aspects of BYOD, only the human aspects related to the use of mobile devices and it did not consider desktop computers. It then investigated how this could be conscripted into the model for building an information security culture to mitigate the risks posed by the employees, who are referred to here as “unintended administrators”.

1.10 Ethical Considerations

Every research project is susceptible to crossing ethical boundaries; as such it is important to observe ethical boundaries when carrying out research Burgess and Pande (2005). Indeed, (Punch, 2006)Punch (2006) maintains that every ethical researcher is responsible for complying with academic integrity and authenticity. In this research, necessary approvals were obtained from the authorities at the bank (see Appendix 3) where the research was conducted, as well as from the participants, who in this instance were the bank's employees. Additionally, ethical clearance was obtained from the University Research Ethics Committee (UREC) under reference number Ref: FLO061SMUS01 (see Appendix 2) .

To ensure the anonymity of the participants, questionnaires were created in a manner that ensured that they did not have to include their personal details. The collected data will be used only for the purpose of this research study so as to safeguard the data from potential misuse. The parties involved digitally signed confidentiality agreements before the study commenced. An email link was used to distribute the questionnaires.

1.11 Research Project Outline and Summary

Figure 2 contains the chapter breakdown in this research project. Chapter 1 contains the research background and problem statement, as well as an overview of the research design and methodology for this study, while Chapter 2 covers the research methodology. Chapters 3 to 5 cover the literature review, with Chapter 3 exploring organisational culture. Chapter 4 will build on Chapter 3 by examining information security culture, which is a subculture of organisational culture. Chapter 5 addresses the components required for building an information security culture and concludes the literature review chapters by exploring the information security in the BYOD. Chapter 6 addresses information security with regard to BYOD and Chapter 7 covers the theoretical contribution made by this research. Chapter 8 discusses the analysis and findings and makes a number of recommendations, while Chapter 9 covers the model evaluation process. This research document concludes with Chapter 10 which summarises the entire research project.

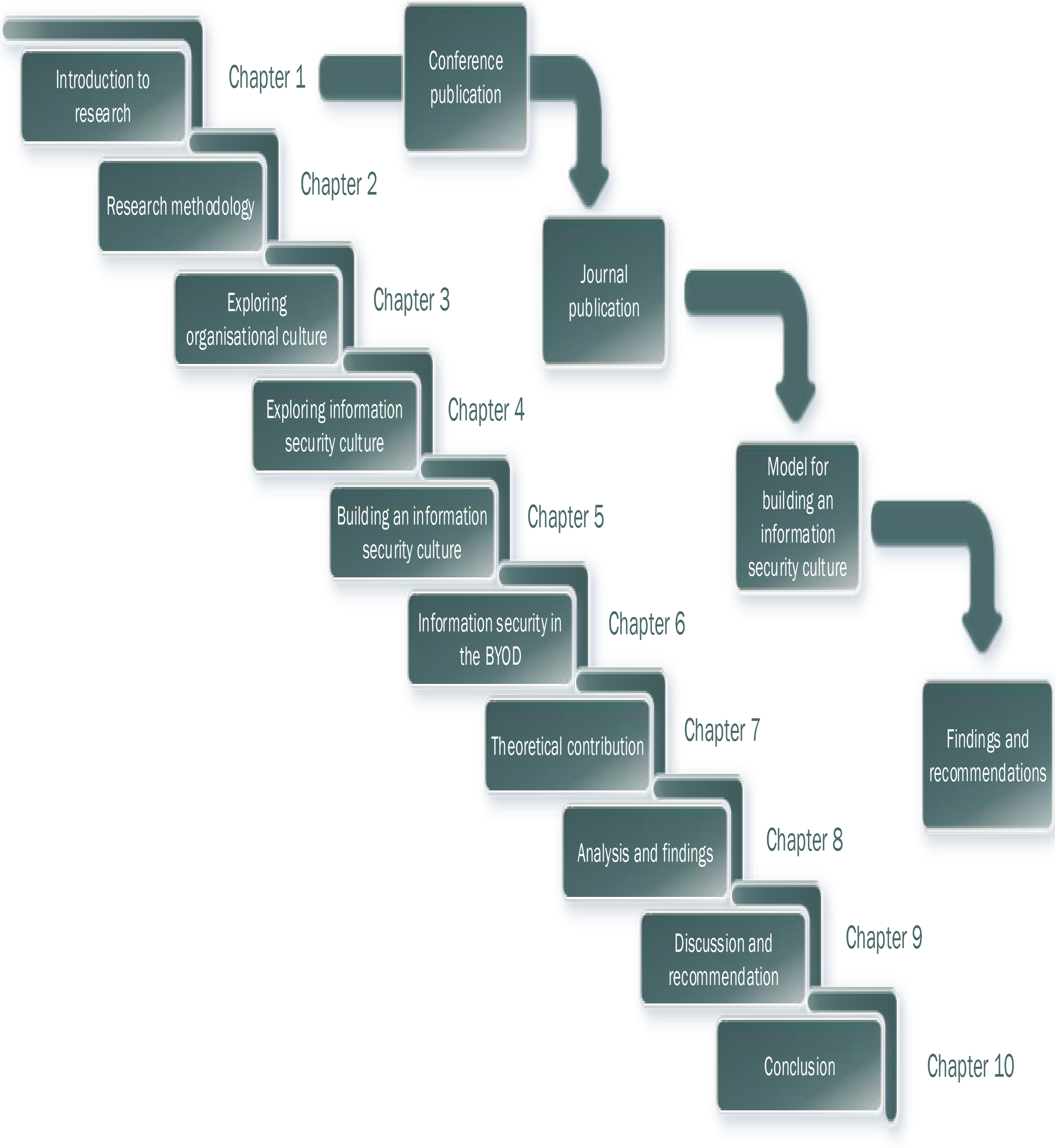
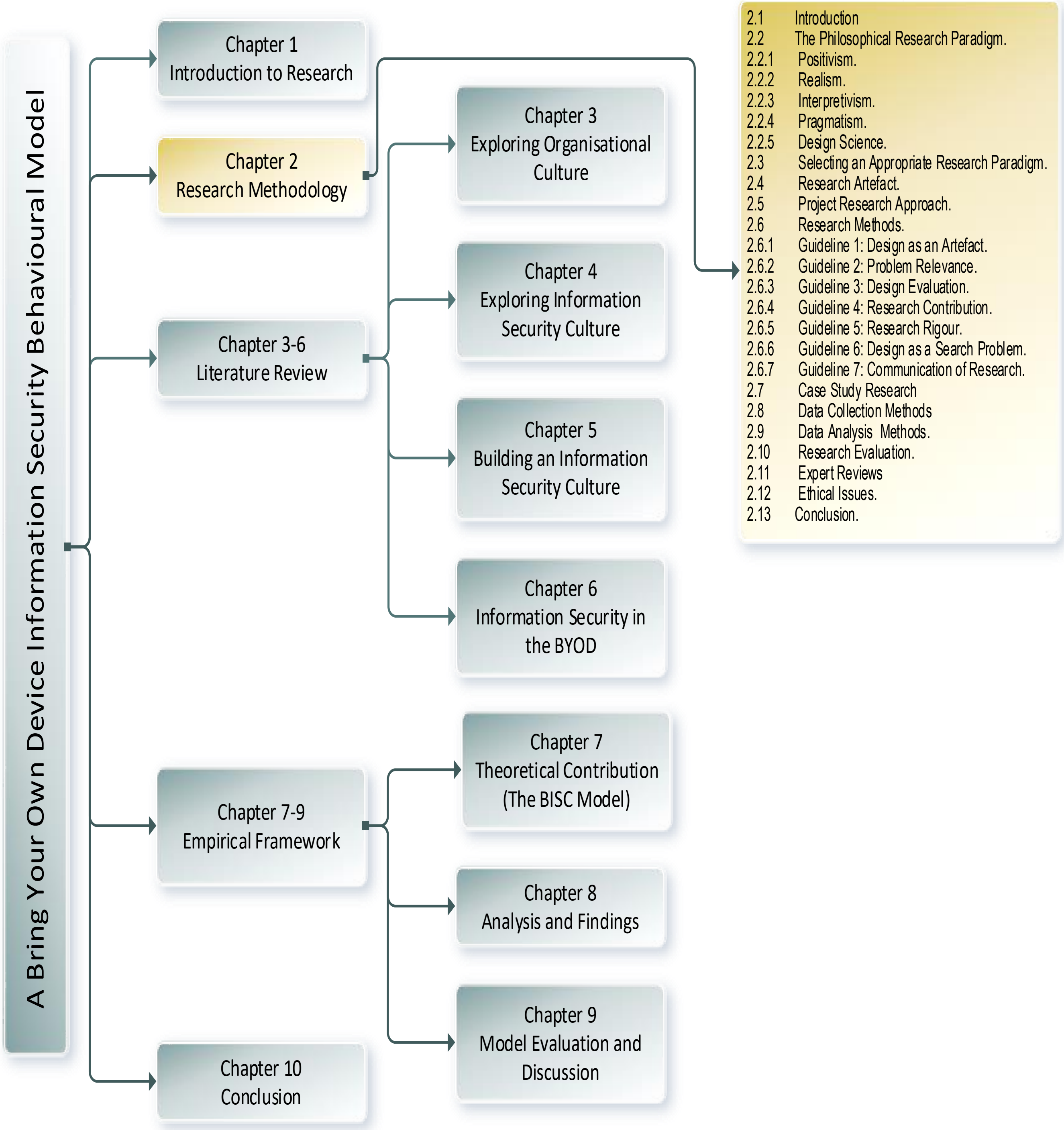

Introduction to research
Chapter 1
Conference publication
Research methodology
Chapter 2
Journal publication
Exploring organisational culture
Chapter 3
Exploring information security culture
Chapter 4
Model for building an information security culture
Building an information security culture
Chapter 5
Information security in the BYOD
Chapter 6
Theoretical contribution
Chapter 7
Findings and recommendations
Analysis and findings
Chapter 8
Discussion and recommendation
Chapter 9
Conclusion
Chapter 10

Figure 2. Chapter Breakdown and Research Plan

Chapter 2 : Research Methodology



A Bring Your Own Device Information Security Behavioural Model

Chapter 1
Introduction to Research

Chapter 2
Research Methodology

Chapter 3-6
Literature Review

Chapter 7-9
Empirical Framework

Chapter 10
Conclusion

Chapter 3
Exploring Organisational Culture

Chapter 4
Exploring Information Security Culture

Chapter 5
Building an Information Security Culture

Chapter 6
Information Security in the BYOD

Chapter 7
Theoretical Contribution (The BISC Model)

Chapter 8
Analysis and Findings

Chapter 9
Model Evaluation and Discussion

2.1 Introduction
2.2 The Philosophical Research Paradigm.
2.2.1 Positivism.
2.2.2 Realism.
2.2.3 Interpretivism.
2.2.4 Pragmatism.
2.2.5 Design Science.
2.3 Selecting an Appropriate Research Paradigm.
2.4 Research Artefact.
2.5 Project Research Approach.
2.6 Research Methods.
2.6.1 Guideline 1: Design as an Artefact.
2.6.2 Guideline 2: Problem Relevance.
2.6.3 Guideline 3: Design Evaluation.
2.6.4 Guideline 4: Research Contribution.
2.6.5 Guideline 5: Research Rigour.
2.6.6 Guideline 6: Design as a Search Problem.
2.6.7 Guideline 7: Communication of Research.
2.7 Case Study Research
2.8 Data Collection Methods
2.9 Data Analysis Methods.
2.10 Research Evaluation.
2.11 Expert Reviews
2.12 Ethical Issues.
2.13 Conclusion.

2.1 Introduction

Research is incomplete without examining the who, what, when and why of the subject under study. Rajasekar, Philominathan, and Chinaathambi (2013) define research as "a logical and systematic search for new and useful information on a particular topic" (p. 2). This is achieved through an investigation which is directed at finding solutions to social and scientific problems through objective and systematic analysis. Hofstee (2006) indicates that the success of a study is determined to a large extent by the method that the researcher chooses to carry out the research. The reproduction, recognition or rejection of research results is determined by how they were arrived at (Hofstee, 2006). According to Robson (2015), if research is to be viewed as scientific, there has to be a way of carrying it out systematically, sceptically, and ethically.

During the research process, the research is guided by the philosophical paradigm which outlines the philosophical underpinnings and the intellectual structure, as well as the underlying assumptions which form the baseline for the research (Göktürk, 2005). In carrying out a research study, assumptions about ontology, which is the nature of reality, as well as epistemology, which is the way in which knowledge is created, are followed by the researcher. The research paradigm gives insight into the researcher's assumptions, the research theme and knowledge construction, whereas the research methodology provides answers to the following questions:

- ✓ How is knowledge attained from the study?
- ✓ What leads to the research goal?

Scientific study follows a structured approach in line with a theory, which informs the research question, leading to the research design and research methods. Research may be regarded as the accumulation of a series of stages. Saunders, Lewis, and Thornhill (2009) recognise six research stages made up of philosophies, approaches, strategies, choices, time horizons, and techniques and procedures.

An inductive logic approach was followed in this study. The main data collection method used in this study is the questionnaire, which was derived from the literature review. The questionnaire was uploaded as an online survey developed using Survey Monkey and emailed to 270 bank employees. Of the 205 respondents, 170 fully completed the survey. The results of the data collected are discussed in detail in Chapter 8 (Analysis and Findings).

The chapter on the research methodology begins with an explanation of the various research philosophies of positivism, realism, and interpretivism, and paradigms of case study research and design science. The way the appropriate research paradigm was selected is also discussed. This is then followed by a discussion on the research artefact, research approach and the research methods. Design science research, which is the selected paradigm for this study, is also discussed in detail. The data analysis methods come next, followed by an account of the data collection methods used in this study, which covers the primary and secondary data collection methods. The chapter concludes by explaining how the integrity of the study’s results was assured under the research evaluation and ethical issues assessment. The next section will summarise the various philosophical research paradigms available to the researcher so as to give a premise for the selection of the appropriate research paradigm.

2.2 The Philosophical Research Paradigm

Collis and Hussey (2003) present a research paradigm as an overall philosophical framework for the way in which scientific knowledge is produced. Rossman and Rallis (2011) view a research paradigm as “shared understandings of reality” (p. 36), whereas Weaver and Olson (2006) remark that it is a “worldview” or “a set of conventions about how things work” (p. 45). Figure 3 shows the three pillars for the research paradigm.

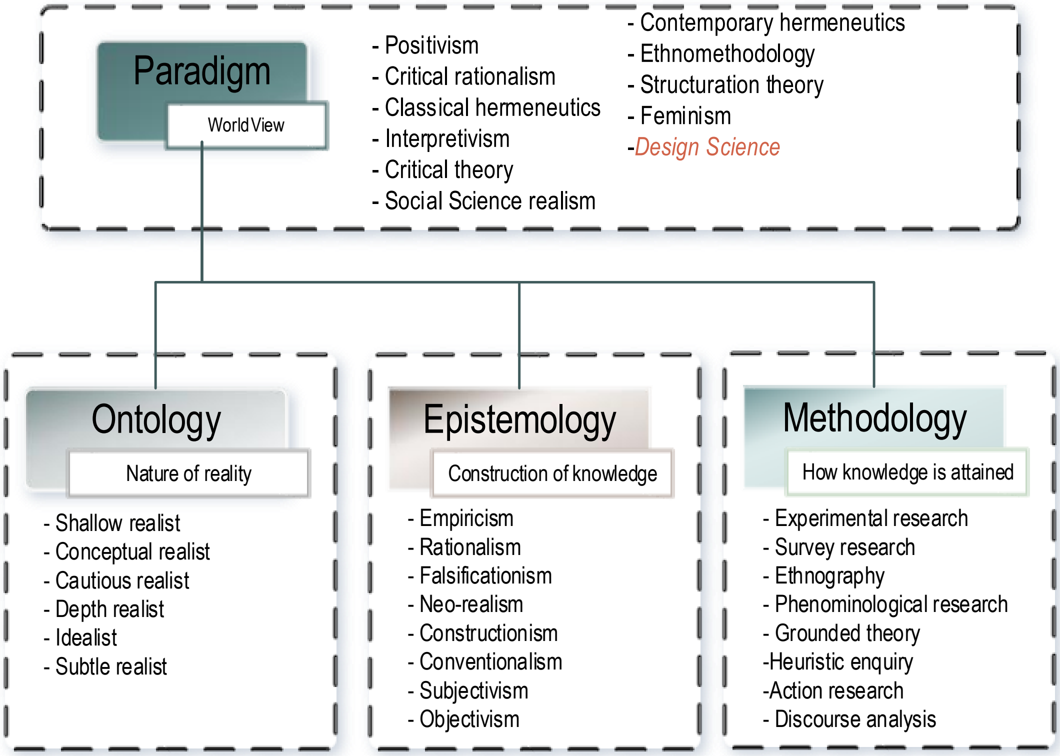


Table 2. Research Paradigm Dimensions

Source: Adapted from Terreblanche, Durrheim, and Painter (2006)

In trying to clarify the structure of the assumptions and philosophies that underpin research, Terreblanche et al. (2006) describe a research paradigm as the nature of enquiry along the lines of ontology, epistemology and methodology. Figure 3 above portrays the architecture of a paradigm as a combination of three pillars: ontology, epistemology and the methodology. These pillars can be explained as follows:

- **Ontology.** For this study this pillar of the research paradigm covers the nature of reality in the context of BYOD information security. The reality on the ground is that the unintended administrator has full administrative control of their mobile device, making it difficult for the CIO to take full control of the management of organisational information security. In making use of the design science paradigm chosen from the adapted model in Figure 3 as the main philosophy for this study, the nature of reality on the ground will be ascertained through inductive means to create the underlying assumptions forming the baseline for the reason for creating an information security culture for the BYOD unintended administrator.

- **Epistemology:** This research paradigm pillar addresses the way this study will address the creation of new knowledge on how an information security culture for the BYOD unintended administrator will be achieved. Theories on human behaviour were used to produce constructs that were then tested through statistical methods. The guidelines from design science were followed in achieving this process.
- **Methodology:** This third research paradigm pillar addresses the means by which the nature of reality can lead to the creation of knowledge through inductive means. The research methodology used in this study is the main theme for this chapter and will be discussed in subsequent sections.

Additionally, the description of a paradigm explains how research could be steered: "Paradigms are patterns of beliefs and practices that regulate inquiry within a discipline by providing lenses, frames and processes through which investigation is accomplished" (Rossman & Rallis, 2003, p. 460). Collis and Hussey (2003) argue that a research paradigm points the way in which a study should be carried out. The selection of a correct research paradigm is the foundation for ensuring that the research methodology satisfies the perspective behind the assumptions of the paradigm. This suggests that a research paradigm must guide every study.

According to Gregor and Hevner (2013), Information Systems research can be divided into two major types:

i. **Behavioural science,** which seeks to develop and verify theories predicting or explaining human as well as organisational behaviour.

ii. **Design science**, which seeks to extend the boundaries of human organisational capabilities by creating innovative artefacts. Design science seeks to expand the limitations of human and organisational aptitudes by creating innovative artefacts (Hevner et al., 2004).

This study is centred on securing the BYOD unintended administrator by fostering an information security culture. The study employed a design science paradigm as it seeks employee participation in the creation of the BISB model. De Vos, Strydom, Fouche, and Delport (2004) support the view that it is not possible for researchers to work in isolation since the domain and structure of research is shared within disciplines.

Kuhn (1970) was the first to explain the philosophical research paradigm and argued that physical science exists in a distinct cycle of periods of normal science preceded by scientific revolutions. After this a comparative study of philosophical paradigms was conducted and it was concluded that unlike in the physical sciences, in social sciences there is no discipline in which a single dominant paradigm could be found (Taljaard, 2016). Critics have raised concerns on this comparison between the physical and social sciences, considering that the function of problem solving is not the same for the two sciences. Problem solving in physical sciences has a clear and specific meaning, whilst in the social sciences it is associated with in-depth understanding, analysis, interpretation and explanation.

Collis and Hussey (2009) further explain that whilst dominant paradigms exist in social sciences, it is the researcher's prerogative to choose a specific research paradigm with specific philosophical assumptions based on the nature of reality (ontology) and how knowledge can be constructed (epistemology) that best fits the objectives of the research study. In support of this early on, Easterby-Smith, Thorpe, and Lowe (2002) remark that a well-chosen philosophy will assist the researcher to evaluate the existing methodologies early in the research process, thereby selecting the most appropriate approach for the research project. The gathered evidence as well as the how it will be interpreted to address the research question will be determined by the research methods. Inferences from the three pillars of research methodology explain how knowledge is attained in the study. In the context of this study, design science guidelines will inform the way knowledge will be attained on information security for the BYOD unintended administrator.

In as much as various paradigms can be distinguished along the basis of their philosophical assumptions that exist in social science, there is disagreement regarding the appropriateness of a chosen philosophical paradigm for Information Systems research (Collis & Hussey, 2009; Saunders et al., 2009). From the viewpoint of Oates (2006), the fact that artefacts are produced with no consideration for the underlying philosophy is a common Information Systems research problem. Several researchers have warned against strict adherence to a particular research paradigm, which they believe will lead to a delay in the scientific process (Göktürk, 2005; Hofstee, 2006; Krauss & Putra, 2005). For this reason, Collis and Hussey (2009) urge researchers not to make use of one specific paradigm or approach in their research. They maintain that using a combination of more than one assists researchers to implement a broader and often more balanced view of the research problem.

Collis and Hussey (2009) highlight that the positivist and interpretivist paradigms are recognised in the context of Information Systems research. Several different realities may be distinguished according to the approach chosen by the researcher to specify the study. This research project will make use of the design science research approach, which will be explained at length in the subsequent sections. Other paradigms that are available to the researcher include critical research and many others discussed in the following sections of this chapter. This is followed by a comparison of the fundamental differences between the paradigms and a discussion of the motivation behind the selection of the main research paradigm that was deemed appropriate for the purposes of this study.

2.2.1 Positivism

According to the positivist epistemology, science is seen as the way to obtain truth to understand the world well enough so that it might be predicted and controlled. Healy and Perry (2000) maintain that positivism predominates research in science and assumes that science quantitatively measures independent facts about a single apprehensible reality. Proponents of a positivist philosophy believe that things should be studied as hard facts, and the results should establish scientific laws which have the status of truth. In a more general sense, the data and its analysis are independent and data does not change as a result of being observed, as researchers view the world through a one-way mirror.

Kołakowski (1972) harnesses a four-point doctrine on positivism as follows:

i. The rule of phenomenalism asserts that there is only experience; all abstractions, be they “matter” or “spirit”, are fallacies.
ii. The rule of nominalism asserts that words, generalisations and abstractions are linguistic phenomena and do not give new insight into the world.
iii. The separation of facts from values.
iv. The unity of the scientific method.

This study explores the factors that must be in place in order to build a model for creating an information security culture for the BYOD unintended administrator. Culture is a social aspect of humanity, therefore the social nature of humankind had to be included in the study. An appropriate paradigm would have to rely on the researcher’s social context. This, in turn, meant that that a pure positivist paradigm was unsuitable for this research project. The next section presents the realist paradigm.

2.2.2 Realism

Realism is becoming a useful paradigm for social scientists (Sobh & Perry, 2006). Its philosophical position is that reality exists independently of the researcher’s mind. This implies that there is an external reality which consists of abstract things that are born of people’s minds but exist in isolation from any one person's influence. Whitbeck and Bhaskar (1977) argue that a person's views are an opening onto that incoherent outer reality. Realism denotes this exterior reality as consisting of structures that are sets of interconnected objects and of mechanisms through which those objects interact. Proponents of realism believe that there is a "real" world "out there" to discover. However, Tsoukas (1989) believes that the real external world is only imperfectly and probabilistically apprehensible. Realists recognise differences between the real world and their particular interpretation of it and try to build various views of this reality in terms of which ones are relative in time and place (Riege, 2003).

The causal structures investigated in a social science are only contingently linked to the experiences that a researcher has in the field; as such the combined special effects of underlying structures and mechanisms result in patterns and experiences, but those patterns will not always occur. The contexts of perceived phenomena are significant. Consequently, the aspiration of realism research is to develop a "family of answers" that covers several dependent contexts and different insightful participants (Perry, Riege, & Brown, 1999).

Although this paradigm is applicable to Information Systems research, it seeks to construct and develop the realist social context of Information Systems (Sobh & Perry, 2006). In as much as this study explores information security, the aspect of culture is more of an incorporeal component of human existence. In this context the realism paradigm seeks to understand the common reality of an information security culture in which many people operate interdependently. This implies, as realists believe, that there is a "real" information security culture out there to discover. However, a purely realistic stance was not deemed suitable for this research project, as pointed out by Tsoukas (1989) when he argues that the real external world is only imperfectly and probabilistically apprehensible. The next section will discuss the interpretivist research paradigm.

2.2.3 Interpretivism

The interpretivist paradigm can also be termed the "anti-positivist" paradigm as it was established as a reaction to positivism and it is sometimes referred to as constructivism because it underscores the ability of the individual to construct meaning (Mack, 2010). Researchers recognise that all contributors involved, including the researcher, bring their own unique interpretations of the world or edifices of the situation to the research. The researcher needs to be open to the attitudes and values of the participants or, more actively, suspend prior cultural assumptions. This research paradigm concerns a number of realities about a single mind-independent reality (Healy & Perry, 2000). Interpretive researchers believe that reality consists of people's subjective experiences of the external world; thus, they may adopt an inter-subjective epistemology and the ontological belief that reality is socially constructed. Interpretivism does not aim to verify or refute hypotheses, as does positivist research, rather it seeks to ascertain, explore and clarify how the factors in a social setting are connected and interdependent (Oates, 2006; Richey & Klein, 2014). Mack (2010) argues that interpretivists are anti-foundationalists who believe there is no single correct route, or particular method, to knowledge.

Oliver (2011) states that while interpretivist research is comparatively subjective, in contrast to positivism, it may be subjective to the researcher's beliefs, values and actions. The interpretivist paradigm was influenced by hermeneutics, which is the study of meaning and interpretation in historical texts and phenomenology, and advocates the "need to consider human beings' subjective interpretations, and their perceptions of the world as our starting point in understanding social phenomena" (Rajasekar et al., 2013, p. 5). This meaning-making cyclical process is the basis on which the interpretivist paradigm was established (Goldkuhl, 2012). Interpretivists reject both objectivism and a single universal truth. The objective of interpretivist research is to reveal inside viewpoints or the real meaning of social occurrences and not to produce a universal, generalisable result as is the case with positivism.

Oates (2006) believes that this paradigm is suitable for most Information Systems research as it seeks to construct and develop the social context of Information Systems. Whilst this research project did focus on the human culture element, it also incorporated quantitative data analysis to support the results of both the literature survey and the conversational analysis. Therefore, a purely interpretivist stance was not deemed suitable for this research project. The following section presents the fourth paradigm of pragmatism.

2.2.4 Pragmatism

Pragmatism is entrenched in the acceptance that a proposition is true if it functions satisfactorily and its meaning is to be found in the practical implications of accepting such a proposition (McDermid, 2006). Pragmatism is concerned with action and change and seeks knowledge through intervention rather than observation (Goldkuhl, 2012). According to Goldkuhl (2012), the creation of knowledge in pragmatism is not limited to descriptions or understanding; instead, it recognises other information forms such as prescriptive, normative, prospective and explanatory knowledge. Pragmatism recognises both the natural and physical worlds, as well as the emergent social and psychological worlds. In pragmatism, a researcher is given the opportunity to state his/her research question and then to determine the research framework that would be the most appropriate to answer it. Wahyuni (2012), maintains that a pragmatic approach inspires the researcher to interpret the research philosophy as a continuum rather than in the context of the two divergent extremes of interpretivism and positivism. This implies that a mixture of ontology, epistemology and axiology is satisfactory for approaching and understanding social phenomena.

Johnson, Onwuegbuzie, and Turner (2007) explain that this approach is also known as mixed methods research, which they describe as the form of research where the researcher combines quantitative and qualitative research techniques, methods, approaches, concepts or language into a single study. Wahyuni (2012) considers pragmatism as an expansive and creative form of research, which requests the researcher to take an eclectic approach to method choice in order to produce research that is inclusive, pluralistic and complementary. However, it was felt that the creation of a behavioural model for building an information security culture for the BYOD unintended administrator is part of the research paradigm: design science research. Accordingly, this paradigm will be discussed in the next section.

2.2.5 Design science

Hevner and Chatterjee (2004) argue that design science offers an effective means of addressing the relevancy gap that has plagued academic research, particularly in the management and information systems disciplines. Design science is a problem-solving paradigm which guarantees that the process of building and applying an artefact creates understanding of a problem (Peffers et al., 2007). Models, instantiations, constructs and methods generally constitute the form of these artefacts. The two broad design science aims for the creation of an artefact are enabling an understanding of the problem in question and confirming that the solution is feasible. Hevner et al. (2004) describe the four categories of artefacts as follows:

i. **Constructs –** provide the language for defining and communicating problems and solutions.
ii. **Models –** represent the real-world situation while assisting in the understanding of the problem and the solution to the problem.
iii. **Methods** – define processes and provide guidance for solving problems.
iv. **Instantiations –** show that constructs, models or methods may be implemented in a working system.

Gregor and Hevner (2013)

Gregor and Hevner (2013) propose a knowledge contribution framework for use by the researcher in placing the contribution or artefact of a design science research project. The authors hypothesise that the research contribution cannot be totally 'new' but that contributions are derived from some previous idea or else are made of something else that occurred before. It can thus be deduced that the contribution of design science research will be underpinned at the start by the context of the problem and the maturity of the solution. Figure 4 shows the design science research contribution quadrant. This study is positioned in the first quadrant of improvement, as it seeks to develop a new solution that improves and mitigates the management of Information Security challenges posed by the BYOD unintended administrator in banks.

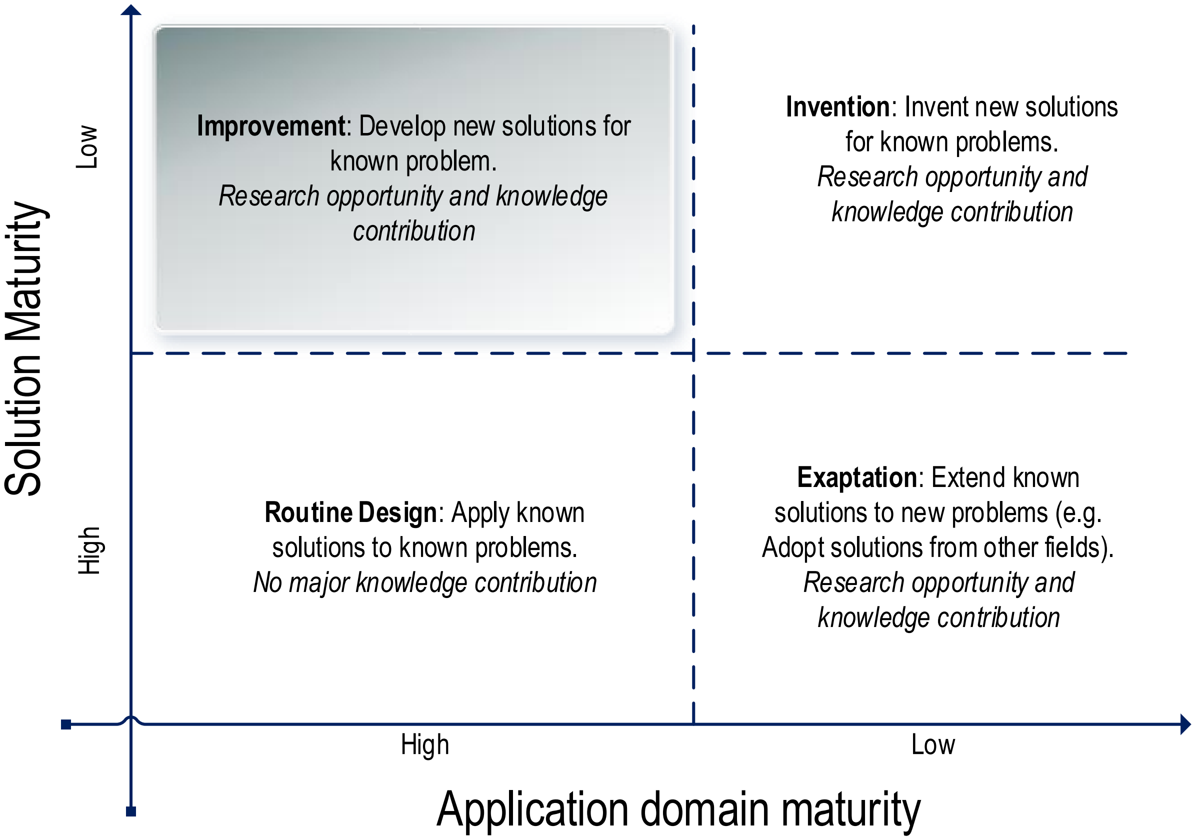

Solution Maturity
Low
High
Improvement: Develop new solutions for known problem.
Research opportunity and knowledge contribution
Invention: Invent new solutions for known problems.
Research opportunity and knowledge contribution
Routine Design: Apply known solutions to known problems.
No major knowledge contribution
Exaptation: Extend known solutions to new problems (e.g. Adopt solutions from other fields).
Research opportunity and knowledge contribution
High
Low
Application domain maturity

Figure 3. Design science research knowledge contribution framework

Source: Peffers et al. (2008)

Below is a brief description of the four quadrants:

- **Improvement**. This study is positioned in this quadrant which identifies known opportunities that will be developed by the researcher contributing to both the research opportunity and the knowledge base. The new model developed from this study will mitigate the information security challenges posed by the BYOD unintended administrator in banks. The artefacts developed are deemed to be more efficient and functional than previous solutions and may take the form of services, processes, technologies, products, or ideas.
- **Invention**. In this quadrant, new solutions for new problems are invented and these solutions contribute to both the research prospect and the knowledge base. This type of research will contribute to new and interesting applications where no effective artefacts are yet available because of a lack of understanding of the problem context. In this study the problem for information security posed by the BYOD unintended administrator is not new and the solutions to be given are basically improvements to the existing information security challenges.
- **Exaptation**. This quadrant extends a recognised solution from another discipline to a new problem, thereby contributing to both the research opportunity and the knowledge base. The researcher is expected to demonstrate that the extension of known design knowledge into a new field is not trivial and interesting, and the production of an effective artefact from a related problem area to fit the current research context.
- **Routine design**. This quadrant occurs when a known solution is applied to a known problem resulting in no major knowledge contribution being expected. If a discovery is made during the research, this would probably move the research project into one of the other quadrants.

The improvement quadrant will be applicable to this research project as the primary objective of this research project is to produce a model that will be used by banks to build an information security culture for the BYOD unintended administrator. This model, or artefact, was applied to a known problem of implementing an information security culture for users who have total control of their devices in terms of BYOD. The next section will examine the selection of an appropriate research paradigm is for this research project.

2.3 Selecting an Appropriate Research Paradigm

In section 2.2 we noted that it is rare in research for a researcher to make use of either a purely positivist or interpretivist paradigm as their research approach. The use of more than one research paradigm in a study enables the researcher to take a broader and often complementary view of the research problem (Collis & Hussey, 2009). Table 4 provides a brief review of the conclusions on the paradigms discussed in sections 2.2.1 to 2.2.5.

Based on the previous discussion of the different paradigms, this study aligns itself with the design science research paradigm as being the most appropriate for the project. The design science research paradigm supports a mixed methods approach, which makes it appropriate for this research as it includes both the qualitative and quantitative collection of data using the questionnaire data collection method. According to a definition by Cameron (2011), a mixed methods approach is "philosophical assumptions that guide the direction of the collection and analysis of data and the mixture of qualitative and quantitative data in a single study or series of studies" (p. 4). The fact that the design science paradigm provides comprehensive guidelines on designing Information Systems artefacts also contributed as the reason for its selection. The objective of this research project is to produce a model for identifying information security behaviour for the BYOD unintended administrator in a bank. An effective set of guidelines provided by Hevner et al. (2004) contributes to the development and evaluation of a novel research artefact, as discussed in section 2.5. For this reason, the design science research paradigm was selected for this research project.

Table 3. Selection of Appropriate Research Paradigm

RESEARCH PARADIGM	CONCLUSION DEDUCED FROM LITERATURE REVIEW
Positivism	A single, objective reality that does not take into account the social nature of humans as an important factor when conducting research is provided for in this research. This implies that the results of positivist studies may easily be generalised. In view of the fact that an information security culture is derived from the social aspects of humans, a purely positivist paradigm was not deemed appropriate for the purposes of this study.
Realism	Realism lies between the positivist and interpretivist stances. This paradigm is applicable to Information Systems research as it seeks to construct and develop the realist social context of Information Systems. While this study explores information security, the culture

	aspect is more of an intangible component of human existence. In this context the realist paradigm seeks to understand the common reality of an information security culture in which many people operate interdependently.
Interpretivism	This paradigm is subjective in nature and allows for values and knowledge to emerge from the researcher–participant interaction. This paradigm is strongly influenced by the qualitative data collection methods that enable the researcher to understand and analyse the phenomenon being investigated. The model will be evaluated by means of a questionnaire and the results will be analysed using descriptive and inferential statistical methods. Thus a purely interpretivist research paradigm was deemed appropriate for the purposes of this research project.
PRAGMATISM	Pragmatism identifies both the natural and physical worlds, as well as the emergent social and psychological worlds. It also views knowledge as being constructed and based on the reality of the world in which we live and which we experience. In addition, it offers the researcher the opportunity to make use of a combination of both quantitative and qualitative methods in order to investigate the research problem. Thus, in view of the fact that this research project would make use of both quantitative and qualitative methods, this research paradigm might have been considered suitable for the project. However, the lack of focus on the research artefact would be a disadvantage if this paradigm were used.
Design science	The design science paradigm solves problems by ensuring that knowledge and understanding of a problem are achieved through the building and application of an artefact. This research paradigm also allows the researcher to make use of a mixed method approach while also directing the focus of the research to the produced artefact. The lack of focus on the artefact in the pragmatist paradigm meant that

	the design science paradigm was deemed to be the most appropriate for the purposes of this research project.

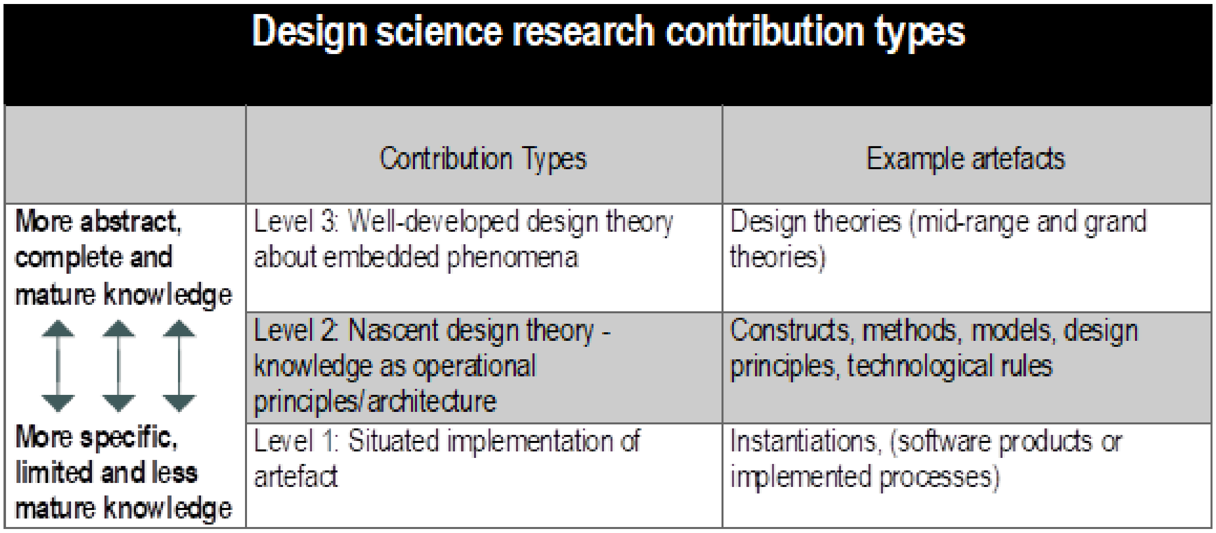
Source: Peffers et al. (2008)

It was felt that the design science paradigm, which offers guidelines or steps on designing and evaluating Information Systems artefacts, could play an important role in attaining the objective of the study. The next section will discuss the research artefact for the research project.

2.4 Research Artefact

Research artefact refers to a thing that has, or can be converted into, a material being through an artificial process (Peffers et al., 2008). Here, an instantiation is provided as an example of an object and a method or software as an example of a process producing a specific design science artefact; or more levels ranging from specific models at a level 1 to mature design theories at level 3.

Table 4. Design Science Research Contribution Types



Design science research contribution types

	Contribution Types	Example artefacts
More abstract, complete and mature knowledge	Level 3: Well-developed design theory about embedded phenomena	Design theories (mid-range and grand theories)
↕ ↕ ↕	Level 2: Nascent design theory - knowledge as operational principles/architecture	Constructs, methods, models, design principles, technological rules
More specific, limited and less mature knowledge	Level 1: Situated implementation of artefact	Instantiations, (software products or implemented processes)

Source: Peffers et al. (2008)

The levels that Gregor and Hevner (2013) make reference to regarding contribution types and artefacts produced by design science research are shown in Table 5 above. Level 1 describes a contribution as being more specific, less mature knowledge and limited knowledge. Gregor and Hevner (2013) further explain that although at level 1 there may be no abstraction or theorisation about the design principles or architecture, the artefact in itself may be realised as a research contribution. Level 2 discusses the nascent design theory which presents knowledge as operational principles or architecture. This contains examples such as methods, technological rules, constructs, design principles and models. The outcome of the current research project is a model which fits into level 2, thereby positioning this research on level 2. A research contribution type at level 3 is described as well-developed design theory on embedded phenomena such as midrange and grand theories. The next section will discuss the research approach followed in this research project.

2.5 Project Research Approach

There are two major types of reasoning in terms of which the research approach may be classified: deductive and inductive (Collis & Hussey, 2009). Figure 5 illustrates inductive and deductive research approaches.

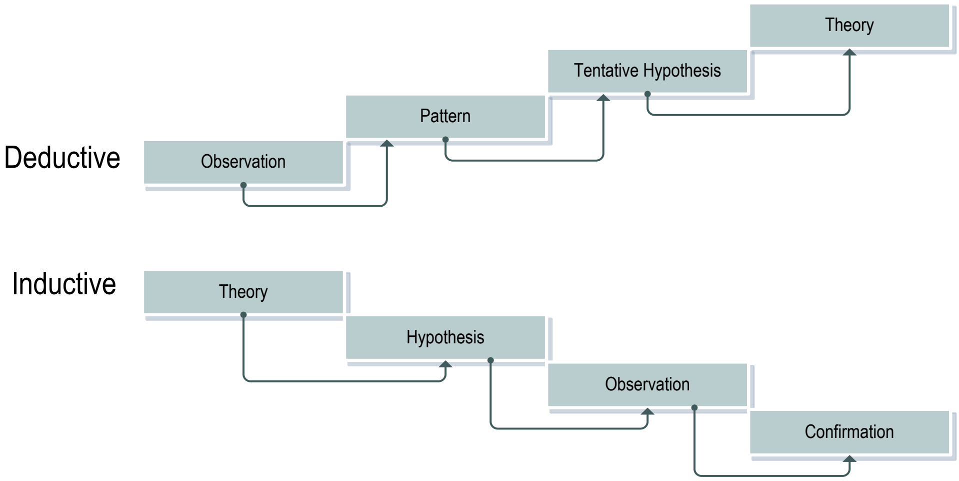


Figure 4. Differences between Inductive and Deductive Logic

Source: Trochim, Donnelly, and Arora (2016)

Burney (2008) describes the deductive research approach as the “uphill climb of deductive reasoning” and the inductive research approach as the “waterfall effect of inductive research”. In creating the model, this research adopted the uphill effect of deductive research. The researcher commenced the project with an in-depth literature review, creating the basis for specific research questions. The research questions were subsequently answered using primary and secondary data selection methods. Research propositions were formulated and statistically tested to confirm the constructs for the research artefact. In this research project, the culmination of the process was a set of constructs that were used to create a model for building an information security culture for the BYOD unintended administrator in a bank. Chapter 7 contains a detailed account of how the constructs were combined in the model for securing the BYOD unintended administrator

2.6 Research Methods

Collis and Hussey (2009) state that it is essential that a researcher selects a methodology that reflects the philosophical assumptions of the chosen paradigm. From the previous description of design science research in section 2.2.5, its goal is evidently to create and evaluate Information Systems artefacts so as to solve the identified organisational problems posed by the unintended administrator. Therefore, based on the fundamental design science principles of knowledge and understanding of a design problem and its solution through the construction of a design artefact, Hevner et al. (2004) provide a set of seven guidelines depicted in a conceptual framework as shown in Figure 6.

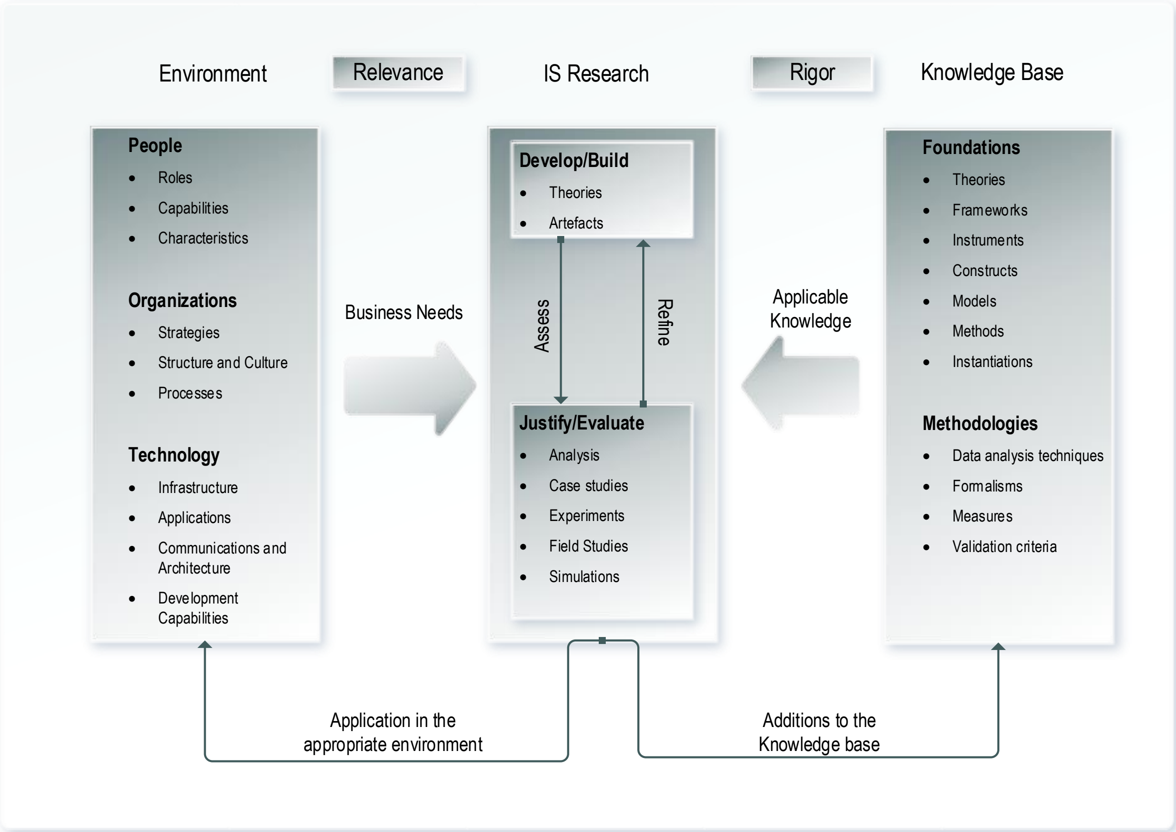


Figure 5. Information Systems Research Framework

Source: Hevner et al. (2004)

The impact of the existing knowledge on Information Systems research as well as the environment were both recognised in Hevner et al.'s (2004) framework. The environment makes reference to the context of the research, which in this case is a commercial bank in Zimbabwe. Accordingly, this environment comprises employees of the bank that make use of BYOD in their various role profiles. The knowledge base is made up of methodologies and theories that are combined in creating a research artefact. The research rigour was enhanced by the use of existing information in the knowledge base. By taking into account the environmental aspects (business need) and the knowledge base (theories and methodologies), a two-stage approach involving building and evaluation is used to conduct Information Systems research. An iterative approach was followed as the researcher makes a contribution to the existing knowledge base by providing an appropriate solution which meets the original business need of the environment.

Although Hevner et al.'s (2004) seven research guidelines direct researchers carrying out design science research, they do not need to be followed in any particular order. The subsequent sections describe the guidelines and provide an overview of how this research project applied these guidelines.

2.6.1 Guideline 1: Design as an Artefact

This research guideline states that research must produce a viable artefact. Hevner et al. (2004) further describe this guideline as one that seeks the establishment of a purposeful artefact created to address an important organisational problem. The primary objective pursued in this research project was to develop an information security behavioural model for the BYOD unintended administrator in commercial banks, which aligns well with this guideline. The output of this research, which is the development of the model as well as the actual development process for the model, will address this guideline.

2.6.2 Guideline 2: Problem Relevance

The research problem investigated in this study is the information security risk posed by the unintended administrator created by the BYOD phenomenon. The unintended administrator has total control over their mobile device. Hevner et al.(2004) explain that in design science, research is there to acquire an understanding that enables the development and implementation of technology solutions that solve important business problems. This research project made use of secondary data in the form of literature reviews in order to establish not only the nature of the problem area but also the phenomena contributing to the existence of such problems.

2.6.3 Guideline 3: Design Evaluation

The purpose of this research guideline is to ensure that the produced artefact has been rigorously assessed in order to ensure the utility, quality and efficacy of the artefact. In order to achieve this, Hevner et al. (2004) stipulate the requirement for a well-executed evaluation method or combination of methods and explain that this is influenced by the design of the artefact. As a result of the design being an inherently iterative and incremental activity, feedback to the construction phase of the artefact is provided by this evaluation phase (Hevner et al., 2004). Statistical tests were also conducted to add to the evaluation process.

Ahmed and Sundaram (2011) propose a number of methods for evaluation which include research symposiums, research consortiums, peer feedback, industry expert reviews, journals, conferences, academic modellers, domain experts, decision makers, system architects, and many others.

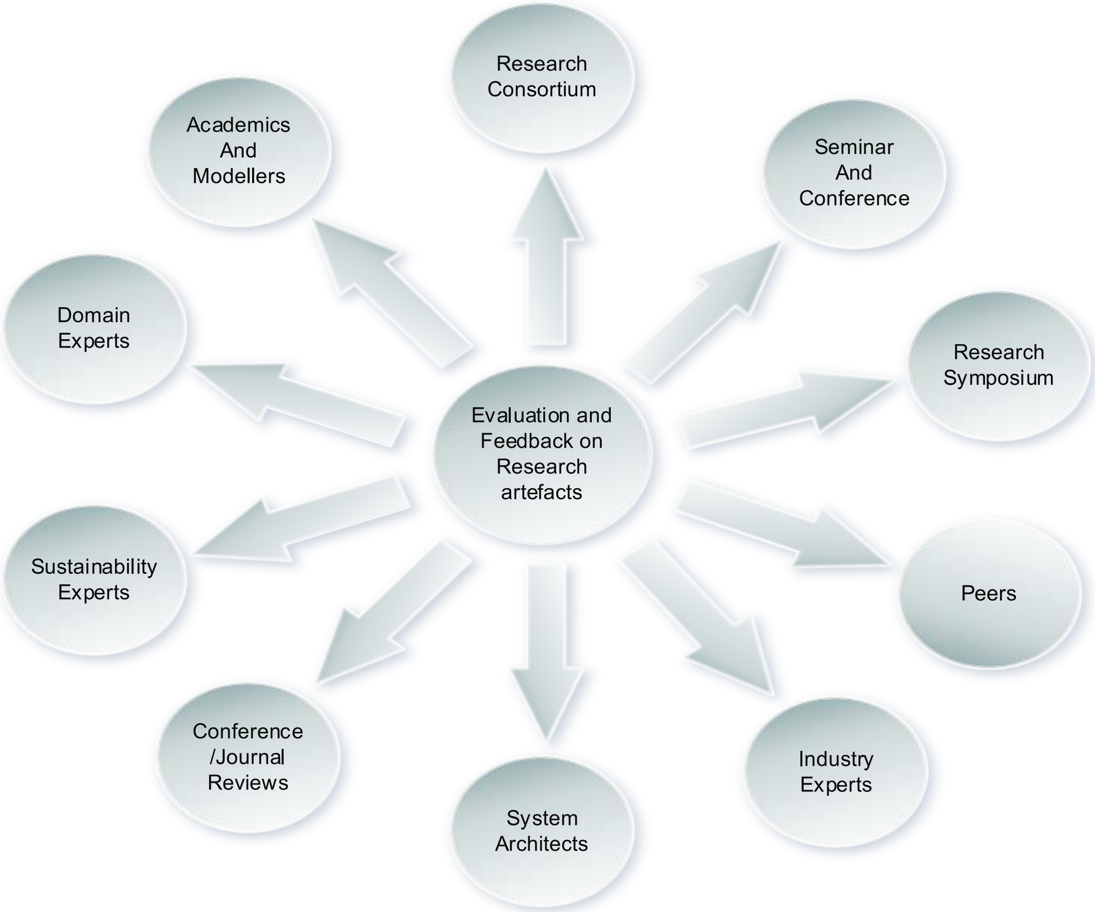


Figure 6. Groups for Evaluation

Source: Ahmed and Sundaram (2011)

Figure 6 depicts the groups for evaluation. This guideline was applied to the study to ascertain the usability of the main research output, namely, the research model. The appropriate evaluation method for this study was chosen as domain expert reviews in the form of CIOs in the banking sector in Zimbabwe. The experts offered comments on the model and the material presented and these comments were then used to refine the model.

2.6.4 Guideline 4: Research Contribution

Hevner et al. (2004) suggest that design science research should contribute to the specified discipline of the artefact designed. They also insist that design science research should provide a clear contribution in the area of the design artefact, design evaluation knowledge and the design construction knowledge. The contributions may be made to the design artefact as well as the research artefact's novelty, generality and significance. The most common contribution in design science, which is directly linked to Guideline 1, is the research artefact. The designed artefact can either provide an alternative solution to a previously solved problem or it can provide a totally new solution to an existing unsolved problem.

Gregor and Hevner (2013) classify the contribution to the research foundation, which in this case is the contribution to design science knowledge bases, into four different forms of the artefact initially defined in section 2.2.5 of this chapter. Figure 4 shows these four different forms which can be summarised as constructs, models, methods and instantiations. This research project is positioned in the 'improvement' quadrant of Figure 4. Gregor and Hevner (2013) explain that in this quadrant the goal is to create more efficient solutions. They note that researchers are expected to contend with a known application context for which useful solution artefacts either do not exist or are clearly suboptimal.

The objective of an information security behavioural model for the BYOD unintended administrator may be achieved by building on existing theories of human behaviour and applying them to the context of information security. The artefact that was produced for the purposes of this research project represents a new solution to the problem of information security in the banking environment caused by the BYOD unintended administrator. Consequently, more secure behaviour of employees in a commercial bank in Zimbabwe would be achieved. The produced artefact is discussed in detail in Chapters 7 and 9. The next section examines the research rigour that was applied in this study.

2.6.5 Guideline 5: Research Rigour

This guideline ensures that appropriate methods are applied in the building and evaluation of the research artefact. According to Hevner et al. (2004), it is important for Information Systems research to be conducted in a manner that is relevant and rigorous. They advise that design science researchers must constantly assess the appropriateness of the metrics they are using, as well as construct effective alternatives. This will remove any doubt that the artefact design is correct. The following steps were taken in this project to ensure research rigour during the artefact construction:

i. A detailed review of the literature was conducted, which culminated in the identification of gaps for related research. This also guided the direction of the study.

ii. The research was guided and validated by making use of theories.

iii. The most appropriate philosophical view was adopted in the research design for this study.

iv. An online survey of the bank employees was conducted and recorded to provide relevant information.

v. The questionnaire used was formulated after a search of the relevant literature had uncovered questionnaires that had been tested and validated in various fields to ensure reliability and validity using the Cronbach's alpha coefficient. A pilot study was conducted before the main survey to ensure the questionnaire satisfied the requirements of the survey.

In ensuring rigour during the artefact evaluation process, several strategies were employed. These included feedback from peers, industry experts and academics. The next section will discuss Guideline 6 as well as the process that was applied during this research project.

2.6.6 Guideline 6: Design as a Search Problem

Hevner et al. (2004) describe design research as an inherently iterative process. They further note that while it is important to establish why a particular solution works, the critical nature of design in Information Systems research makes it important to first establish whether the artefact solution can work. Figure 8 illustrates multiple entry points and iterations derived from other literature sources.

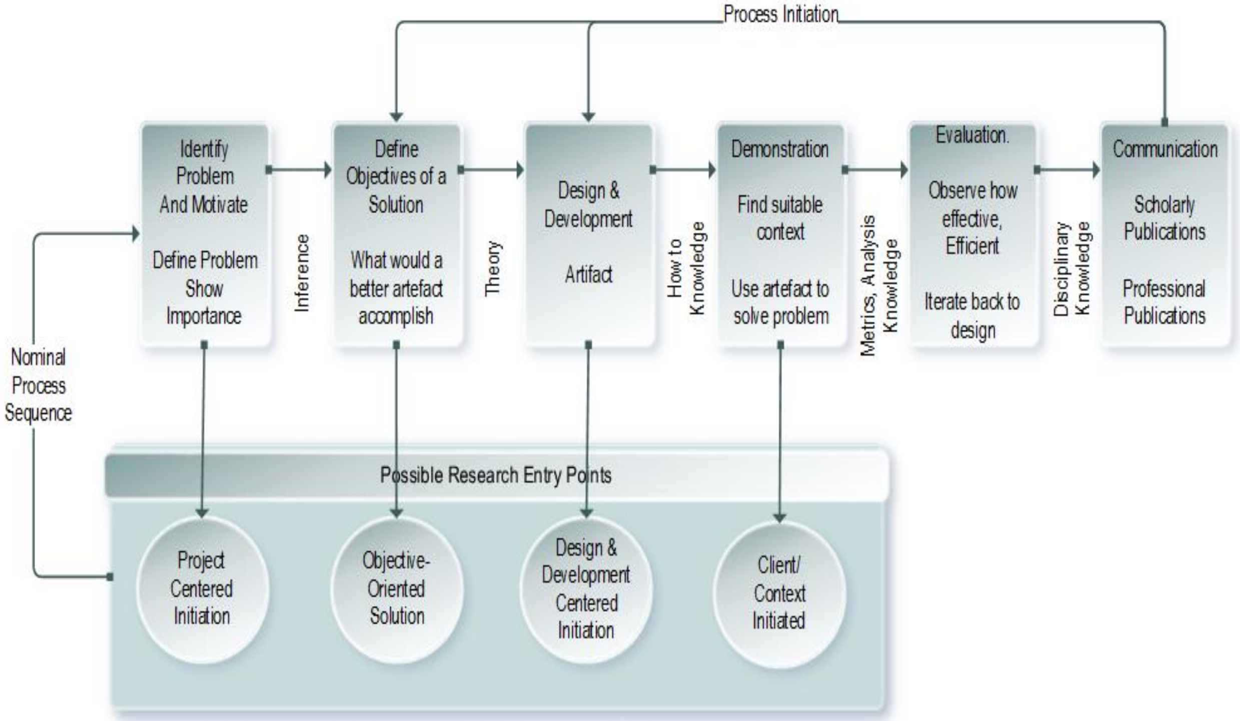

Process Initiation
Identify Problem And Motivate
Define Problem Show Importance
Inference
Define Objectives of a Solution
What would a better artefact accomplish
Theory
Design & Development
Artifact
How to Knowledge
Demonstration
Find suitable context
Use artefact to solve problem
Metrics, Analysis Knowledge
Evaluation.
Observe how effective, Efficient
Iterate back to design
Disciplinary Knowledge
Communication
Scholarly Publications
Professional Publications
Nominal Process Sequence
Possible Research Entry Points
Project Centered Initiation
Objective-Oriented Solution
Design & Development Centered Initiation
Client/ Context Initiated

Figure 7. Design Science Research Method Process

Source: Peffers et al. (2007)

Hevner et al. (2004) maintain that design science is a search process designed to discover an effective solution to a problem. In this study, the proposed model was developed based on the research questions formulated from the literature survey on organisational information security culture. The last guideline on the communication of results will be discussed in the next section.

2.6.7 Guideline 7: Communication of Research Results

This guideline concerns the manner in which the research will communicate the research findings. The results of this study will be published in journals and at conferences. Targeted audiences can be divided into technical and management audiences. Technical audiences require detailed specifications and explanations of the artefact, which they will implement in the relevant context. Management audiences, on the other hand, require high-level explanations of the solution with special emphasis on how the artefact solves the research problem in order to confirm that the solution is applicable and feasible. In order to ensure effective communication in this research, this will be managed as follows:

- Findings will be published in academic journals and at conferences.

- The complete dissertation will be made available at the Fort Hare University Library as well as on the Internet.
- Findings from this research will be presented to the commercial bank in Zimbabwe in order for it to implement an information security culture for the BYOD unintended administrator.

Given that the seven design science guidelines were followed, the fact that valid deductions were reached is reinforced.

2.7 Case Study Research

The empirical investigation performed in the current study took the form of a single case study on a commercial bank in Zimbabwe. While often criticised by the broader academic community for its inability to produce generalisable results, this form of research has been popular in Information Systems, with Chen and Hirschheim (2004) reporting that 36% of Information Systems studies adopted it between 1991 and 2005. Yin (2010) remarks that "a case study is an empirical enquiry that investigates a contemporary phenomenon within its real life context especially when the boundaries between phenomenon and context are not clearly evident" (p. 13).

A single exploratory case study approach was followed. The study produced an information security behavioural model based on the case of a commercial bank in Zimbabwe. Yin (2004) points out that "[t]he case study method is best applied when research addresses descriptive or explanatory questions and aims to produce a first-hand understanding of people and events" (p. 3). Firstly, a literature review was conducted on individual and organisational information security traits for the BYOD. This culminated in six constructs which were then used to formulate the research instrument. Six propositions were also formulated based on the traits. A survey was conducted on the 270 employees of the commercial bank on which the case study was conducted. These traits were then subjected to statistical testing, as discussed in Chapter 8. The results were subsequently combined to form the BISB model which is presented in detail in Chapter 7. There are ten departments in the bank where the study was conducted and an interview was conducted with each departmental head; this person is also a member of the executive management committee (EXCO). Additionally, an expert review process was also used to evaluate the model and the results of this process are presented in Chapter 9. The next section explores how the data collection process was conducted in this study.

2.8 Data Collection Methods

The step-by-step process flow diagram, presented in Figure 8, provides a summary of how the data collection was conducted. Initially, a questionnaire was created from the literature review process. This was then sent to the target audience via an email link. Feedback collected was then sorted and integrity checks conducted. The data was then analysed using SPSS and the results of the analysis are presented in Chapters 8 and 9.

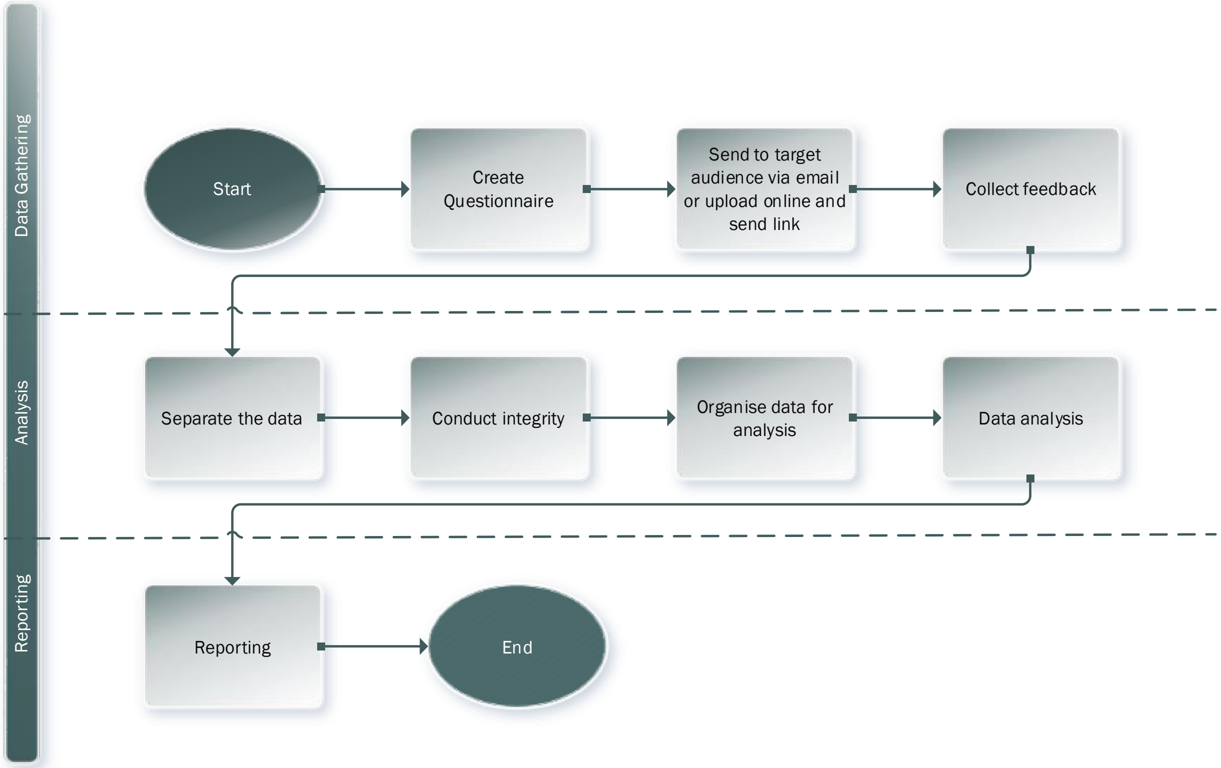


Figure 8. Data Collection Process Flow

Creswell and Clark (2011) suggest different types of mixed methods design, referred to as strategies of inquiry, to guide the choice of the type of mixed method to be used. These designs can be classified as either qualitative or quantitative and sequential or concurrent. The questionnaire was the main quantitative data collection method used while the qualitative data collection methods included a literature review, interviews and observations. The data collected pertained to the cultural constructs of behavioural intention, attitude, knowledge, habit, training, environment and governance. A mixed method approach design was used in this research study as this method gives a multidimensional and complete understanding of the issues under study.

Johnson and Onwuegbuzie (2004) explain that a mixed methods approach does not replace the quantitative or qualitative approaches but rather capitalises on the strengths of the two methodologies. Accordingly, two main issues were considered in the method design:

- ✓ Whether or not to operate in one dominant paradigm
- ✓ Whether or not to conduct the qualitative and quantitative phases concurrently or sequentially.

Johnson et al. (2007) recommend that, regardless of the mixed method design used, findings must be integrated at some point during the research process. A visual representation of the two considerations is contained in Figure 9

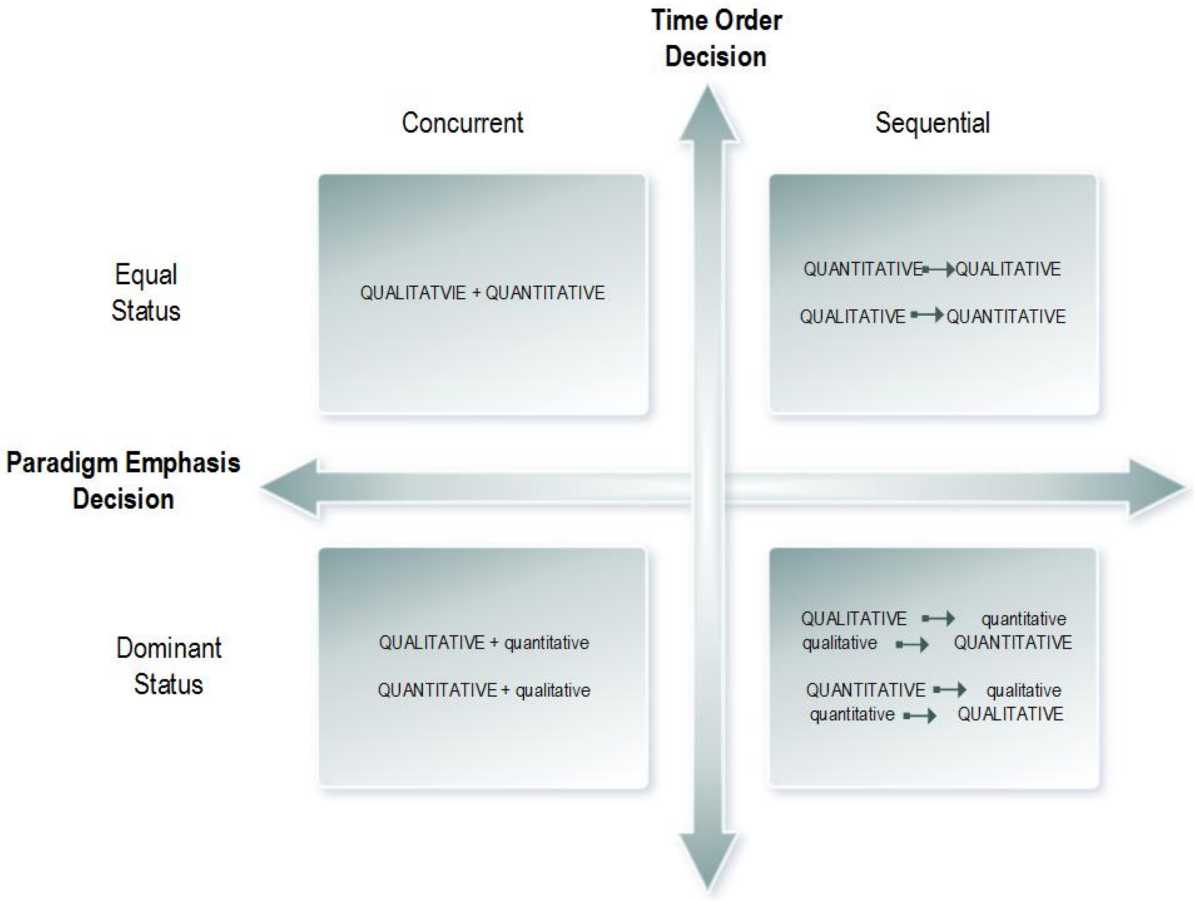

Time Order Decision
Concurrent
Sequential
Equal Status
QUALITATVIE + QUANTITATIVE
QUANTITATIVE → QUALITATIVE
QUALITATIVE → QUANTITATIVE
Paradigm Emphasis Decision
Dominant Status
QUALITATIVE + quantitative
QUANTITATIVE + qualitative
QUALITATIVE → quantitative
qualitative → QUANTITATIVE
QUANTITATIVE → qualitative
quantitative → QUALITATIVE

Figure 9. Mixed Method Design Matrix with Mixed-method Research Designs shown in the Four Cells

Source: Ionides (2002)

The data collection was conducted between September and October 2016. A questionnaire was designed based on the seven components of information security culture, making use of Likert scales as follows:

i. **Knowledge**. This component included questions to extract employees' literacy levels on the use of BYOD in the bank and comprised six questions which were added to the research instrument.

ii. **Attitude**. This component included questions aimed at understanding the employees' attitude towards information security; nine questions were developed and added to the research instrument.

iii. **Habit**. The questions covering this component were geared to understanding the employees' habits when using BYOD and four questions were developed and added to the questionnaire.

iv. **Training.** This component was meant to evaluate the need for training on information security; six questions were developed and added to the questionnaire.

v. **Environment**. This component addressed the macro environment of the organisation that the unintended administrator operates in. It also addressed what is acceptable in this regard, the acceptance or rejection of the BYOD phenomenon, as well as the controls and appetite for risk.

vi. **Governance**. This component measured the governance of the devices used; four questions were developed and made part of the research instrument.

vii. **Behavioural intention**. This component measured the employees' intention to follow BYOD policies and security standards; accordingly, five questions were developed and made part of the questionnaire.

The questionnaire was loaded on Survey Monkey and distributed to 270 employees in the bank. The results were collected and uploaded into SPSS for analysis. Chapter 8 of this document contains the data analysis and the findings emanating from the statistical calculations conducted. Figure 10 shows the process which was followed during the data collection process.

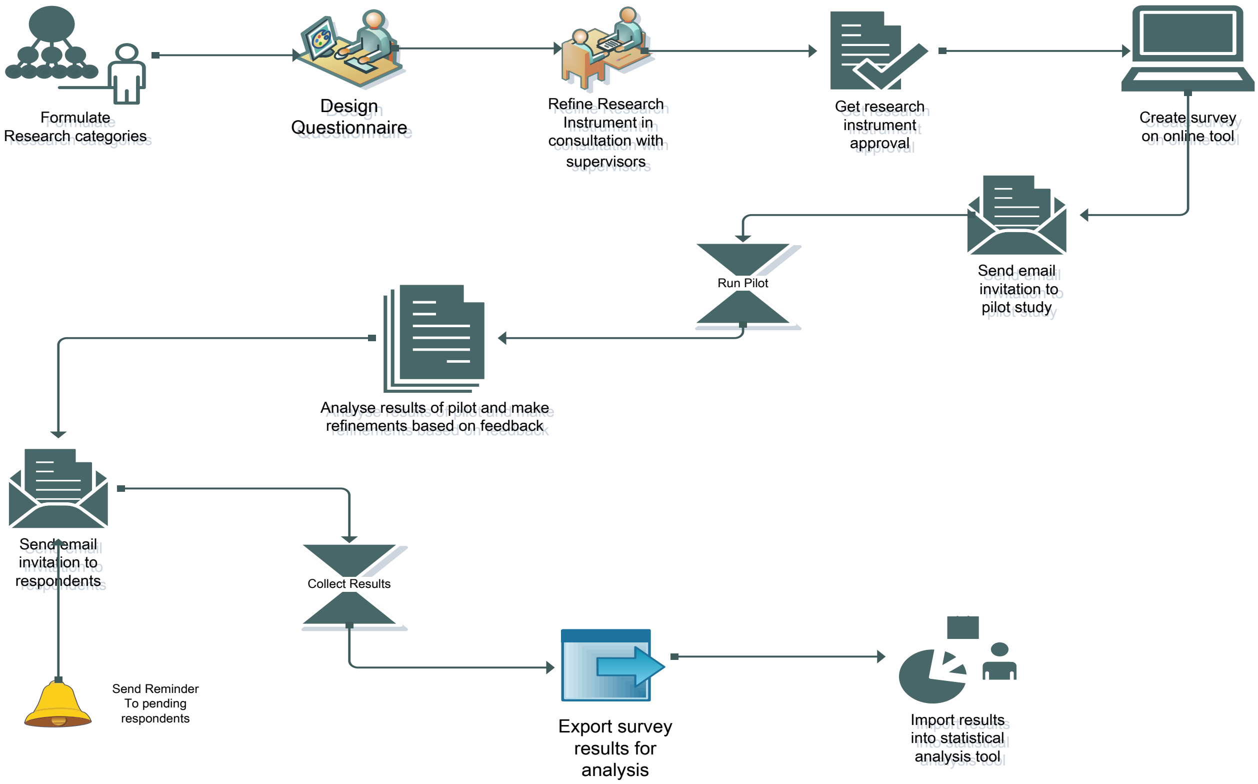

Formulate Research categories
Design Questionnaire
Refine Research Instrument in consultation with supervisors
Get research instrument approval
Create survey on online tool
Send email invitation to pilot study
Run Pilot
Analyse results of pilot and make refinements based on feedback
Send email invitation to respondents
Collect Results
Send Reminder To pending respondents
Export survey results for analysis
Import results into statistical analysis tool

Figure 10. Research Process

Initially, research categories were formulated based on the findings obtained from the literature review. This was then followed by the design of a questionnaire (see Appendix 1). The next section will discuss the primary and secondary data collection methods employed.

Data collection for this research was split into primary and secondary data collection. Primary data is collected to address a particular research question whilst secondary data is collected to address other research needs (Myers & Klein, 2011). Examples of secondary data sources include previously published materials such as books, articles and completed studies (Cooper & Schindler, 2003). In this study, the data collection methods employed were are discussed in the following sections:

2.8.1 Primary Data Collection Methods

The primary data collection process followed in this study consisted of four methods, which were applied at various stages of the study as follows:

- **Questionnaires.** The questionnaire was formulated on the basis of the traits obtained from the literature and was the main primary data collection method. The questionnaire was deployed using Survey Monkey.
- **Observations.** Observation made by the researcher during the research process complemented the primary data collection methods.
- **Interviews.** The interviews conducted during the research with the ten departmental heads in the bank also constituted primary data collection.
- **Expert review.** The survey conducted on the industry experts constituted the fourth method that was used for primary data collection in this study

2.8.2 Secondary Data Collection Methods

The literature review process conducted in this study formed the secondary data collection process followed in this study. This was done as follows:

- **Study of the theories.** A study of the relevant theories from the social sciences was carried out. This brought rigour to the overall study process especially as the literature was used to confirm the applicability of the individual constructs that influence the behavioural intention to implement an information security culture.
- **Prior studies.** Prior studies and case studies conducted in the banking sector were also cited in the study to bring context to the banking sector as well as application to the theories that were used.

Hofstee (2006) states that the infinite quantities of data available from various sources around the world on the rise daily has meant that the applicability of secondary data analysis is virtually endless. The data collection process for this research study is addressed under Guideline 6, which discusses design as a search process. The data collection method outlined in Figure 11 started with the literature review and culminated in the formulation of the research instrument.

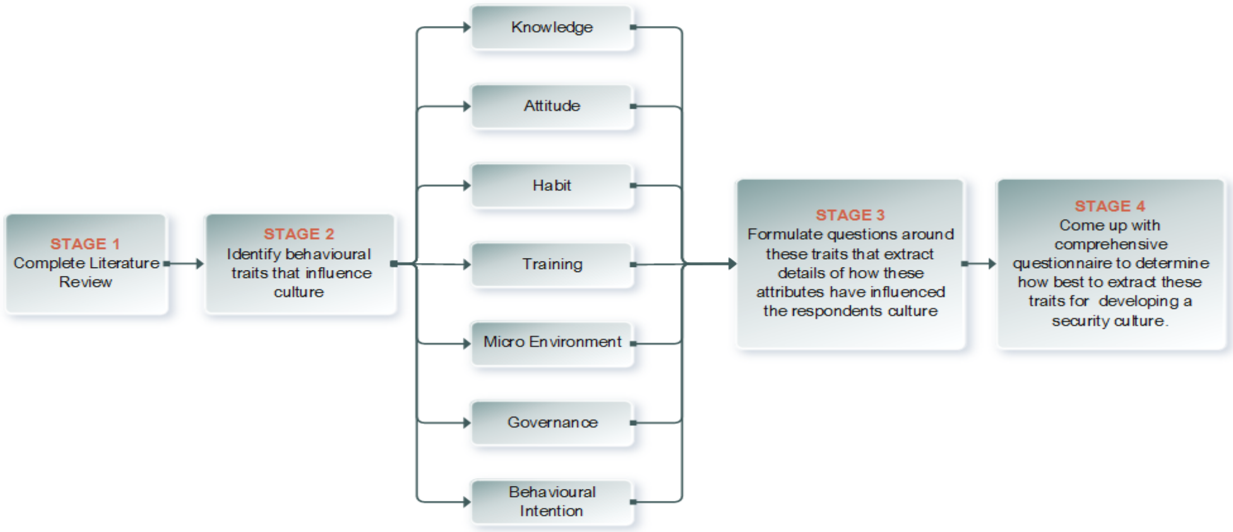

STAGE 1
Complete Literature Review
STAGE 2
Identify behavioural traits that influence culture
Knowledge
Attitude
Habit
Training
Micro Environment
Governance
Behavioural Intention
STAGE 3
Formulate questions around these traits that extract details of how these attributes have influenced the respondents culture
STAGE 4
Come up with comprehensive questionnaire to determine how best to extract these traits for developing a security culture.

Figure 11. Primary Data Collection Process Flow

Figure 12 illustrates the questionnaire formulation process flow based on the constructs of knowledge, attitude, habit, governance, behavioural intention, environment and training. Following the collection of this data, semi-structured interviews were conducted with divisional heads in the bank with the aim of understanding the departmental application of information security. As discussed earlier in this chapter, there are ten departments in the bank where the study was conducted. Each department has a divisional head who is a member of the executive management committee (EXCO). These departments include Finance, Marketing, Human Resources, Information Technology, Audit, Marketing, Retail Banking, Wholesale Banking, Risk and Business Development. Semi-structured interviews were conducted with these divisional heads to understand the information security culture for these divisions based on the seven factors used in to formulate the questionnaires. The ten departments use BYOD at various levels depending on their role profiles. Questionnaires formed the primary data collection method while the literature review informed the questions which were formulated to collect the secondary data. These questionnaires contain both qualitative and quantitative sections, which then resulted in the use of a mixed method approach for data analysis. The questions were based on the individual and organisational traits obtained identified by the literature review.

This study took the form of a case study for a selected bank in Zimbabwe. The study population was composed of bank employees who use mobile computing devices to do their work but did not consider laptops. The question design format included Likert-type scales, and ‘yes’ or ‘no’ questions ranked so as to obtain targeted output on the BYOD phenomenon.

2.9 Data Analysis Methods

Following data collection, the next step was to analyse the data so as to make deductions and conclusions. Tharenou, Donohue, and Cooper (2007) caution that it is important to use appropriate data analysis techniques. The first stage of qualitative data analysis involves processing the collected data using coding, editing, tabulation and classification (Cooper & Schindler, 2003; Leedy & Ormrod, 2010). The questionnaire was the main research instrument used in this study and the collected data was exported to SPSS.

Lichtman (2014) warns that data analysis is the least understood and most complex qualitative process, whose complexity lies in the pursuit of the “right concepts” or in the realisation that some findings are more superior than others. Lichtman (2014) adds that researchers should rid themselves of the notion that one data set is more significant than another. There is no right or wrong answer in qualitative research as there are only acceptable explanations of the phenomena based on the researcher’s experience. Combining various approaches increases the relevance of an analysis through a trade-off in strengths and weakness in either of the data sets (Pelino et al., 2014). Descriptive statistics were used for analysing and presenting that data, as presented in Chapter 8.

SPSS was used to make relevant statistical conclusions on the quantitative data. The analysis processed included summarising the collected data by inspecting the existing relationships between the constructs, as well as determining the elements to be isolated for the research (Leedy & Ormrod, 2010). Reliability and validity for the questions were achieved by means of Cronbach’s alpha coefficients for the factors. The relationships between the factors that may influence the BISB model for the unintended administrator were checked using factor analysis. In addition, multivariate statistical descriptive measures were used to describe and present the results.

The research artefact, that is, a model for building an information security culture for the BYOD unintended administrator, was formulated from the information obtained from the data analysis. The findings of the data analysis are discussed in Chapter 8 (Analysis and Findings). The next section will discuss the evaluation of the research project to improve the credibility of the research.

2.10 Research Evaluation

Hevner et al. (2004) proffer the option that a research artefact can be evaluated on the basis of components like functionality, completeness, consistency, accuracy, performance, usability, reliability, best fit and many other parameters. Evaluation can be done in the form of case studies, field studies, statistical analysis, architectural analysis, optimisation, dynamic analysis, controlled experiments, simulation, structural testing or even functional testing (Peffers et al., 2010). Theoretical propositions and research hypotheses are also appropriate research evaluation techniques that are of particular interest to this study.

- **Theoretical propositions**. These form the framework or the structure that can hold or support a theory from a research study. The theoretical proposition also helps to predict, explain and appreciate phenomena or to challenge and extend existing understanding within the limits of the critical underlying assumptions of the particular subject under study. Detailed application of the theoretical proposition process is discussed in Chapters 8 and 9.
- **Research hypotheses**. A hypothesis is the research statement generated by researchers to try and speculate on the result of a research or an investigation. The research hypothesis can either be a null hypothesis (H_0) or alternative hypothesis (H_1).

This research makes use of theoretical propositions to evaluate the traits obtained from the literature review, which were then used as constructs for the model. The theoretical propositions were also instrumental in the evaluation of the research artefact together with the expert review process conducted. The next section explores the evaluation of the expert review process.

2.11 Expert Reviews

In order to evaluate the integrity of this study, the factors in Table 5 were evaluated. In Zimbabwe, there is a Bankers Association of Zimbabwe (BAZ) committee that is made up of all banks. The main committee is run by the chief executive officers of the various banks. There are also other subcommittees that focus on important areas such as treasury, IT, operations as well as many other banking arms. The Bankers Association of Zimbabwe (BAZ) Chief Information Officers (CIOs) Forum is one such subcommittee that deliberates on IT issues for the banks in Zimbabwe. The BISB model was presented to the BAZ CIO Forum using a guided set of questions leading to the evaluation process for the model (see Appendix 6).

Experts have a deeper level of understanding on the information security challenges caused by the BYOD unintended administrator as compared to individuals who are not experts in the area (Johnson, 2013). Section 9.5.1 examines the expert review approach followed in detail. Fifteen questions were formulated and shared with eighteen CIOs and, of these, sixteen CIOs participated in the evaluation process. The results obtained will be discussed in detail in this chapter, forming the basis for the evaluation process for the BISB model. As stated in section 2.2.5 of this chapter, this study follows Hevner et al.'s (2004) design science guidelines. In order to contextualise the evaluation process, the next section establishes the link between evaluation processes and the design science paradigm by placing it under guideline number three.

Table 5. Evaluation of Interpretivist Research

Evaluating Criteria	Definition	Application in this Study
Trustworthiness	This addresses the accuracy of the collected data	The questionnaire was created using verified literature from questionnaires found in the literature review on the seven constructs. The collected data was cleaned and verified. Peer reviews and expert reviews were used to review the artefact. The questionnaire was sent to peers and experts as a pilot study to verify the relevance and validity of the questions to be sent out.
Confirmability	The degree to which the results may be confirmed or corroborated by others .Capability of tests by experiment or observation so as to be either verified or falsified	Statistical data collection techniques were used to create the artefact in this research project. Semi-structured interviews, a literature review and the researcher's field notes from observations and interviews with EXCO heads of the various bank divisions were used.
Dependability	The chances of producing the same result if the study were replicated	The use of well-known, established theories and models that have been tested in numerous research projects contributed to the reliability of this project.
Credibility	The accuracy of the results reflecting the social phenomena under observation	The case study was carefully selected to meet the requirements of building an organisational information security culture. Mixed methods research with the use of questionnaires, semi-

		structured interviews and the researcher’s field notes from the interviews, as well as observations and expert review process was employed
Transferability	Degree of applicability in other environments or institutions	The characteristics of case studies were observed and the seven constructs were backed by theories from the human sciences.

The ethical considerations taken into account will be discussed in the next section.

2.12 Ethical Issues

Punch (2006) cautions that academic integrity and honesty, as well as respect for other people, are the researcher’s prerogatives. Saunders et al. (2009) maintain that research consists of stakeholders who participate in teamwork, therefore there is a need to ensure that no stakeholder is negatively affected. The following were observed as a way of ensuring that ethical principles were fully observed:

- ✓ Approval from the University of Fort Hare Research and Ethics Committee (UREC) was granted under certificate reference number FLO061SMUS01 (attached in Appendix 2).
- ✓ Written permission to conduct the study was obtained from the bank (see Appendix 3).
- ✓ The participants were fully informed about the purpose of the study as well as any issues, benefits and risks that might arise from the study.
- ✓ All participants were made aware that the researcher would use the information provided for academic purposes only and were instructed to report any issues to the correct authorities first and then to call the number provided on the consent form .
- ✓ The confidentiality of the participants and of the information provided was assured.
- ✓ The raw data was securely stored and proper access control measures were put in place.

The researcher was aware of the above ethical considerations, and all reasonable efforts were made to conduct the research project without malice or prejudice to the respondents and to present the findings and conclusions honestly. The parties involved signed confidentiality agreements before the study commenced. Terms and conditions were communicated and made available before and during the study and were put on the online portal. The questionnaires were distributed by various electronic means with email being the main one. Where necessary, hard copies were also made available to the participant for signing. The option to decline to participate was also made available to the participant to ensure that consent was given freely.

2.13 Conclusion

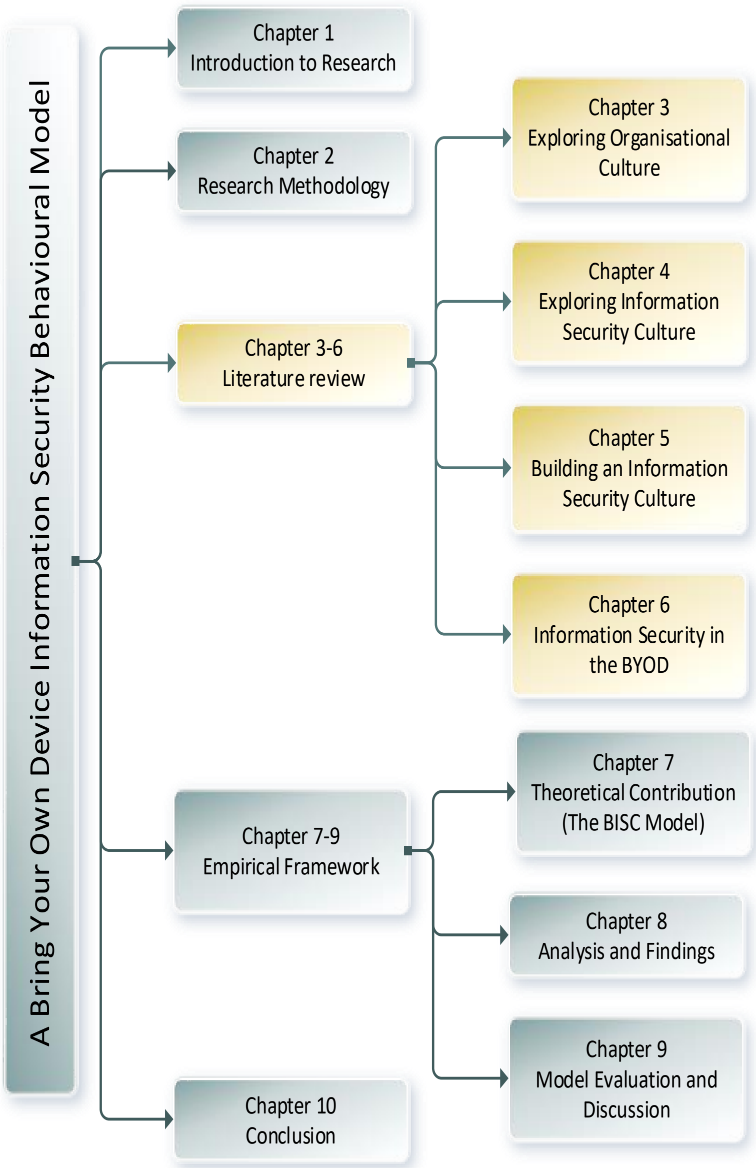
This chapter explored the research methodology followed in this study. The design science research paradigm was selected for this research study and the seven guidelines presented by Hevner et al. (2004) were followed in no particular order for the creation of the research artefact for this study. The research outcome, namely, the BISB model, will be discussed at length in Chapter 7. Design science research allows for mixed methods to analyse the data. An inductive research approach was adopted for this study. The researcher began the research project through a literature search which constituted the secondary data collection process for this study. Secondary data collection included a literature review of relevant theories and prior studies on information security behavioural traits in organisations, which were subsequently applied to the BYOD.

The statement of the problem the formed the focus of this study was based on a specific research question and four sub-questions which summed up the research questions discussed in section 1.3 of Chapter 1. The primary data collection method for this research study comprised a questionnaire which was based on the findings of the literature review (i.e. the secondary data collection method). Notes made by the researcher on observations made during the fieldwork, as well as the semi-structured interviews with the heads of departments of the commercial bank, also formed part the primary data collection methodology. During the model evaluation process, the expert review constituted the other primary data collection method.

Six constructs were obtained from the literature study and used to formulate research propositions for the study. The constructs include attitude, knowledge, training, governance, environment, and habit. Chapter 7 discusses the constructs in detail culminating in the model. A questionnaire was created in Survey Monkey using these seven constructs and was sent to employees in the bank via an email link. The data collected was processed and loaded into SPSS for multivariate analysis. Factor analysis was used to examine the factors (which can be referred to as constructs). Reliability was tested using the Cronbach's alpha test. Other descriptive statistical tests were also used to support the research findings. Detailed data analysis tests conducted for this research are described in Chapter 8. The next section will discuss the literature study carried out which culminated in the research instruments for this study.

Literature Review

A theoretical foundation of the study on how an organisation can build an information security culture


A Bring Your Own Device Information Security Behavioural Model
Chapter 1
Introduction to Research
Chapter 2
Research Methodology
Chapter 3-6
Literature review
Chapter 3
Exploring Organisational Culture
Chapter 4
Exploring Information Security Culture
Chapter 5
Building an Information Security Culture
Chapter 6
Information Security in the BYOD
Chapter 7-9
Empirical Framework
Chapter 7
Theoretical Contribution (The BISC Model)
Chapter 8
Analysis and Findings
Chapter 9
Model Evaluation and Discussion
Chapter 10
Conclusion

Overview of the Literature Review

The consumerisation of information technology (IT) through enterprise mobility has changed the way organisations manage their IT. Technology-driven solutions have been developed to manage various BYODs in organisations. Since employee-owned mobile devices now carry information that in the past was confined to the organisational network boundaries, an organisation's information security culture can no longer be ignored (Alhogail, 2015). Organisations now need to take formative steps toward building a culture where every employee takes personal responsibility for the security of information on any device they own that has access to the corporate network (Alfawaz, Nelson, & Mohannak, 2010). This study seeks to establish ways in which organisations can build an information security culture to mitigate the risks posed by the BYOD unintended administrator. To ascertain how the BYOD unintended administrator can be secured against information security risk, a case study of a bank in Zimbabwe, a developing country in southern Africa, was carried out. Since banks are generally associated with a very low-risk appetite Thakor(2015), remarked that information security is an important area of focus in the banking industry, with banks being compelled to be actively involved in information security trends and requirements. In order to achieve this goal a literature review was conducted which will be discussed in Chapters 3 to 6 with the following objectives:

- To understand the difference between organisational culture and information security culture
- To understand information security culture and how it can be created within Zimbabwe's banks
- To identify critical success factors and constructs for building an information security culture in an organisation
- To build an information security culture model around the BYOD unintended administrator
- To help banks in mitigating the risks posed by the BYOD unintended administrator.

Social scientists have proposed a number of theories through which to rigorously examine the processes by which a culture can be created in an organisation. These theories portray various viewpoints on building a culture for the BYOD unintended administrator in a banking organisation. The detailed explanation on how these theories work will be given in the sections and chapters of the literature review. These theories are as follows:

i. Schein's theory on organisational culture (Chapter 3)
ii. Hofstede's theory (Chapter 3)
iii. Denison's theory (Chapter 3)

iv. Ajzen’s theory of planned behaviour(TPB) (chapter 4)

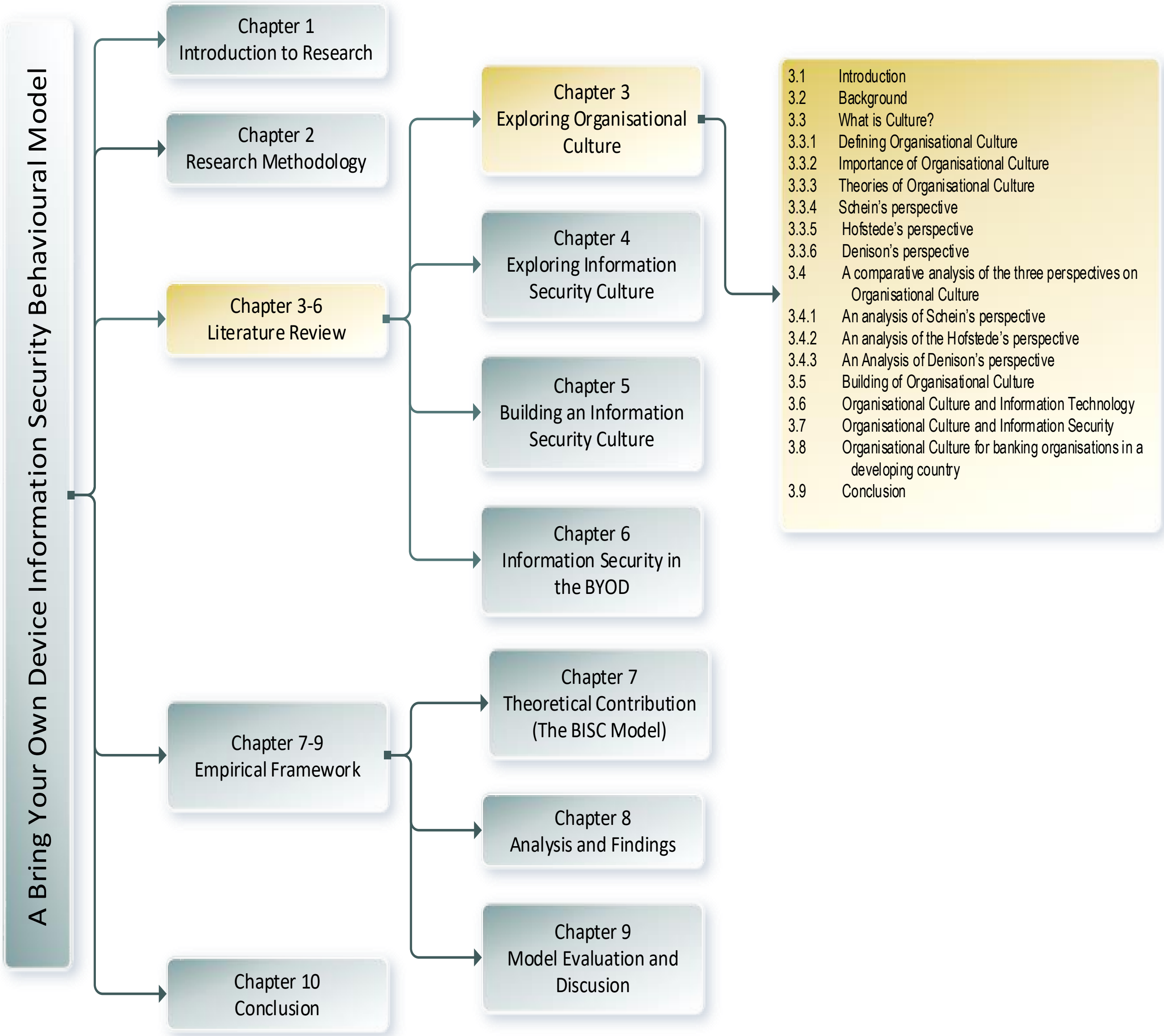
v. Ajzen’s theory of reason action (TRA) (Chapter 4)

vi. General systems theory (GST) (Chapter 1).

These theories address different aspects of how culture is developed in organisations. The main theories used in this study are Schein’s organisational culture theory, Hofstede’s theory, Denison’s theory, TRA and the TPB. The GST is not a prominent theory in this study as it was used sparingly to establish the links between the various perspectives contained in the other theories. To achieve these objectives, the literature is organised in such a way that Chapter 3 explores organisational culture, Chapter 4 explores information security culture, and the concluding literature review chapters, Chapters 5 and 6, address ways of building an information security culture as well as an information security culture with regard to BYOD.

Chapter 3 : Exploring Organisational Culture

"Culture is considered the glue that holds an organisation together and for others, the compass that provides directions." Bruce Tharp


A Bring Your Own Device Information Security Behavioural Model
Chapter 1
Introduction to Research
Chapter 2
Research Methodology
Chapter 3-6
Literature Review
Chapter 7-9
Empirical Framework
Chapter 10
Conclusion
Chapter 3
Exploring Organisational Culture
Chapter 4
Exploring Information Security Culture
Chapter 5
Building an Information Security Culture
Chapter 6
Information Security in the BYOD
Chapter 7
Theoretical Contribution (The BISC Model)
Chapter 8
Analysis and Findings
Chapter 9
Model Evaluation and Discusion
3.1 Introduction
3.2 Background
3.3 What is Culture?
3.3.1 Defining Organisational Culture
3.3.2 Importance of Organisational Culture
3.3.3 Theories of Organisational Culture
3.3.4 Schein's perspective
3.3.5 Hofstede's perspective
3.3.6 Denison's perspective
3.4 A comparative analysis of the three perspectives on Organisational Culture
3.4.1 An analysis of Schein's perspective
3.4.2 An analysis of the Hofstede's perspective
3.4.3 An Analysis of Denison's perspective
3.5 Building of Organisational Culture
3.6 Organisational Culture and Information Technology
3.7 Organisational Culture and Information Security
3.8 Organisational Culture for banking organisations in a developing country
3.9 Conclusion

3.1 Introduction

Information security culture (ISC) is situated as a subculture of organisational culture (OC) and thus OC cannot be ignored when building an ISC (Al Hogail, 2015). Several researchers and academics have agreed that while technology and policy are the key pillars of organisational security, they require culture as the central pillar. Regulation provides a mandatory way of implementing a standard, whilst a culture will promote an awareness of information security human behaviour that is driven by employees' willpower, belief and self-determination (Alhogail & Mirza, 2014). Zakaria, Gani, Nor, and Anuar (2007) call this a "human firewall" safeguarding organisational assets. To ensure that adequate and relevant checks and balances are identified and implemented in a successfully manner the OC should be the basis for an ISC (Da Veiga & Eloff, 2010).

This chapter explores the way OC is built in an organisation with a special focus on banks. A literature review of theories from the social sciences that explain OC concepts and characteristics will be used to underpin the relationship between OC and ISC. The chapter concludes by establishing the importance of OC in relation to information security. This relationship introduces certain critical success factors when building an ISC.

3.2 Background

Every organisation is defined by its unique culture which is deeply rooted in the nature of its business, history, leadership and even geographical location. In corporate organisations OC is also referred to as corporate culture. OC is the basis of the brand and performance for the particular organisation (Schuman, 2006). Studies conducted by Zakari, Poku, and Owusu-Ansah (2013) on the banking industry in Ghana showed that the relationship between OC and performance has engaged the attention of players in that industry. When it comes to issues around organisational security, one cannot ignore the employees as they play a vital role in implementing the culture of the organisation; employees form the first line of defence when implementing or managing security in an organisation (Al Hogail, 2015).

The establishment of an ISC is achieved by building relevant information security beliefs and values that guide employee behaviour in regard to IT and systems (AlHogail, 2015). The culture of an organisation is defined by the collective behaviours displayed by the employees. Matsumoto (2007) maintains that culturally dependent social roles and individual role identities define the individual behaviour which will then be transferred into the organisations. Robbins et al. (2009) confirm that organisational behaviour is what people do in an organisation and how their behaviour affects the organisation's performance. Setting up an ISC for an organisation may result in transforming employees' behaviour towards IT (Alhogail & Mirza, 2014). However, this process may be faced with resistance, misunderstanding or confusion if proper change management is not followed.

Organisations need to create an environment where security is everyone's responsibility. Zakaria et al. (2007) posit that a good ISC can act like a "human firewall", protecting information assets. This suggests that an organisation's security is as good as its people. Whilst technical security systems may be in place, the effectiveness of these systems is only as good as the people who are using, observing and implementing them. An ISC in an organisation will be faced with many behavioural issues that put information security at risk (Dojkovski, Lichtenstein, & Warren, 2010). From the literature on this topic, it is evident that change is always faced with resistance as it affects the status quo. It can be concluded that the easiest way to implement change in organisations is first to address the human needs.

In order to understand OC, one needs to understand how the organisation is built. The next section will define culture in the context of technology, after which the levels of OC will be examined. To provide academic rigour within the definitions, we will study the existing theories on OC and conclude by establishing the relationship between OC and culture ISC towards technology.

3.3 What is Culture?

Culture is viewed as "the collective programing of the human mind that distinguishes the members of one human group from those of another" (Finch, 2009, p. 3). The study of culture has been carried out in various disciplines leading to several definitions, dimensions and conceptualisations (Connolly & Lang, 2012). Ali and Brooks (2009) argue that the study of culture is deeply rooted in anthropology, social psychology and sociology. However, anthropology provides a more specific and applied understanding of culture which is applicable to organisational research (Tharp, 2009). Tharp (2009) argues that culture is centred on three basic human activities: what people think, what people do, and what people make. He also suggests that culture is unique to a people and it can be learnt actively or passively and be transmitted from one person to the next either formally or informally (Tharp, 2009). Culture is affected by various responses and influences as well as circumstances that characterise a particular society. This suggests that culture is dynamic, therefore it is imperative to identify the undercurrents of culture. In organisations, the culture is often derived from the strategy, the environment as well as the mission and the vision of the organisation and permeates the entire organisation (Davidson, Coetzee, & Visser, 2007).

Ozigbo (2013) states that humans are social beings who have demonstrated the tendency to group together in communities in order to survive. Accordingly, an OC is at the core of the survival of every organisation such that understanding culture in organisations is fundamental to the description and analysis of organisational operations. When an organisation is formed, this ability to stay together is controlled by a certain set of habits, attitudes and behaviours towards each other, as well as the nature of the organisation and the ways in which day-to-day results are obtained. Subsequently, IT has pervaded organisations, demanding a shift in the culture for organisations from various touch points (Kaufman, 2014). BYOD is one of the technologies which has influenced the entire OC. In order to have a broader view of culture in the context of organisations, the next section will explore culture as applied to organisations, and this will direct the discussion towards the creation of a culture on information security.

3.3.1 Defining Organisational Culture

OC is a widely documented topic whose definitions are published in various contexts and industries. In the banking industry, OC is viewed as the shared beliefs and values that develop within the banking organisation. These guide the behaviours of its members to maintain suitable patterns of social systems to form a coordinated behaviour in order to survive in the dynamic environment (Denison, Janovics, & Young, 2006). Schein (2004) defines OC as "[a] pattern of shared basic assumptions that a group learns as it solves its problems of external adaptation and internal integration that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think and feel in relation to those problems" (p. 17). Another definition by Lundy and Cowling (1996) views OC as the way things are done in a particular organisation. This definition provides a casual but practical description of culture without necessarily providing an understanding of culture.

In the context of IT, the study of OC is key as it explains how people behave in relation to technology. OC provides meanings for routine organisational events, thereby reducing the amount of cognitive processing members need to expend in understanding certain behaviours (Matsumoto, 2007). The culture of an organisation is something that can have an enormous impact both on the way in which an organisation operates and its effectiveness. It is also something that can be assessed and, if necessary, changed over time. OC interventions are known for their difficulty and duration. Van Niekerk and Von Solms (2010) argue that OC is unique to each organisation based on some omnipresent assumptions that are often not easy to unpack. They further assert that these assumptions direct the activities in an organisation and are often shared by the people in it (Van

Niekerk & Von Solms, 2010). Academic and applied exploration of OC has gained attention from many researchers as it provides a basis for understanding how any given organisation operates.

According to Von Roessing (2010), OC results from the pattern formed from the pervading beliefs, attitudes, assumptions, and behaviours. Von Roessing (2010) further suggests that the key to culture in any organisation is enshrined in its employees, as employees' perceptions are created by the organisation's culture. These perceptions are usually based on internal organisational aspects such as compensation, recognition, promotion prospects and other managerial policies. The perceptions are also driven by factors outside the organisation, such as religion, ethnicity, socioeconomic background, geographic location and personal history. These external factors that may not appear to have much impact on day-to-day operations manifest themselves in behaviours brought to the workplace and are often much more important than expected since they form grounds for workplace behaviours and norms.

Waisfisz (2010) defines OC as the way in which members of an organisation relate to each other, to their work, as well as the outside world, and which distinguishes them from other organisations. Technological innovations in the area of enterprise mobility continue to affect the relationship between organisations, workers and the workplaces, including the way in which information security is managed. In order to unpack this new technology trend, it is important first to examine OC. To confirm the way OC is built, theories from the social sciences on how cultures can be built were applied. From these social sciences constructs, the culture developmental steps towards technology were followed to develop a way for building an OC around information security. The next section will address how theories will underpin the OC.

3.3.2 Importance of Organisational Culture

In most organisations, OC is an integral management control tool. Employees in an organisation are governed by policies and standards which all emanate from the OC (Lim et al., 2009). Such policies enforce the way in which standards and values in a particular organisation are upheld. These policies are rooted in the organisational strategic focus as well as in the OC and either positively or negatively influence the performance of a business. Singh and Phil (2012) believe that in this era of massive technological innovation, a culture that embraces technology will benefit the organisation whilst a technology-averse culture can result in the organisation losing out to the competition.

OC can offer a shared system of meanings, which forms the basis of communication and mutual understanding among its employees. From the literature, it is evident that OC forms an integral part of any organisation as well as its employees' well-being. Sun (2008) expands this view by stating that OC determines the functions of the organisation as well as its processes. The function of OC manifests in the creation of a feeling of identity and belonging among employees. This creates commitment to the organisation, allowing the creation of a competitive edge to enable the members in the organisation to appreciate acceptable behaviour and social system stability (Martins & Terblanche, 2003).

Human beings have a natural sense of belonging which is espoused in their cultural identity and values. OC gives meaning to these values thereby ensuring a sense of belonging. For organisations to achieve their visions and missions, they indirectly create the culture that promotes them (Martins & Terblanche, 2003). Based on the conclusion that OC is the way employees live together in an organisation, it is almost certain that the way in which an organisation chooses its IT as well as the information security standards is centred on its culture. Additionally, culture can have an influence on employee motivation; morale and goodwill; productivity and efficiency; the quality of work; innovation and creativity, and attitude (Campbell, Stonehouse, & Houston, 2002). OC, however, is more than just an internal phenomenon; a company's culture is often felt outside of its own four walls. In this way, culture becomes an integral part of a company's brand. In order to understand the application of culture as a pivotal organisational component, it is important to understand the theories that support it. The next section addresses theories of OC with a view to ascertaining how the unintended administrator is affected or influenced.

3.3.3 Theories of Organisational Culture

In academic research, theories present a systematic view of phenomena by specifying relations among variables using a set of interrelated constructs, variables, definitions and propositions (Lunenburg, 2011). In this research, theories of OC help in understanding organisations through a cultural lens with a focus on the values, attitudes and beliefs of their members.

In building an OC there is a need to consider employee behaviour and attitudes in relation to the different levels of rank and authority, as well as their influence on the overall operation of the organisation (Robbins et al., 2009). The extent of acceptance of the culture in an organisation is usually set by the top management and is cascaded down the hierarchy, with the employees' attitudes and behaviours determining the uptake in either a positive or negative way. In order to have a clear understanding of OC, we will investigate the following three theories which address behavioural and classification aspects of culture:

i. Schein's theory of organisational culture
ii. Hofstede's theory of organisational culture
iii. Denison's theory of organisational culture

The next chapter will discuss ISC and how it can be built. This will be based on the OC, bearing in mind that ISC is a subculture of OC.

3.3.4 Schein's Perspective

Schein (1990) is one of the most influential authors on OC. He argues that OC may be analysed on three separate levels, namely, artefacts, espoused values, and basic underlying assumptions. The three levels are separated on the basis of the degree to which the cultural phenomenon is visible to the observer. In order to understand OC from Schein's perspective, we will look at the proposed levels in detail. The ultimate view is to apply the perspective to banks in securing the BYOD unintended administrator by means of building an ISC:

- **Level 1 – Artefacts.** This level addresses the visible and tangible organisational structures and processes shared by the members of the organisation. It consists of aspects that are easy to observe and difficult to construe. These aspects include the type of colours associated with the organisation's branding and the ambience of the premises. In the context of this study, this level also includes the device brands used, for instance Apple, Lenovo, Dell and so forth. This level does not, however, provide explanations as to why employees choose certain brands or behave in a certain way. These factors will then be explained by the espoused values that look at culture at a deeper level.

- **Level 2 – Espoused values.** Schein (1990) suggests that the reasons for the employee to consider observed artefacts lie in the espoused values as they constitute the organisation's vision, mission and strategy. This is the organisation's official viewpoint, the base from which the organisation's operations are driven. The culture of the organisation is thus determined by the tacit assumptions shared by the organisation and the employee . In the context of this study, in building a culture this level is useful for employees to learn the values of the organisation.

- **Level 3 – Shared tacit assumptions**. Certain proven strategies result in assumptions developing about an organisation and these are found at the deepest level of OC. These assumptions form the basis or the premise for OC formulation. The success of these strategies in relation to specific behaviours, values and beliefs result in them being taken for granted and the OC will eventually emerge from the successful beliefs and cultures. Shared tacit assumptions include aspects like the type of strategies that the organisations implement to meet their strategic focus and how the members of the organisations think about themselves, and the nature of organisations in relation to each other and the world.

Figure 12 shows the relationship that exists between the three levels as postulated in the model proposed by Schein.

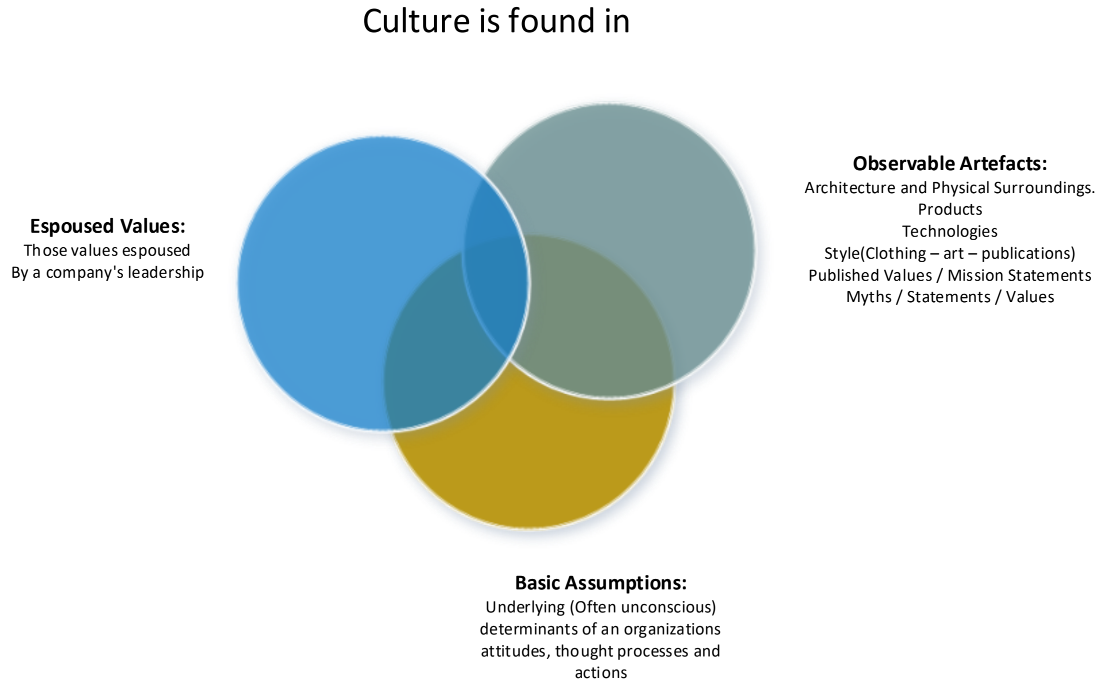

Culture is found in
Espoused Values:
Those values espoused
By a company's leadership
Observable Artefacts:
Architecture and Physical Surroundings.
Products
Technologies
Style(Clothing – art – publications)
Published Values / Mission Statements
Myths / Statements / Values
Basic Assumptions:
Underlying (Often unconscious)
determinants of an organizations
attitudes, thought processes and
actions

Figure 12. Levels of Organisational Culture

Source: Schein (2004)

Schein's perspective on OC provides a basis for researchers to identify the specific attributes of a culture in the behaviour and belief system in an organisation. However, Schein's perspective merely illustrates where OC is premised without providing the existing types of OC or the way in which the various cultures correlate within the organisation (Liu, Kiley, & Ballard, 2006). Schein's model confirms the importance of behaviour and attitude in the OC. McGrath (2003) states that the three levels of artefacts, espoused values and shared tacit assumptions all appeal to employee behaviour in some way and this will influence how the employee fits within the OC. Hofstede's model, explored in the next section, addresses the gap relating to the existence of various organisational types by classifying OC into six types.

3.3.5 Hofstede's perspective

Hofstede (2011) carried out studies on national culture, which later extended to OC, in which he analysed the perspective of value and practice. Hofstede (2010) introduced the "onion diagram" which manifests cultural differences in the form of the following four levels (Waisfisz, 2010):

- **Symbols.** These contain a particular meaning only recognised and shared by those who share the culture. They are in the form of gestures, words, objects, language, jargon, dress, and hairstyles. It is possible to develop new symbols to replace the old ones.
- **Heroes**. This refers to those persons, alive or dead, real or imaginary, who possess characteristics that are highly valued in a culture, and who serve as models for behaviour.
- **Rituals.** These are collective activities, technically superfluous in reaching desired ends but which within a culture are considered socially essential, and are therefore carried out for their own sake. Examples of these types of activities include ways of greeting and paying respect to others and social and religious ceremonies.
- **Values.** These are broad tendencies to prefer certain states of affairs over others. Values are among the first things children learn not consciously but implicitly. Because they are acquired so early in life, many values remain subconscious to those who hold them. Therefore, they cannot be discussed nor can outsiders directly observe them. They can only be inferred from the way people act under various circumstances.

Hofstede, Neuijen, Ohayv, and Sanders (1990) argue that there are shared perceptions among employees on the daily practices that form the core of an organisation's culture. They also point out that, while practices are the visible part of an organisation's culture, values are the invisible part. According to this perspective, OC is defined as the way in which members of an organisation relate to each other, their work and the outside world in comparison to other organisations. Figure 13 shows the different levels of culture in Hofstede's (2010) onion diagram.

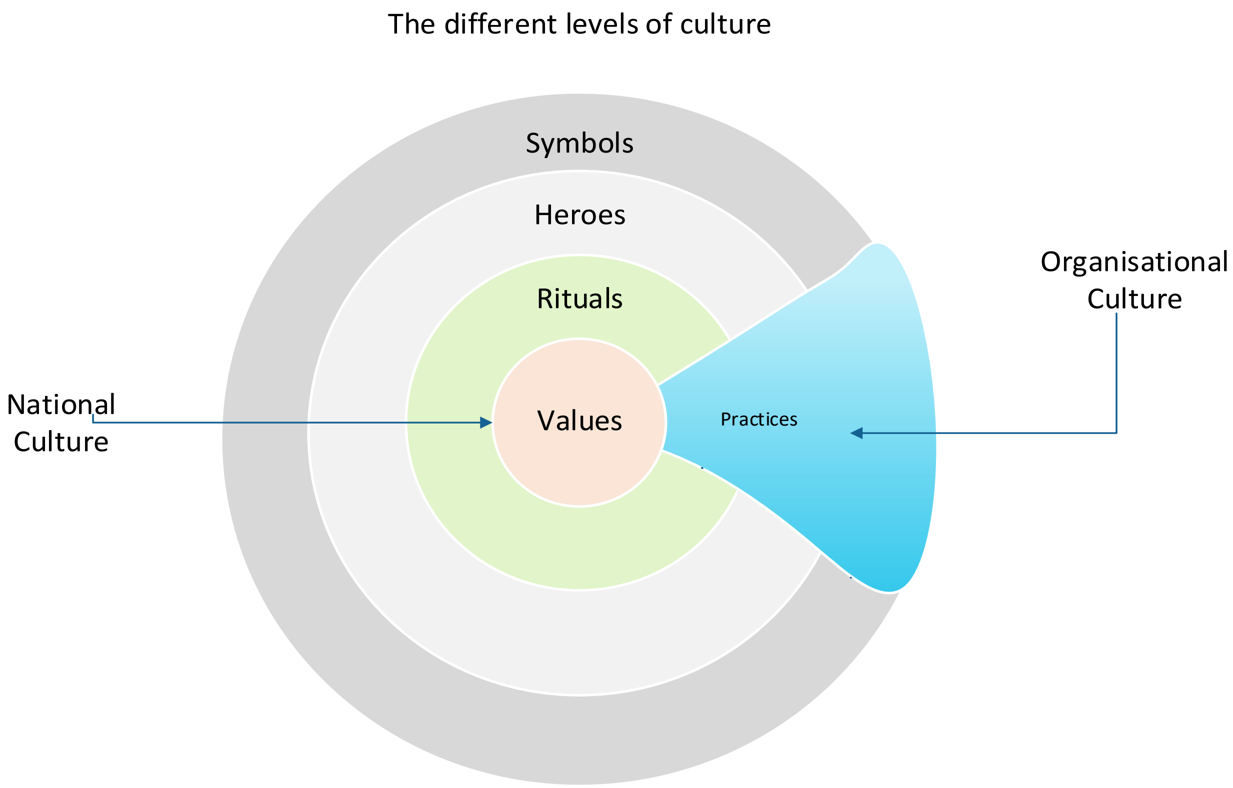


Figure 13. Hofstede's Onion Diagram on Different Levels of Culture

Source: Waisfisz (2010)

After carrying out further studies on organisational practices, Hofstede et al. (1990) divided OC into six dimensions:

i. **Process-oriented versus results-oriented.** In this process, dealing with day-to-day work is regarded as the central aspect. However, in a results-oriented organisation, the employees' performance is only evaluated by the result. There is no concern about the means by which the result is achieved. For instance, in the banking sector regulated processes are a key day-to-day aspect of the operations of the organisation which makes banking a process-oriented industry (PWC, 2013).

ii. **Employee-oriented versus job-oriented**. Employees make important decisions. In contrast, in a job-oriented organisation, managers reserve good employees for their own departments and have little concern for employees' personal problems. Considering the strict regulations associated with banking environments, most of the important decisions are based on pre-laid plans that are communicated from the management (Santomero, 1997).

iii. **Parochial versus professional.** In a parochial organisation, employees derive their identity mostly from the organisation to which they belong. In a professional organisation, on the other hand, employees identify themselves according to the type of job they do and their level of seniority. In banks both parochial and professionalism exist. Depending on rank, employees can identify themselves with the organisation, sometimes by wearing uniforms. Top management is identified by their positions, as evidenced by the size and type of offices they occupy as well as the type of cars they drive.

iv. **Open system versus closed system.** This culture dimension describes the communication environment in an organisation. In open system organisations, employees cooperate with each other and like to exchange ideas. New employees can fit into their work environment easily with the help of senior members of the organisation. However, in closed system organisations, the people and the organisation are closed and secretive, so that new employees take a long time to fit in. Depending on the role, employees in banking organisations can be met with both open and closed systems. For instance, in the IT section access to some information and systems is role specific such that role segregation determines the rate at which new employees can fit into the system (Biggar & Heimler, 2005).

v. **Loose control versus tight control**: This culture dimension refers to the extent of internal structuring in an organisation. In loosely controlled organisations there are no strict rules and procedures to guide employees' behaviour. This kind of organisation is adaptable and easy to change. In contrast, in a tightly controlled organisation, employees need to follow procedures and rules set up by their organisation. For example, meeting times must be kept punctually and employees need to be well groomed at work. Tight control is the trademark for banking organisations. Owing to the risks associated with banking transaction processing and money laundering, there is a need for tight controls in banks, as imposed by both the regulators and from within management to ensure the security of depositors' funds (Biggar & Heimler, 2005; Lucca, Seru, & Trebbi, 2014). Secure systems are also a requirement for ameliorating the controls in the transaction process.

vi. **Normative versus pragmatic**. The term 'pragmatic' defines an organisation with a market-driven culture. Normative organisations recognise their mission with regard to the external environment as the implementation of unbreakable regulations. Banks are highly regulated which makes them normative organisations (Ojiako, Manungo, Chipulu, & Johnson, 2010). If a pragmatic approach is applied to banks, they tend to lose focus on security and, as was the case in Zimbabwe, the absence of strict regulation of compliancy may cause disruptions and sometimes liquidation (Jabangwe & Kadenge, 2013).

By using international comparisons, Hofstede devoted a series of studies to understanding how national culture influences organisational processes. He showed that OC is somewhat manageable while national culture works as given facts in management (Hofstede, 1981). Whilst Schein's perspective illustrates where OC is premised without giving the existing types, Hofstede classifies culture into six dimensions based on employee values and perceptions. However, these two models do not provide any measurement of culture. In the next model by Denison, employees' opinions and perceptions are measured.

3.3.6 Denison's perspective

At the centre of Denison's OC perspective are basic organisational beliefs and assumptions designed to measure specific aspects of an organisation's culture through four factors: mission, adaptability, involvement and consistency. According to the literature, these four factors have an influence on organisational performance. For the purpose of this study, we will focus only on the four main cultural factors that focus on OC. Each of the factors is subdivided into three smaller areas which expand the performance contribution of OC. The extended version of this theory addresses national culture which is an outcome of the research carried out over fifteen years with data from over three thousand organisations and more than one hundred thousand respondents (Hofstede et al., 1990). The four elements of Denison's model focus on different aspects of culture and point out various functions of culture in organisations. Consistency and mission address aspects concerning the stability of the organisation, whilst involvement and adaptability give impetus to change. Consistency and involvement view culture as focusing on internal organisational dynamics, whilst mission and adaptability see culture as the relation of the organisation to the external environment (Denison et al. 2006). The table below presents Denison's model from the perspective of the factors, the focused study and the goal that the model seeks to achieve.

Table 6. Denison’s Organisational Culture Survey

Factor	Study	Goal of the Framework presented by the Study
INVOLVEMENT	Empowerment	Decisions are always made at the level where the best information is available.
	Team orientation	Cooperation across different parts of the organisation is actively encouraged.
	Capability development	There is continuous investment in employees’ skills.
CONSISTENCY	Core values	The leaders and managers “practice what they preach”.
	Agreement	When disagreement occurs, we work hard to achieve win-win solutions.
	Coordination and integration	It is easy to coordinate projects across different parts of the organisation.
ADAPTABILITY	Creating change	The way things are done is flexible and easy to change.
	Customer focus	Customer comments and recommendations often lead to changes.
	Organisational learning	We view failure as an opportunity for learning and improvement.
MISSION	Strategic direction and intent	There is a clear mission that gives meaning and direction to our work.
	Goals and objectives	There is widespread agreement about goals.
	Vision	We have a shared vision of what the organisation will be like in the future.

Source: Denison (1990)

These four factors are explained under separate headings below and with appropriate examples from banking organisations.

i. Involvement

This cultural factor reflects the level of an employee's involvement in the management process. Organisations with a high level of employee involvement will develop an employee's capability at all levels and create a sense of ownership, responsibility and loyalty toward their organisation.

Involvement is further divided into the following three cultural indices: empowerment, team orientation and capability. Studies conducted by Davidson et al. (2007) in a South African investment bank showed that where there was involvement, the sales growth in the bank increased as a result of the collective ownership by employees.

ii. Consistency

This cultural factor asserts that an organisation with a strong and cohesive internal culture tends to be more efficient. To explain, an organisation with a high level of consistency, conformity and consensus can easily achieve agreement among members at all levels, even when they have different points of view with regard to difficult questions in the decision-making process. Consistency is further divided into the following three cultural indices: core values, agreement and coordination, and integration. Consistency in banking organisations is a key performance indicator considering that banking is all about customers trusting the banks (Selamat & Babatunde, 2014). Customers and employees trust an organisation that operates in line with predictable business standards.

iii. Adaptability

This cultural factor focuses on the organisation's ability to adapt quickly to signals from the external environment, such as customers' demands. An organisation with a strong capacity to adapt can translate those signals into internal behavioural changes, which increases its chances of survival and development. In this model, this factor is measured by the three indices of creating change, customer focus and organisational learning. According to King (2012), banking organisations should invest in technologies that enable their customers to do banking from wherever they are. Technologies like BYOD and other enterprise mobility trends like mobile banking and branchless transaction processing channels are key adaptations that banks require in order to remain competitive.

iv. Mission

Mission examines whether organisations have a clear sense of vision, strategic direction, goals and objectives. Furthermore, it indicates whether these statements are understood and shared among all members of the organisation so that everyone will utilise the mission statements as a reference in their everyday work. In terms of this model, this cultural factor is measured by the three indices of strategic direction and intent, goals and objectives, and vision.

In Denison's model, we observe a quantitative multidimensional assessment of the main OC factors. This assessment has also been correlated with organisational performance measures. Denison (1990) argues that this approach allows for the assessment of the ways in which organisations or sub-groups within organisations deal with seemingly contradictory or competing goals and demands. In terms of such a model, OC might be viewed as the system that permits organisations to make coordinated adaptive responses to the numerous competing and even paradoxical demands.

3.4 A Comparative Analysis of the Three Perspectives on Organisational Culture

The three models discussed here address pertinent aspects that are collectively important in building a culture within an organisation. However, there is still no consensus on the way to build OC. Building an OC is a unique process for each organisation and is driven mainly by the organisational attributes of vision, mission and strategy, as well as business type (Denison, Janovics, Cho, & Young, 2004).

3.4.1 An Analysis of Schein's Perspective

Schein provides a premise for understanding the anatomy of culture that will allow the development of OC. The contribution of each of Schein's levels is explored as a basis for building an overall OC. The three levels are separated on the basis of the degree to which the cultural phenomenon is visible to the observer (Schein, 1990).

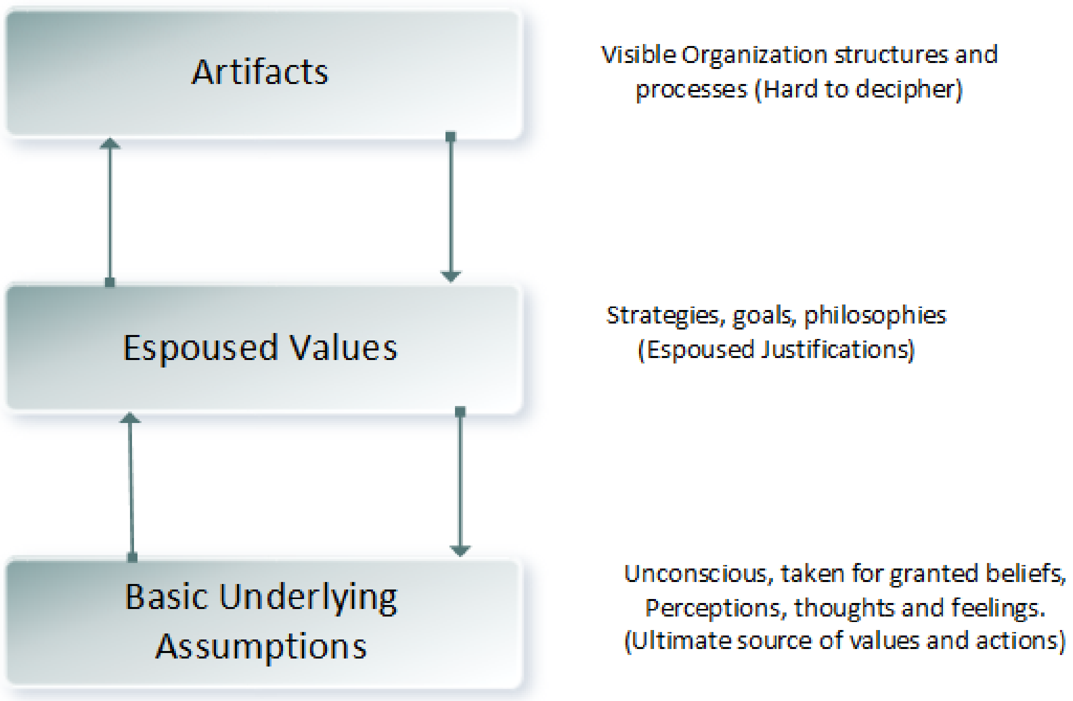

Artifacts
Visible Organization structures and processes (Hard to decipher)
Espoused Values
Strategies, goals, philosophies (Espoused Justifications)
Basic Underlying Assumptions
Unconscious, taken for granted beliefs, Perceptions, thoughts and feelings. (Ultimate source of values and actions)

Figure 14. Shein's Levels of Culture

Source: Waisfisz (2010)

The artefacts level is the most visible level of the organisation in which OC is manifested, that is, through tangible aspects common among the organisation's members. The characteristics of the OC can be seen with a human eye which, according to Sun(2008), is an observable way in which things are done in the organisation. When building an OC around technology at this level, it is easy to observe whether the organisation uses mobile devices for work as well as establish the device model. The preference and behaviour in using these devices may also be visible at this level, for instance it can observed whether the employees really prefer their own mobile devices or the ones the company gives them. It can also be observed whether the behaviour around the use of mobile devices in the organisation portrays any specific pattern. This will give an understanding of what to consider when building an ISC for the use of the devices, which is the main theme of this study. If this is then applied to a banking organisation, the type of acceptable devices can be identified. This will inform the bank's strategy for implementing a BYOD solution that accommodates the employees' preferred devices.

The next level of espoused values refers to the belief system shared within the organisation. This develops from the organisation's day-to-day operations. By virtue of diverse backgrounds, employees come into the organisation with different beliefs that are then absorbed into a set of values constituting an organisational belief system (Hu, Dinev, Hart, & Cooke, 2012). Hogg (2013) posits that in building an OC, an understanding of the belief system is important as it gives direction as to the norms that are acceptable to the organisation. For instance, if one of the organisational values is to respect deadlines, as is the expectation in banks, building a culture around the use of mobile devices will be easy as employees will have the privilege of accessing their office at any time. An organisation that does not have a culture of respecting deadlines may find it difficult to build a culture around the use of mobile devices.

The deepest level of OC from Schein's perspective is composed of shared tacit assumptions. These constitute the underlying assumptions and the premises on which the OC is based. The OC phenomenon from other levels is understood through this level as it addresses aspects such as how members of an organisation think about themselves, the relationships among members, and the nature of the organisation, as well as the world at large. Banking organisations have existing classifications depending on the country ranking scale. In Zimbabwe, banks are classified as either tier one, tier two or tier three with tier one being the highest (RBZ, 2014). This classification is based on a number of parameters of which the level of investment in technology is one. The tier into which a bank fits informs the assumptions around the level of technological investments expected in it. The bank at which the survey was conducted is a first-tier bank.

From this model, we can take a view on how to identify cultural characteristics ranging from behavioural norms, visible aspects to the underlying belief systems in formulating an OC. According to Maximini (2015), Schein's perspective is a process-oriented approach to OC which regards it as a continuous recreation of shared meaning. However, it shows only where OC is located without providing specific types of cultures. The next subsection is an analysis of Hofstede's perspective on OC which is based on the four cultural layers that will result in OC being divided into six dimensions.

3.4.2 An Analysis of Hofstede's Perspective

Hofstede (2011) divided culture into four layers. Values are placed at the core and are defined as broad preferences for one state of affairs over others and in terms of which one group separates itself from another. Values include such preferences as freedom over equality or equality over freedom. Robbins et al. (2009) state that values deal with aspects such as evil versus good, abnormal versus normal irrational versus rational and many other such aspects. From this perspective we can identify three interesting aspects of OC relations:

- The way employees relate to each other
- The way employees relate to their work
- The way employees relate to the outside world.

This perspective sums up OC as the way in which members relate to each other, their work and the outside world (Hofstede, 1981).

These three attributes distinguish an organisation from others. Accordingly, when describing OC we explore the relations among members. A study conducted by Zakari and Poku (2013) on the banking sector in Ghana and another by Nguyen (2014) on Standard Chartered Vietnam both concluded that the way members on the same level relate, as well as the way they relate across hierarchies of the organisational structure, is important in building an OC. The way employees relate to their line managers in an organisation also has a bearing on its culture. For instance, are employees able to speak their minds or do they act according to the manager's directives? Another example is how the employees relate to each other when there is a situation that requires coordination.

Regarding relations in the workplace, the culture describes among other things the culture in regard to observing rules. It also describes, for example, the way an organisation views employees' innovations as well as whether instructions are directed from management. An understanding of these dynamics assist in the building of an OC as they give an acceptable starting position.

In considering relations outside the organisation, culture describes the way organisations value their customers and their vendors and suppliers of certain services and products. This level also provides insights on whether or not outsiders are welcome within the organisation. The issue of whether employees are inward or outward looking is also identified within this level, because when building a culture, this will give direction on how the innovations and recommendations will be viewed from outside. For instance, the value that the organisation will attach to a new business trend and technologies will be built by examining this level.

3.4.3 An Analysis of Denison's Perspective

At the core of Denison's model on OC we find organisations' basic beliefs and assumptions. The model is based on employee behaviour which outlines four elements of OC. Other given models are psychology driven and are often designed and created within the academic environment. Denison's model is driven by its application to all levels of the organisation, closely linked to bottom-line business results (Rahmani & Ghorbani, 2015). Other models described above are often not very clear about specific links to business results and there has been little if any research conducted to place cultural elements in relation to performance. Figure 15 depicts Denison's OC model and gives a brief description of each component.

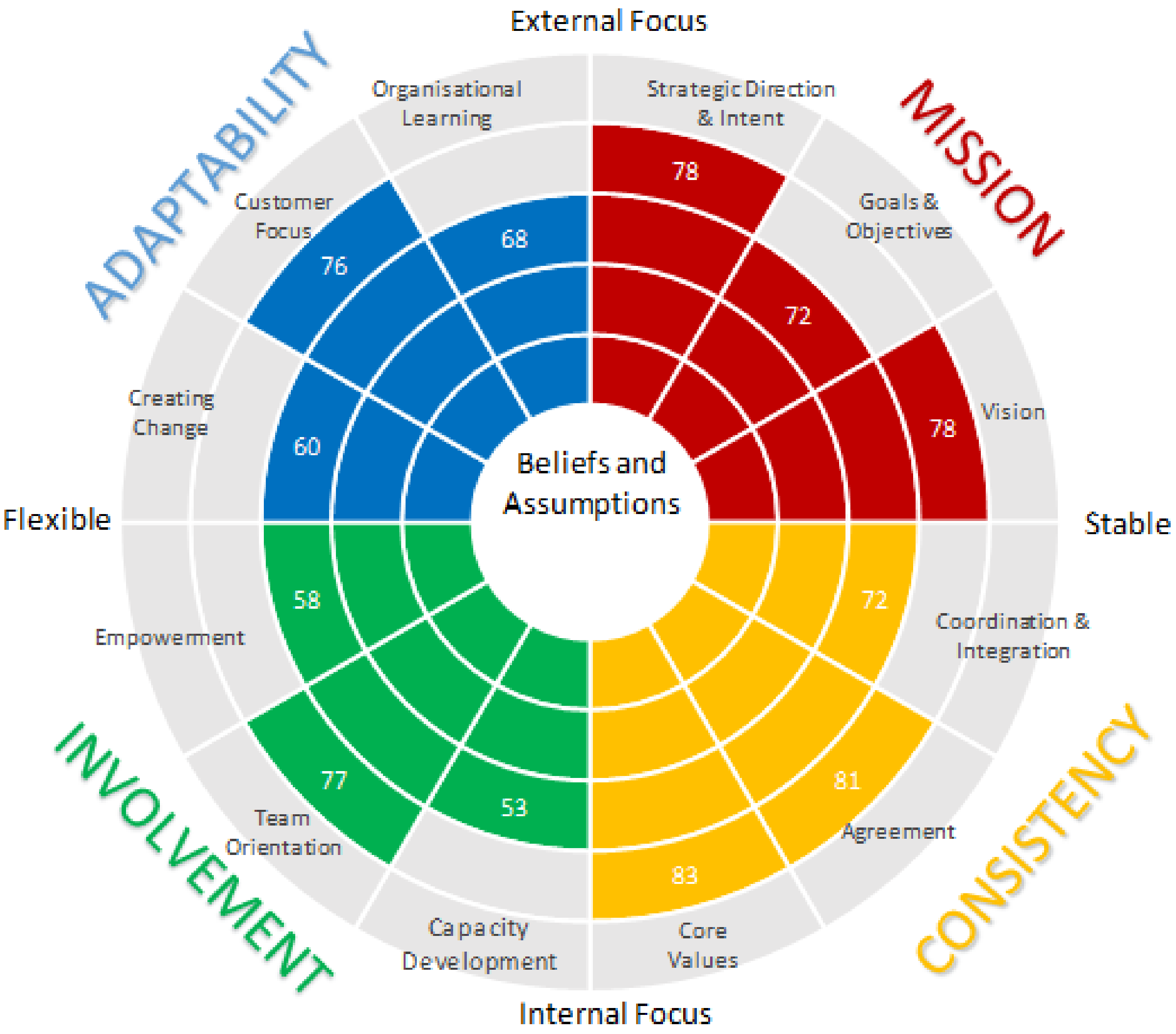


Figure 15. Denison's Organisational Culture Model

Source: Denison et al. (2006)

Denison's model is designed to measure specific aspects of culture in an organisation under the areas of mission, adaptability, involvement and consistency. This model shows that OC has a significant impact on behaviour and performance in an organisation. It also shows that OC is closely linked to organisational strategy, performance and management practices. The model is designed to measure employees' opinions and perceptions or the underlying beliefs, values and assumptions they share.

The model also addresses the behaviours and practices that exemplify them. In building an OC the model facilitates important conversations and generates thoughtful actions that drive change.

A study conducted by Mir (2014) on the impact of OC and risk management in the banking sector in developing countries confirms that in building an OC, the model provides a parallel approach to driving cultural change which takes the form of organisation-wide actions, departmental or functional actions, team actions as well as leader or manager actions.

Based on the analysis of the models above, the following sections will examine how an OC can be built. Each model has its own focus areas on OC in the general sense. For the purpose of this study, we will examine how an OC around technology will be built. The focus areas of every model will be cited where relevant to qualify the research.

3.5 Building of Organisational Culture

In order to build an OC there is a need for organisations to focus more on employee behaviour, attitudes and perceptions (Fey & Denison, 2000). The three models discussed above all showed that employees' habits and behaviours have a significant bearing on building a culture in organisations. From Schein's perspective, the three levels are all discussed from the employees' perspective. Hofstede argues that the distance from power, resulting from the result of rank in the organisation the employee holds, plays a significant role in the creation of a culture. Hofstede further states that whether or not employees buy into the way of conducting business in an organisation is basically a function of how they relate to it. Denison's perspective dwells more on employee behaviour as a result of their belief systems and assumptions.

From this discussion it is clear that the employee plays a central role in building a culture in the organisation. Bennett (2015) states that employee participation is required for an organisation to build a culture of innovation. Tharp (2009) states that culture develops from either the organisational stakeholders' active or passive participation. Understanding the employee is therefore the first step in building the OC. Banks are associated with procedures and well-formulated set rules in performing their day-to-day businesses. Accordingly, Doan (2014) suggests that in building an OC in banks, active participation from the employees plays a key role as it comes as a form of regulation.

The next section will address the relationship between OC and IT. This will be followed by an examination of the relationship between OC and information security, which then forms the basis for an examination of information security as a culture within an organisation.

3.6 Organisational Culture and Information Technology

Information technology (IT) as a business enabler for organisations has become commonplace in today's workplace (Singh & Phil, 2012). The outcome and the interactions between IT and OC can result on the one hand in acceptance and the effective use of IT, or user resistance, total rejection or even sabotage on the other (Mehri & Yeganeh, 2015). OC as defined by Lundy and Cowling (1996) refers to the way things are done in particular organisations. The way an organisation conducts its day-to-day operations cannot be changed overnight, whilst a technology can. There is an interesting contradiction in the rate of change between OC and IT. As such, OC is always playing catch-up to changes in IT. Trompenaars and Turner (1997) point out that technology works by the same rules everywhere regardless of the cultural values. Whilst this is true for computers as machines, it is not entirely true for the human machine.

Research has shown that the real problem is not the impact that IT has had on OC but rather how organisations have learnt to adopt IT and use it for the development of the organisation (Magdalena, Fotache, Munteanu, & Dospinescu, 2009). IT has come with some disruptive and pervasive tendencies in regard to culture, such that organisations have now been compelled to change some of their cultural norms and values. IT had developed to become ubiquitous, providing employees with access to computing requirements on the move. This new technology is referred to enterprise mobility (Diogenes & Gilbert, 2015). BYOD is one such a form of enterprise mobility that has notably affected the working culture of organisations (Singh & Phil, 2012). A study on the banking sector by King (2012) concluded that banking is no longer about a place where customers go to perform transactions but rather about how customers perform their transactions from wherever they are. In line with this notion, banks are compelled to adapt to the technological changes to remain relevant.

Researchers argue that IT leads to specific effects on organisations, thereby causing changes to OC, norms, structure, performance, and other business attributes. According to Mehri and Yeganeh (2015), when there is a misfit between IT and OC, three options exist:

- Reject the IT to seek a solution that is more compatible with the culture.

- Redesign the technology before implementing it.
- Proceed with adoption and face the challenges as they present themselves.

From the findings and observations above, it is clear that IT is a change agent for culture. The rate and direction of change is basically driven by the degree of participation for the organisation. Another cardinal aspect of the impact of IT on culture is information security (Kuusisto & Ilvonen, 2003). The next section will explore the relationship between OC and information security.

3.7 Organisational Culture and Information Security

Based on the findings of the literature review, it is imperative that organisations focus on employees' behaviour to achieve information security, as their security effectively depends upon how employees do or fail to do certain tasks. Lim, Chang, Maynard, and Ahmad (2009) posit that the management of information security is becoming more complex in today's businesses because people are both a cause of information security incidents and key participants in the implementation of the protection against them. Chang, Ho, and Chang (2014) argue that whilst productivity is viewed as the biggest benefit of BYOD, there is need for organisations to invest in a culture of security when using BYOD devices so as to enjoy the full productivity benefits.

The way things are done in particular organisations, that is, the OC, has a bearing on the overall information security appetite of the organisation (Sun, 2008). The culture of the organisation in relation to its information assets, as well as how risk averse it is, will form the basis of its information security(Rajendran, Furnell, & Gabriel, 2009). The security of the information in an organisation is all about the culture of the people in it (Johnson & Goetz, 2007), as technology works in the same way everywhere, regardless of values, belief systems or location (Trompenaars & Hampden Turner, 2008). From this assertion it is evident that there is need for the information security standards and the cultural values of an organisation to be harmonised. Where OC fails to fit in with the information security standards , organisations have no choice other than to reject the IT, seek IT that is more compatible with the culture, redesign the technology before implementing it, or proceed with adoption and face the challenges as they come (Mehri & Yeganeh, 2015).

Applying this perspective in the banking environment, compliancy with regulations takes precedence over everything else, such that information security has to fit in with the bank's OC which is driven by the regulatory framework it is operating under (Woretaw & Lessa, 2012). An organisation's information security is therefore driven by the organisation’s culture. Accordingly, an organisation that is security aware will have an ISC. This will be discussed in depth as the main theme of the next chapter.

Gessner et al. (2013) suggest that personal devices need to be kept up to date with security applications such as anti-viruses, software patches, firmware and settings on configuration. If the unintended administrator does not keep the device up to date with security software patches, the device becomes the greatest vulnerability for the organisation’s network (Armando, Costa, Verderame, & Merlo, 2014). Employee behaviour is the outcome of the interaction between the interrelated social roles and the unique role identities in the organisation (Matsumoto, 2007). Robbins et al. (2009) define organisational behaviour as “what people operate in an organisation and how their behaviour affects the performance of the organisation” (p. 3). From this definition, it is apparent that employee behaviour is a key determinant of organisational behaviour, and thus both organisational behaviour and OC will form the foundation for an organisation’s information security culture (ISC) (Chatterjee, Sarker, & Valacich, 2015).

3.8 Organisational Culture for Banking Organisations in a Developing Country

The wave of erosion of public trust in banks across the globe has invoked anti-money laundering regulations in the banking sector (Ndlovu, Bhiri, Mutambanadzo, & Hlahla, 2013). Thakor (2015) argues that because of this wave of security-related challenges, information security in banking is now commanding significant regulatory attention and a strong OC can be viewed as an off-the-balance-sheet complement to the bank’s capital.

There are two types of banking institution that exist in most developing countries: those with the local shareholders in a given country and those with foreign shareholders. The maturity of OC in these two types of institution is at contrasting levels. A study by Mambondiani, Zhang, and Arun (2014) on Zimbabwean banks discovered that foreign-owned banks normally have OC standards that are directed from the external head office. On the other hand, locally owned banks have a deficiency in the application of reasonable OC standards. Whilst regulatory standards have guidelines on the policies that they enforce, the OC has a bearing on the quality and level of implementation for standards.

A study by Rasid, Manaf, and Quoquab (2013) on Islamic banking in Malaysia pointed out that OC together with other factors like leadership style play a pivotal role in the successful operation of the business. In banks, performance is closely related to reputation. A bank that has a culture of security or a culture that is deemed good in the eyes of its customers will reap good business proceeds. The bank's strategy, structure and culture are closely linked and are the key components for business performance if properly aligned (Childress, 2011). A good OC is indeed a key component of a successful banking organisation.

A study by Davidson et al. (2007) on the relationship between OC and financial performance in a South African investment bank showed that an organisation's culture has a significant impact on performance. Coetzee et al. (2007) used Denison's cultural model to measure some OC metrics which led to this finding. Another study by Doan (2014) on Standard Chartered Bank Vietnam examined OC using Schein's perspective. When Standard Chartered Bank hired new employees, they had a policy in place that allowed the employees to learn all of the organisation's espoused values before facing clients. The Bank also embraced the Vietnamese collectivist culture which is a key organisational behaviour in Vietnam. For instance, employees gather for coffee every morning and those who do not participate tend to feel like outsiders. The study also shows that a diversity of opinions helped to minimise risks and organisational decisions are followed absolutely and faithfully.

In summary, OC is gradually taking centre stage, even in banks, as a competitive edge. Whilst the core business in all banks is with bank customers, there is now a new way of allowing banking services on the move through ubiquitous computing (King, 2012). This, however, is resulting in other security challenges which require participation from every employee towards the adoption of a culture. Several information security methodologies can be used to guide the operation of information security aspects that are targeted at addressing the threats that information resources are exposed to. One example is ISO/IEC 27002:2005, which deals with acceptable standards for information security management. Another example is the Control Objectives for Information and Related Technologies (COBIT), which is a control framework that links IT initiatives to business requirements and brings them into line with the resources that will assist in management control. These and many other information security standards form the basis of an ISC if adopted by an organisation.

Da Veiga and Eloff (2010) view information security culture as

> "… the attitudes, assumptions, beliefs, values and knowledge that employees/stakeholders use to interact with the organisation's systems and procedures at any point in time. The interaction results in acceptable or unacceptable behaviour (i.e. incidents) evident in artefacts and creations that become part of the way things are done in the organisation to protect its information assets. This information security culture changes over time "(p. 198).

To substantiate the important cultural behaviours in relation to the BYOD phenomenon, theories from the human sciences will be used. These are discussed in the following section.

3.9 Conclusion

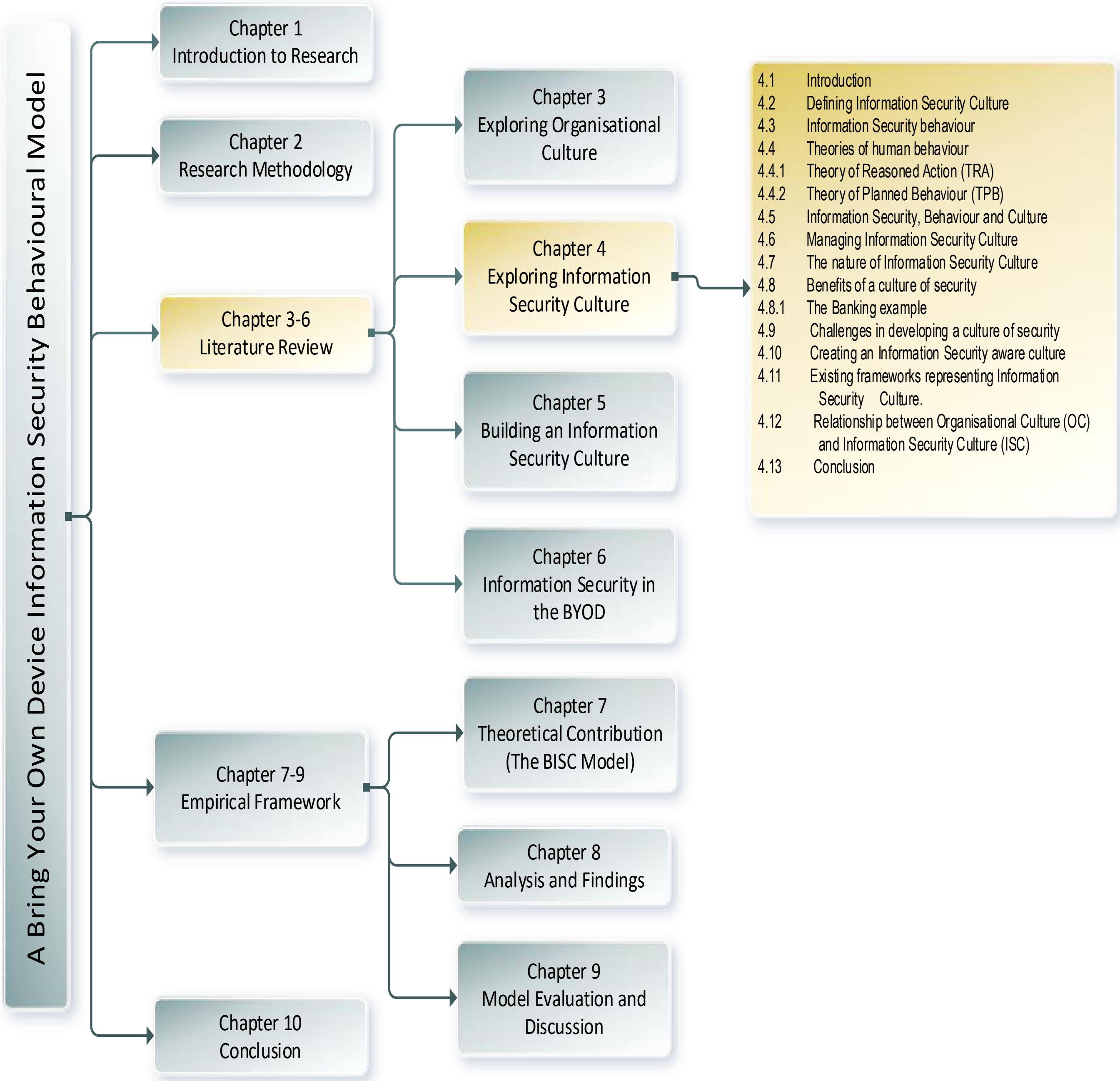
According to Schuman (2006) and GE Capital (2012), OC is the "complexion" of the organisation. It basically dictates how the people behave within the organisation as well as towards external factors such as new technologies. An understanding of the OC assists in the building of an ISC. This chapter explored OC by exploring the theories of organisational behaviour which underpin the way organisations are now identified by their cultures. The statement of the problem to be addressed in this study is to mitigate the risks posed by the unintended administrator created by the BYOD phenomenon in the Zimbabwean commercial banking sector. A BYOD ISC is accordingly deemed to be the solution to the challenges posed by the unintended administrator. According to the sources cited in this chapter, an OC is the way things are done in any given organisation.

Various theories have been put forward to explain how culture can be built. Schein posits that culture can be viewed across three levels of any given organisation, namely, artefacts, espoused values and shared tacit assumptions. Hofstede (2010) maintains that culture manifests across four levels of the organisation in the form of the symbols, heroes, rituals and values that a people share. Denison's perspective on culture is based on basic organisational beliefs and assumptions designed to measure OC through the four factors of mission, adaptability, involvement and consistency. These three theories were explained in detail in this chapter to help to support the basis for building an organisational ISC based on individual employee traits and thus bring rigour to the study. From this chapter it can be deduced that there is a direct relationship between OC and IT, specifically in the context of the BYOD phenomenon. In Chapter 1, BYOD was presented as an employee-driven initiative which is influenced to a great extent by employee habits, knowledge and attitudes. The same traits combined with the organisational environment, governance and the training that the employees are given influences the culture towards the BYOD. The theories discussed in this chapter confirm, from a social science viewpoint, that there is a direct link between employee traits and organisational traits which if combined influence the organisational ISC.

The cited examples of banks in developing countries prove that a sound OC is the new prerequisite for performance and profit. The next chapter will discuss information security as a culture in detail and then build around the BYOD phenomenon. This will lead to critical building blocks for an ISC for the unintended administrator of BYOD. Chapter 4 will explore ISC theories and the relationship between ISC and OC. The chapter culminates in the identification of critical success factors for building an ISC in general. It should be noted that the ultimate aim is to build an ISC around BYOD. A case study of a bank in Zimbabwe will be used to set the premise for this research.

Chapter 4 : Exploring Information Security Culture

"Culture, more than rule books, determines how an organisation behaves." Warren Buffet


A Bring Your Own Device Information Security Behavioural Model
Chapter 1
Introduction to Research
Chapter 2
Research Methodology
Chapter 3-6
Literature Review
Chapter 3
Exploring Organisational Culture
Chapter 4
Exploring Information Security Culture
Chapter 5
Building an Information Security Culture
Chapter 6
Information Security in the BYOD
Chapter 7-9
Empirical Framework
Chapter 7
Theoretical Contribution (The BISC Model)
Chapter 8
Analysis and Findings
Chapter 9
Model Evaluation and Discussion
Chapter 10
Conclusion
4.1 Introduction
4.2 Defining Information Security Culture
4.3 Information Security behaviour
4.4 Theories of human behaviour
4.4.1 Theory of Reasoned Action (TRA)
4.4.2 Theory of Planned Behaviour (TPB)
4.5 Information Security, Behaviour and Culture
4.6 Managing Information Security Culture
4.7 The nature of Information Security Culture
4.8 Benefits of a culture of security
4.8.1 The Banking example
4.9 Challenges in developing a culture of security
4.10 Creating an Information Security aware culture
4.11 Existing frameworks representing Information Security Culture.
4.12 Relationship between Organisational Culture (OC) and Information Security Culture (ISC)
4.13 Conclusion

4.1 Introduction

Information security culture (ISC) has developed to become an organisational aspect which is essentially an important subculture of the overall organisational culture (OC) (Chen, Ramamurthy, & Wen, 2015). It provides a guide for employee behaviour when interacting with IT systems to avoid actions that may expose the organisation to information security breaches and risks (AlHogail, 2015). Earlier studies by AlHogail and Mirza (2014) concluded that an ISC gives direction on how information assets are managed in an organisation with the aim of protecting them and influencing employees' security behaviour. The same authors also argue that a security culture has to be inherent in the thoughts and actions of all the individuals at every level of an organisation. A study by Von Solms and Von Solms (2004) agrees with this conclusion by noting that several information security controls can be managed properly if a comprehensive culture of information security is in place such that the employees know and understand, as well as buy into, the necessary security precautions.

Research has shown that organisations lose billions of dollars in revenue through information-related attacks. Thus, creating an ISC in organisations forms a basis for the formulation of an improved level of security management. According to the Deloitte Consumer Review Report for 2015, there are two types of organisation: those whose security has been compromised and know it and those whose security has been compromised and do not know it (Deloitte, 2015b). This suggests that, in essence, no organisation is safe; as such organisations have to make conscious efforts to secure their information. The first step to ensuring a safer level of security in an organisation is to create security aware behaviours and attitudes among the employees (AlHogail & Mirza, 2014). A combination of correct attitudes and behaviours towards information security results in the creation of an ISC. Thus, if a culture of information security already exists in the organisation, the implementation of information security technical solutions will be effective.

This chapter explores ISC in detail. It commences by defining ISC in the context of OC, followed by exploring how information security behaviours can be created. Considering that behaviour is a key component of building a culture, the study on how information security behaviours can be built gives impetus to the way an ISC can be created. Theories from the social sciences relating to the building of culture will be used. The chapter will conclude by establishing the relationship between OC and ISC.

4.2 Defining Information Security Culture

Chapter 3 highlighted that ISC is espoused in the organisation's culture. AlHogail and Mirza (2014) argue that the descipline of ISC is fairly new, and it is often explained and defined using a mixture of principles and theories from other research areas. They propose that ISC be defined as "the collection of perceptions, attitudes, values, assumptions, and knowledge that guides the human interaction with information assets in an organisation with the aim of influencing employees' behaviour to preserve information security" (Al Hogail & Mirza, 2014, p. 2). ISC can also be defined as the way things are done in an organisation to protect information assets (Da Veiga & Eloff, 2010). Figure 16 below defines information security from the perspective of Schein (1990).

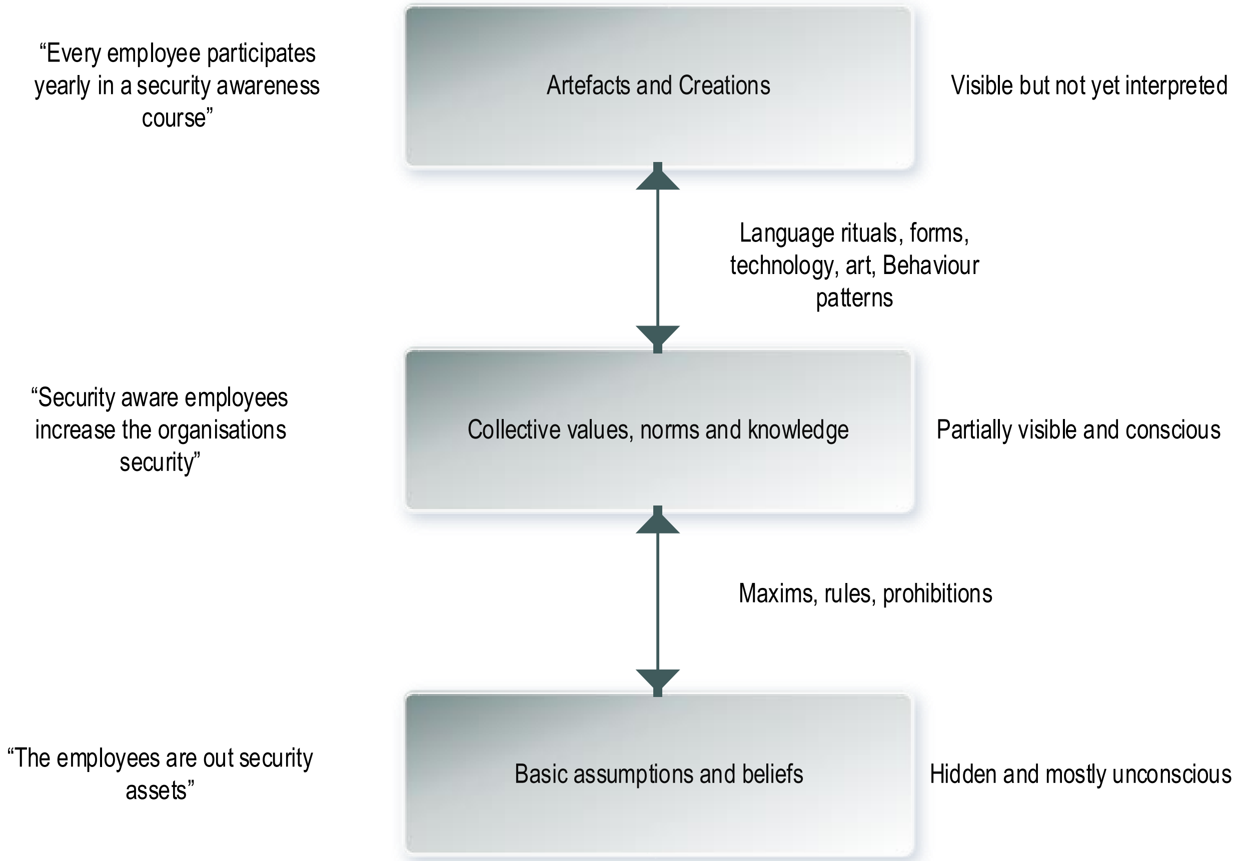

"Every employee participates yearly in a security awareness course"
Artefacts and Creations
Visible but not yet interpreted
Language rituals, forms, technology, art, Behaviour patterns
"Security aware employees increase the organisations security"
Collective values, norms and knowledge
Partially visible and conscious
Maxims, rules, prohibitions
"The employees are out security assets"
Basic assumptions and beliefs
Hidden and mostly unconscious

Figure 16. The Layers of Information Security Culture

Source: Schlienger and Teufel (2003)

Udeh and Dhillon (2008) define ISC as "the totality of human attributes such as behaviour, attitudes, and to the protection of contributing values that all kinds of information in a given organisation" (p. 1).

Ngo, Zhou, and Warren (2005) propose a more employee-centric view of ISC by defining it as how things are done by employees and the whole organisation in a manner that is naturally consistent with information security principles. Schlienger and Teufel (2003) believe that it is a collective phenomenon that grows and changes over time and can be influenced and designed by management to some extent. This definition resonates closely with the perspective of Schein (1990). Figure 16 shows a combined diagrammatic explanation of Schein's perspective incorporating the viewpoints of Schlienger and Teufel (2003).

Schlienger and Teufel (2003) expand the position that information security is a subculture to OC by pointing out that information security is consequently a subculture in regard to organisations' general security functions. This expands on Schein's perspective discussed in section 3.6.1 in Chapter 3 where he classifies culture into three major components – artefacts, values and shared tacit assumptions. Figure 16 illustrates these three components and their interactions. Schlienger and Teufel (2003, p. 405) give a more detailed definition: "Security culture encompasses all socio-cultural measures that support technical security measures, so that information security becomes a natural aspect in the daily activities of every employee."

The definitions of ISC cited above all identify the employees as being at the centre of its existence through the various behaviours they display towards information assets. In order to have a clearer understanding of information security as a culture, there is a need to explore the behaviour that led to the creation of an ISC.

4.3 Information Security Behaviour

This section will explore behaviour in relation to information security and addresses those attributes and characteristics of the users who observe information security. Behavioural ISC is the subsection of information security that deals with those factors that motivate security-driven actions with regard to information systems (Stephanou & Dagada, 2014). Information security behaviour that is sustained over time evolves into an ISC that is evident in artefacts. Researchers in human behaviour argue that there is a need to direct and monitor human behaviour towards technology to ensure conformance to security standards and requirements (Stephanou & Dagada, 2014). This viewpoint suggests that there is a need to understand human behaviour in order to have an effective ISC.

Alfawaz et al. (2010) identified four modes into which employee behaviour towards security can be categorised. These modes are based on an individual's acknowledgment of the security rules and possession of the essential skills for performing certain actions. The identified modes are:

i. Knowing–doing mode
ii. Knowing–not doing mode
iii. Not knowing–doing mode
iv. Not knowing–not doing mode.

In each of these modes, different and dynamic behavioural characteristics are portrayed depending on the individual's skill, knowledge and values. The transition from each mode is determined by the various characteristics as they apply to the individual employee. The table below describes each mode and gives some examples of how employees fit into them.

Table 7. Information Security Behaviour Modes

Information Security Behaviour Modes		
Modes of Individual Behaviour	**Description**	**Example of Related Information Security Behaviour**
Mode (1): Not knowing–not doing	In this mode the subject does not know the organisation's requirements for information security behaviour and does not have security knowledge. As a result, they are not displaying the right behaviour (violation of the rules for security behaviour and security is compromised).	Information security policy is not in place or is not properly communicated to the user: sharing passwords; downloading Internet software; visiting harmful web contents
Mode (2): Not knowing–doing	The subject does not know the information security requirements/rules of behaviour and does not have security knowledge but is nevertheless exhibiting the right security behaviour (following the rules – security is not compromised).	Although no means is provided to the users, they are unknowingly following the rules: reporting valuation, sharing related information and knowledge

Mode (3): Knowing–not doing	The subject knows the rules of behaviour and has the required knowledge and skills, but is not displaying the right behaviour (violation of the rules of behaviour – security is compromised).	Even though a policy is in place and well communicated, users intentionally violate the related rules: users take shortcuts to accomplish risky tasks; users ignore related procedures and rules.
Mode (4): Knowing–doing	In this mode the subject knows the rules of behaviour and has the knowledge/skills and they are doing the right behaviour (following the rules; security ID not compromised).	Information security in place and well communicated, and users are abiding by rules.

Source: Alfawaz and Nelson (2010)

The various modes are portrayed in Figure 17. The transition from one mode to another is dynamically driven by the amount of information that the employee has about the organisation. The behaviour in terms of information security also comes into play as it determines the subjective norms regarding turnaround times and implementation of tasks (Mehri & Yeganeh, 2015).

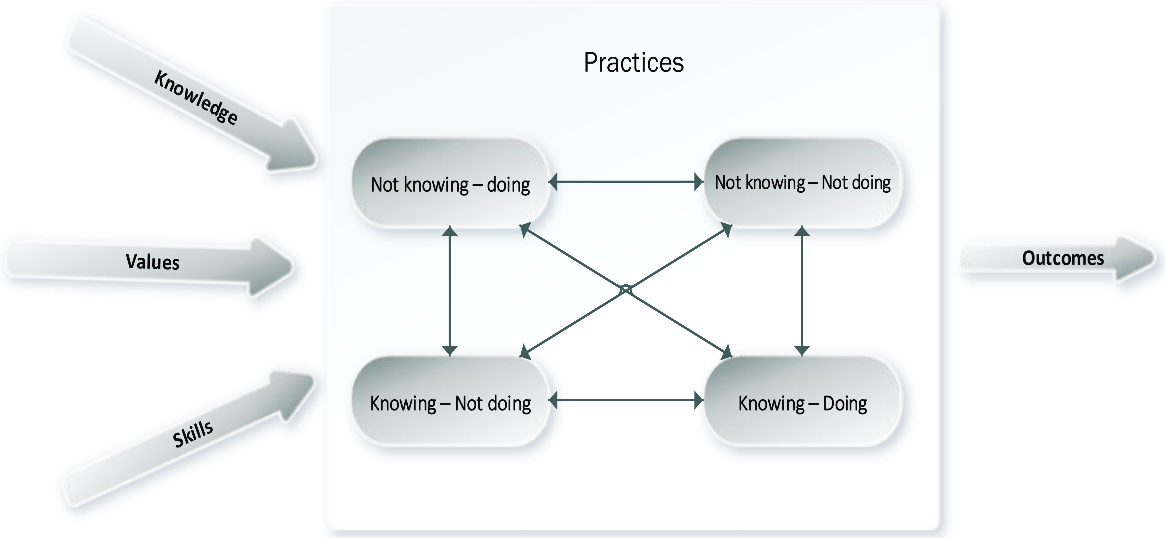


Figure 17. Information Security Behaviour Modes

Source: Schlienger and Teufel (2003)

The various modes determine the level of security behaviours that the employees exhibit. Related studies which were conducted by Chatterjee et al. (2015), which extend the view originally introduced by Ajzen (2002), note that these behaviours are driven by the skills, knowledge and values espoused within the organisation as well as the shared tacit assumptions. In order to understand the way behaviours are created, we will make use of theories from the field of psychology.

4.4 Theories of Human Behaviour

Fishbein and Ajzen were both working on similar concepts to explain human behaviour and eventually collaborated to create and publish a model in 1980. In terms of their findings, human behaviour can be predicted by analysing certain behaviour performed by human beings. Fishbein and Ajzen (1981) subsequently presented the theory of reasoned action (TRA), which holds that an individual's behaviour or action is driven by his or her intention to perform such behaviour/action. A refined version on the TRA, the theory of planned behaviour (TPB), was made necessary by the limitations of the TRA in dealing with behaviours over which people have incomplete volitional control.

Alhogail et al. (2014) argue that the information discipline is better explained and defined by borrowing from other disciplines. This study will make use of psychological research to explain the behavioural attributes of employees. In the following section we will examine the two theories and explore how they can influence the creation of an ISC. Some examples from banking organisations will be cited for both theories.

4.4.1 Theory of Reasoned Action (TRA)

The TRA posits that individual behaviour is driven by behavioural intentions which are a function of an individual's attitude toward the behaviour and subjective norms surrounding the performance of the behaviour (Ajzen, 2002). TRA works best when applied to behaviours that are under the person's volitional control (or they think they are). This theory states that people think about the consequences and implications of their actions and behaviour and then they decide whether to do something. The theory views behaviour as a function of the attitude towards specific actions or subjective norms regarding that action.

Applying this theory to building an ISC, the aspect of employee behaviour and attitude can be explored in building a culture in which employees are made aware that they have control over the organisation's information assets. After carrying out a meta-analytical review of the application of the TRA and TPB

Downs and Hausenblas (2005) noted that intentions and perceived behavioural control play a big role in how employees behave. They also noted that intention was strongly associated with attitude and that it predicted exercise behaviour. A study by Albarq and Alsughayir (2013), on the applicability of TRA to Internet banking usage intention, using structural equation modelling, found that attitude and actual behaviour closely inform the security alertness that the Internet banking users displayed when transacting. Figure 18 presents a schematic presentation of the TRA showing the two basic components of attitudes toward a specific action. The first addresses aspects like the consequences of engaging in a particular behaviour or how desirable the consequences of the behaviour are. The second component addresses the subjective norms regarding that action, which addresses aspects such as normative beliefs (other people's expectations of the employees) and the employees' motivations to comply (which addresses such aspects as whether the employees choose to comply, as well as the costs and reason for making either choice).

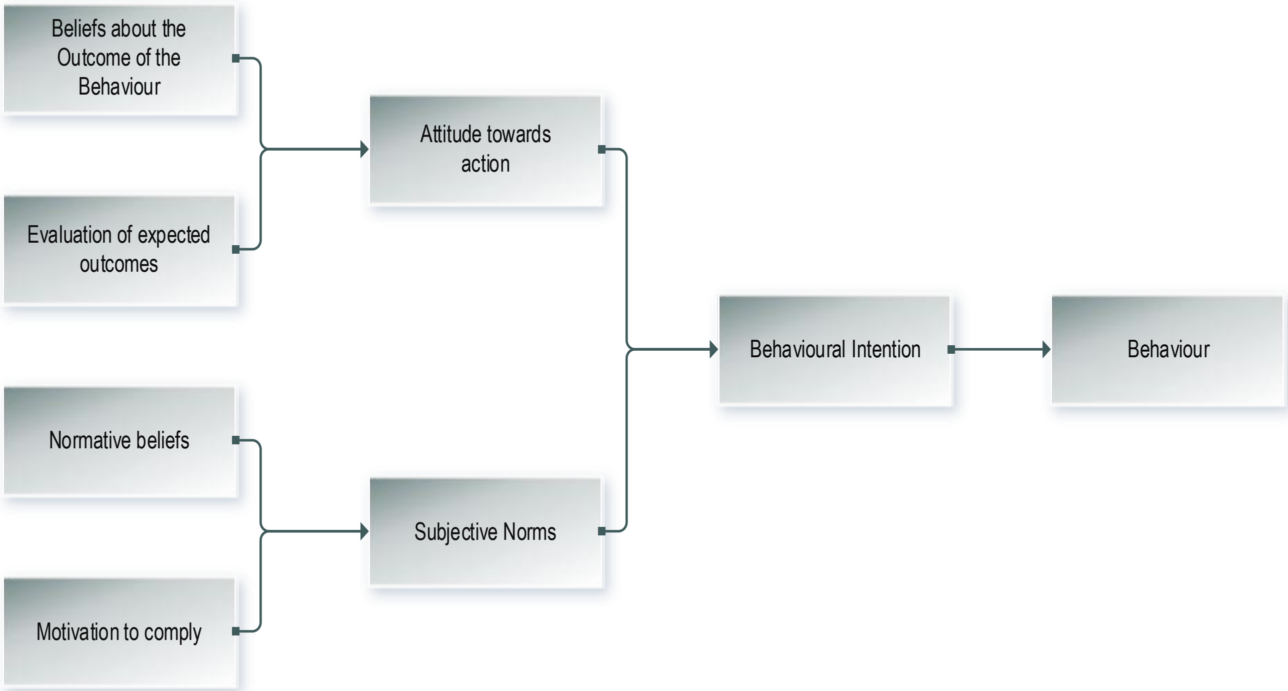


Figure 18. Illustration of the Theory of Reasoned Action

Source: Adapted from Morris, Marzano, Dandy, and O'Brien (2012)

This theory concludes that intention must be highly correlated with behaviour. Whether or not a person intends to perform a healthy behaviour should correlate with whether or not they actually do the particular behaviour. The theory does not address the impact of the attitudes and subjective norms on the people who have little power over their behaviour or those who believe they have little power. Because of this limitation, Ajzen (2002) added perceived behavioural control as the third element, resulting in extending the TRA to the TPB. The next section will address the TPB, which has three basic components.

4.4.2 Theory of Planned Behaviour (TPB)

The TRA proposes a model which can measure how human actions are guided by predicting the occurrence of a particular behaviour, provided that behaviour is intentional (Ajzen, 1991). The TPB, on the other hand, works best when the behaviour is NOT perceived to be under the person's control. In view of the fact that intentions are the precursors of behaviour, the constructs of the TRA are motivational and depend on the strength of the intent to perform the behaviour. The greater the strength, the harder the person is expected to try. Two components determine intention: attitude toward the behaviour and subjective norms (each are weighted according to importance).

The introduction of the additional factor of perceived control differentiates TPB from the earlier TRA. Perceived behavioural control is determined by two factors: control beliefs and perceived power. Perceived behavioural control indicates that a person's motivation is influenced by how difficult the behaviours are perceived to be, as well as the perception of how successfully the individual can, or cannot, perform the activity. A study conducted by Sadeghi and Farokhian (2011), on the role of behavioural adoption theories in online banking services, noted that the there was little correlation between satisfaction and security as a result of the absence of perceived behavioural controls in the customers' participation on the Internet banking platform . This could have been a result of the customers' confidence levels in electronic banking services. In a study on India's Internet banking, Bhatt (2011) concluded that TPB predicts behaviour from intention, and perceived behavioural control addresses the readily available resources, skills, and opportunities, as well as the employee's own opinion on the significance of achieving the results.

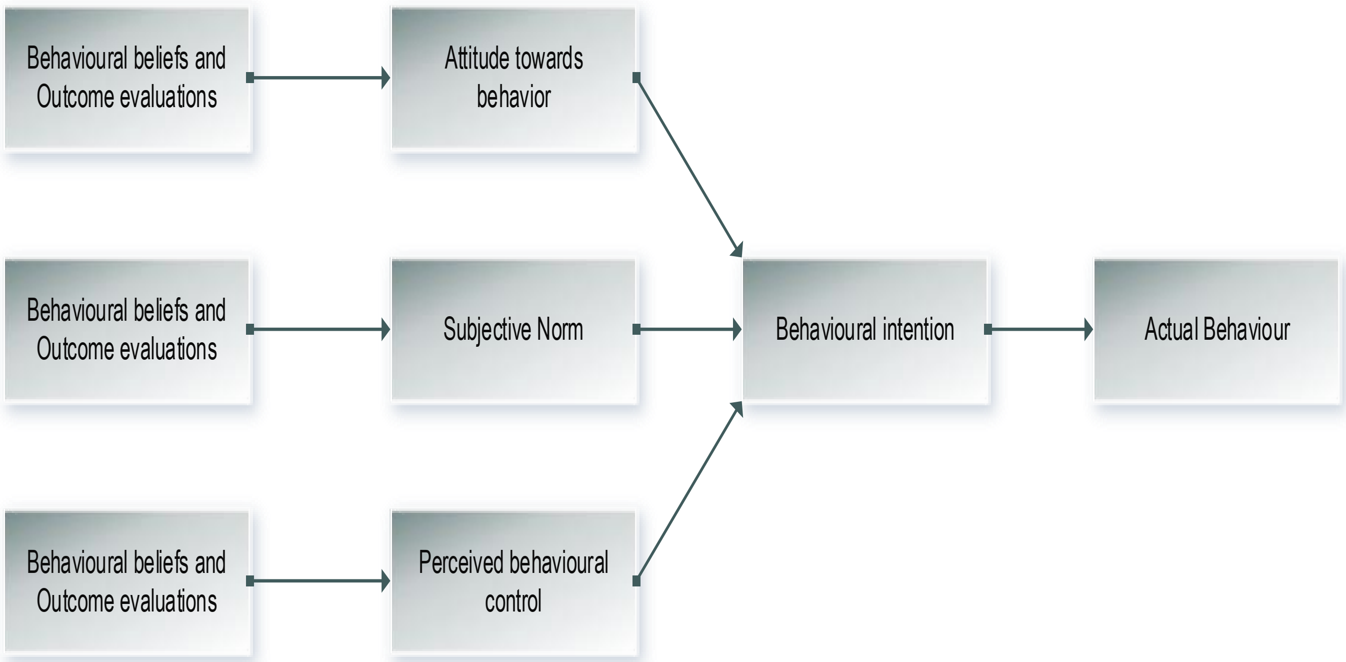

Behavioural beliefs and Outcome evaluations
Attitude towards behavior
Behavioural beliefs and Outcome evaluations
Subjective Norm
Behavioural intention
Actual Behaviour
Behavioural beliefs and Outcome evaluations
Perceived behavioural control

Figure 19. The Theory of Planned Behaviour

Source: Ajzen (2002)

Figure 19 above gives a schematic representation of the TPB. The perceived behavioural control, subjective norms and behavioural intentions determine the individual's behaviour. The TPB will be very useful for building an ISC, especially since the employees are the unintended administrators of their devices. As such administrators have perceived control of the BYOD mobile devices, the security of the device is determined by their subjective norms; that is, their belief about how the device should be secured. Their behavioural intentions will determine whether or not they want to observe the security of information contained on the device. Applying this in the banking sector, the TPB is an important theory in ensuring that employees are trained to observe the governance and regulatory dictates of the industry (Nayak, Nath, & Goel, 2014). These combined with their attitudes, knowledge and habits will result in the right behavioural intention towards information security. Chapter 7 of this document discusses this analogy in detail, resulting in the formulation of the research output of this study.

4.5 Information Security, Behaviour and Culture

An ISC greatly influences the interactions between employees' behaviour and the information security attributes. The research outcomes of the studies carried by Da Veiga and Eloff (2010) showed that information security components influence information security behaviour, which in turn fosters the ISC.

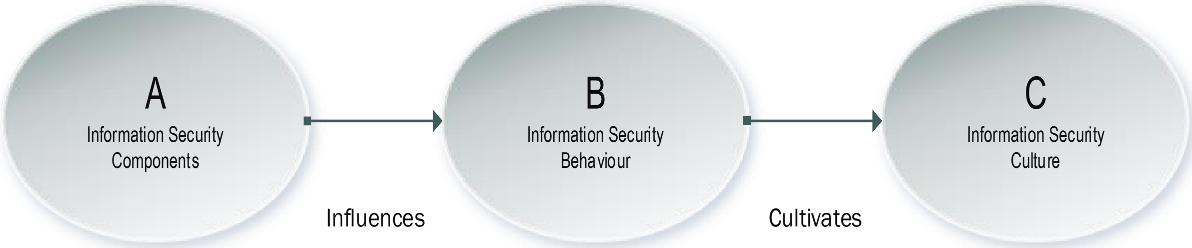

A
Information Security Components
Influences
B
Information Security Behaviour
Cultivates
C
Information Security Culture

Figure 20. Influencing Information Security Behaviour and Cultivating an Information Security Culture

Source: Alfawaz et al. (2010)

Figure 20 shows that for organisations to cultivate an ISC there is a need for a close correlation between the information security behaviour and information security components. Information security behaviour entails those aspects of employee behaviour which deal with the way employees interact with the information assets in a responsible manner (Alfawaz et al., 2010). Information security components refer to those tools and mechanisms, such as an information security policy, that the organisation embraces in managing its information assets.

4.6 Managing Information Security Culture

Information security as a subculture of OC shares a number of common attributes with ISC. Schlienger and Teufel (2003) state that culture must be maintained and changed continually. They further argue that this is a continuous process, which in essence is a cycle of evaluation and change maintenance (Schlienger & Teufel, 2003). The initial step is to analyse the culture for information security (a process they described as pre-evaluation) (Schlienger & Teufel, 2003). The outcome of this pre-evaluation is either that the culture will fit the organisation or that it does not fit. If the culture fits it will be reinforced, if it does not fit then the culture will have to be changed so that it fits in with the organisation's strategy.

The decision and direction that these changes take will be mainly informed by the strategic focus for the organisation. Organisations adopt technologies in order to achieve their strategic initiatives and various change management processes are following individually by organisations to achieve the strategic focus. The ISC management cycle can be explained by the figure below.

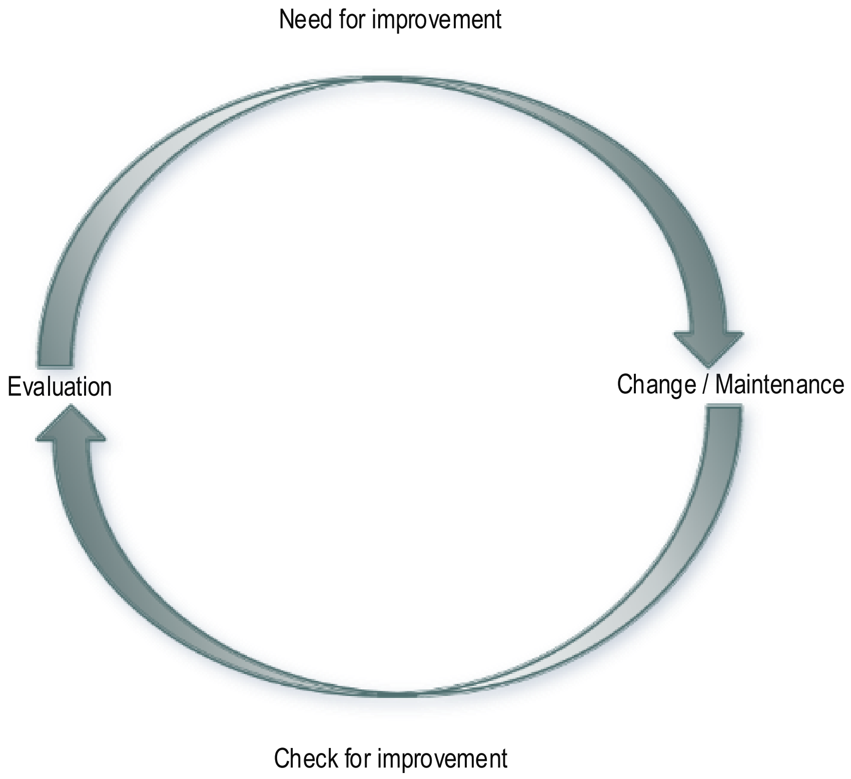


Figure 21. The Information Security Culture Management Cycle

Source: Schlienger and Teufel (2003)

The model above shows that the management of information security is a cyclical process, which is mainly predicated on the organisation's strategy. This further confirms that information security management is an ongoing process which is premised on the organisational behaviour which, in turn, is a function of the employees' collective behaviours towards the way things are done in an organisation. The next section examines the nature of the ISC which correspondingly has a bearing on the way information security can be managed.

4.7 The Nature of Information Security Culture

Research has shown that technical solutions alone are insufficient in managing information security incidents. A combination of technical and non-technical solutions provides a commendable level of comfort in managing information security. Zakaria et al. (2007) argue that information security is considered a technical subject; as such, many information security practitioners come from a technical background. This position is cited as one of the reasons why technical solutions for information security management have comparatively gained more attention than non-technical solutions.

Non-technical aspects are relevant in building an ISC as they aid in making it a routine for every employee to exercise information security as a day-to-day task. When employees from all levels absorb ISC as the norm, the overall security of the organisation will grow. The nature of information security as a culture is such that ownership needs to be available from all levels: senior management, middle management and even the lower levels. Figure 22 shows that there is a continuum from the national culture, organisational culture and information security culture, with technical and non-technical members also needing to be given the same buy-in and ownership. This will become a dynamic aspect of the organisation driven by the strategy and innovations emanating from the information security systems and devices.

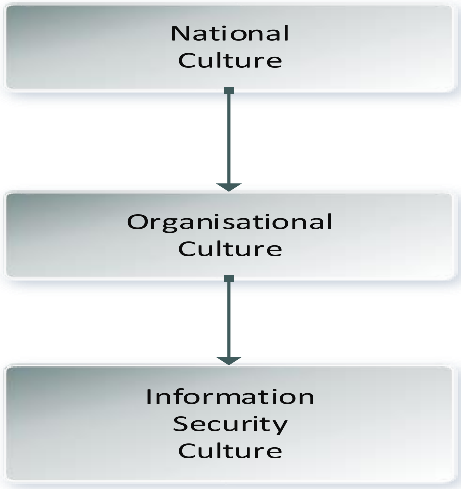


Figure 22. The Information Culture Hierarchy

Source: Adapted from Li and Siponen (2011)

The ISC exists as part of a hierarchy as shown by the diagram in Figure 22. The diagram shows that OC is a subculture of national culture and ISC is a subculture to OC.

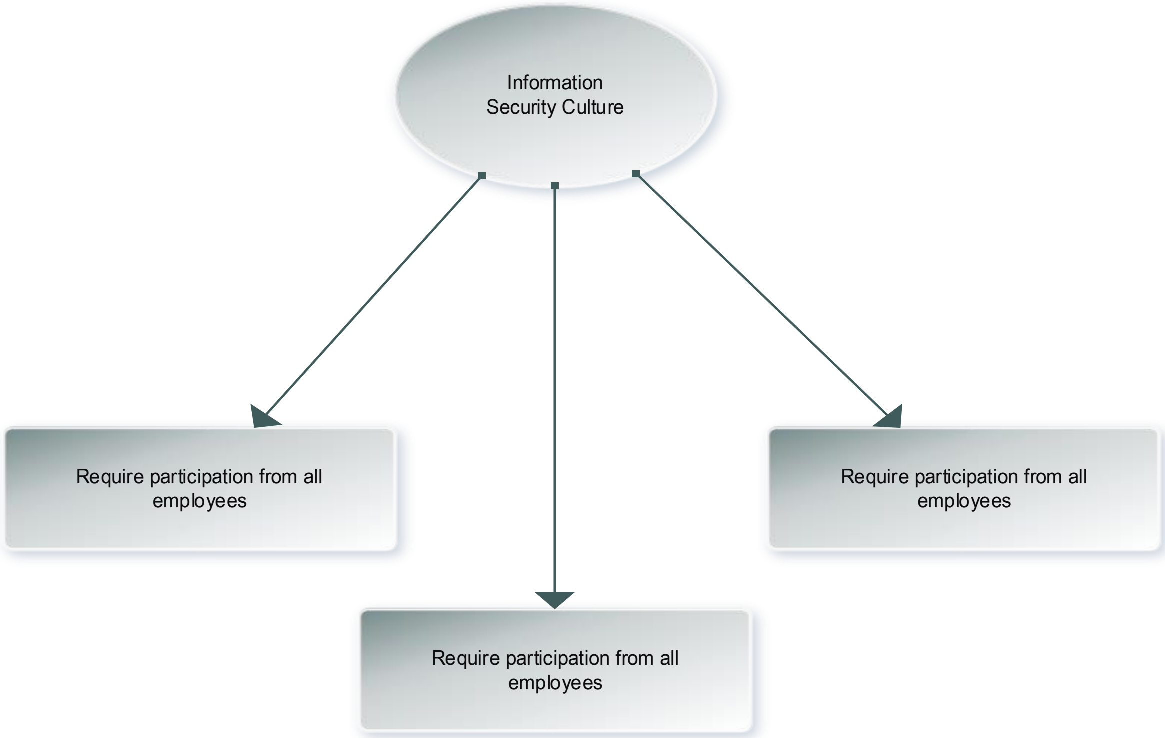

Information Security Culture
Require participation from all employees
Require participation from all employees
Require participation from all employees

Figure 23. Characteristics of Information Security Culture

Source: Zakaria et al. (2007)

Figure 23 shows the common characteristics of ISC as identified by the research findings of Zakaria et al. (2007). The figure shows that an ISC requires participation from all employees at all levels with different technical orientations. This brings a convergence of employees' subjective norms. Subjective norms are a person's own estimate of the social pressure to perform the target behaviour and are assumed to have two components. These interact and are beliefs about how other people, who in some way may be important to the person, would like them to behave (normative beliefs) (Bada, Sasse, & Nurse, 2015). These two components are:

i. **Perceived behavioural control**. This is the extent to which a person feels able to enact the behaviour. It has two aspects – how much a person has control over the behaviour and how confident a person feels about being able to perform or not perform the behaviour. It is determined by control beliefs about the power of both situational and internal factors to inhibit or facilitate the performing of the behaviour.

ii. **Direct measures and indirect (belief-based) measures**. These are psychological (internal) constructs. Each predictor variable may be measured directly, for instance by asking respondents about specific behavioural beliefs and outcome evaluations. Direct and indirect measurement approaches make different assumptions about the underlying cognitive structures and neither approach is perfect.

The ISC is, in fact, characterised by both technical and non-technical aspects, which will ensure a commendable level of comfort in dealing with information assets.

4.8 Benefits of a Culture of Security

Ula, Ismail, and Sidek (2011) argue that information security has become a critical component of modern banking. Culture is a necessary precondition for the establishment of an appropriate level of security in any organisation. ISACA (2009, p. 30) notes that, “the greatest benefit of a culture is the effect it has on other dynamic interconnections within an enterprise” (p. 40). A culture leads to the establishment of a greater level of internal and external trust for organisations (PwC, 2011). The establishment of a security culture will result in consistency of results, easier conformance, and compliance to laws and regulations. This will create a secure organisation.

Trust is one of the key result areas for organisational performance. Employees work better in organisations they trust and customers give more business to organisations they trust. Trust can be seen as “an ingrained assuredness that a person, thing is indeed what he/she/it purports to be” (Musselwhite, 2011, p. 41). The absence of a culture of security in an organisation will result in information becoming less reliable. This may in turn result in poor decision-making, since the decisions made will be based on fallacious or incomplete information (Ross & Masters, 2005). Poor decision-making will translate into reputational risk for the organisation, loss of market share, loss of customer confidence, credit risk and massive financial loss (Beidokhti & Ghaderi, 2011).

4.8.1 The Banking Example

A study by Salvi and Kadam (2014) on the HDFC Bank of India reported that “culture, ethics and behaviour of individuals and the enterprise are often underestimated as success factors in governance and management activities. Nonetheless, they are important contributors to the success of an enterprise" (p. 7). Even big banks that generally do a better job of security can be victims of security breaches. Any mishandling of confidential information assets can result in huge financial loss, and the bank's reputation will be severely damaged and a bank's entire business model is based on the trust of its customers.

The bank shareholders appoint a board of directors to ensure that all day-to-day operations are performed with integrity. The board in turn appoints an executive management team that hires technical employees to carry out the bank's day-to-day operations. According to Von Solms (2001), the basis of the hiring process is the trust shared by both levels. Information security comprises technology, processes and people behavioural systems. Although the technical aspects of information security require due attention, a more threatening and underrated aspect of information security is the human element (Lim, Ahmad, Chang, & Maynard, 2010). Many losses are not caused by a lack of or faulty technology but rather by technology users and faulty human behaviour. Martins and Eloff (2006) underline that employees' behaviour and their interaction with computer systems have a significant impact on the security of information. The purpose of an ISC is to address the various human factors that can affect an organisation's overall information security efforts (Van Niekerk & Von Solms, 2005).

After conducting a number of studies on the ISC in the Ethiopian banking sector, Woretaw and Lessa (2012) noted that banks prioritise engagement in ICT as one of their key strategic initiatives resulting in a commendable bank performance. For the majority of banks, information security is driven by the group information security department headed by the chief information security officer (CISO). Another study by Zakari and Poku (2013) on the banking industry in Ghana concluded that the success of all banking operations is based on the trust and the security culture that banks are associated with. Customers keep the details of their financial spend in a bank. In a related finding on the Nigerian banking sector, Babatunde, Selamat, and Salman (2014) argue that a culture of security is a key performance indicator in the banking industry, making information security the hallmark of a successful bank. From the literature review above we can conclude that in order to remain in business, banks require a culture of security. Since culture involves human beings, there are always challenges when it comes to the acceptance of the changes that comes with a new culture. These challenges will have an impact on how a security culture eventually pans out. In Chapter 7, individual traits of knowledge, habit and training are singled out in detail as being central to the employees' behavioural intention towards an information security. These are combined with organisational traits of governance, environment and the training that the employees receive from the organisation.

From the HDFC Bank survey, the following eight information security behaviour factors were identified:

i. **Information security is practised in daily operations (individual and organisational traits)**. The researchers identified that the banks' expectations of employees were included a principle of zero tolerance for unacceptable behaviour relating to information security. They also revealed a plan of rewarding good behaviour, recognising and rewarding people for good work regarding risk management, and constantly reminding everyone through the tagline "Security is incomplete without you". This has ensured that information security is practised in daily operations. individual and organisational traits are thus visibly at play in this factor. Chapter 7 will discuss these traits in detail.

ii. **People respect the importance of information security policies and principles (employee behaviour and organisational environment)**. Salvi and Kadam (2012) found that a security culture has been built over time through constant training efforts. Employees understood the importance of information security and took security initiatives seriously. Audit also played an important role in enforcing various security policies and principles.

iii. **People provided with sufficient and detailed information (employee knowledge and organisational training)**. This included information security guidance through training provided by the bank and encouragement to participate in and challenge the current information security situation.

iv. **Everyone is accountable for the protection of information in the enterprise (awareness training).** The information security group is responsible for identifying and managing the risk whereas the business heads are held ultimately accountable. This makes all the stakeholders feel both responsible and accountable for the protection of information in the enterprise.

v. **Stakeholders are aware of how to identify and respond to threats to the enterprise (governance and a conducive environment).** Threat identification is part of the training provided to stakeholders. Stakeholders are encouraged to report incidents, for example send an email to the ICT department about any spam or phishing email received. The incidents reported to ICT on a day-to-day basis indicate how everyone has been trained to identify and report such incidents.

vi. **Management proactively supports and anticipates new information security innovations and communicates these to the enterprise (governance)**. There is full management support to interact with industry and share knowledge and experience with a larger audience, as well as learn from other enterprises. Management is also receptive to accounting for and dealing with new information security challenges.

vii. **Business management engages in continuous cross-functional collaboration to allow efficient and effective information security programmes (environment)**: The structure of various committees is an example of continuous cross-functional collaboration. Making information security independent of the IT function has provided a broader reach and direct access to various business groups across the organisation.

viii. **Executive management recognises the business value of information security (governance and environment):** The CIO works at a strategic level, reporting to a senior person in the bank. This has empowered the CIO to drive various information security initiatives with a great amount of freedom. This is a good indication of management's recognition of the business value of information security leadership.

4.9 Challenges in Developing a Culture of Security

Alhogail et al. (2014) argue that the human factor is a central aspect of the security of information in organisations. If proper change management is not followed, the culture will experience challenges in implementing the expected change within the organisation. Related research by Doan (2014) singles out attributes such as behaviour, attitude and personality as having a significant impact on how the culture of security can be developed. While some employees have a "we have always done it this way" attitude, others have personalities that do not welcome change. This will reduce the overall uptake of a proposition. The absence of the right skills can also negatively impact the development of a security culture.

Whilst other threats to information security exist, the user of the information systems remains the biggest threat. This user threat poses a serious risk whatever the amount invested in technologies (Von Solms & Von Solms, 2004). Most organisations view information security as a technology challenge; as such drawing attention to the fact that the actual challenge is from within requires more than a recommendation. Human beings are often driven by their personal and social identities, which shape their habits based on the knowledge they have. These personal and social identities inform their unique attitudes, beliefs and perceptions, which they carry to work and confer on their role profiles in the organisation.

One of the major challenges to developing a culture of security is skill, which is usually a measurement of employee knowledge. Udeh and Dhillon (2008) state that in most organisations, employees have developed "security blindness" in dealing with information assets in their day-to-day operations as a result of their personal and social attributes of doing things in a particular ways, which makes up their habits. Nonetheless, these personal and social identities can be changed to develop and impose a culture of information security (Schlienger & Teufel, 2003). Thomson, Von Solms, and Louw (2006) maintain that the strongest link in any organisation's security can be formed by well-trained and conscientious employees. Organisations have come up with various ways to combat insider risks; these include technology, policies, procedures and practices. Nevertheless, these are still devoid of a structured framework that gives a reference point for practitioners when creating a culture of information security within organisations.

4.10 Creating an Information Security Aware Culture

Building a culture entails transitioning from one culture to another. This process involves moving from the current state to a preferred state. Bridges (1987) developed a model for transition management which consists of three phases, namely, ending, neutral zone, and new beginning. According to this model, these phases are not separate phases with clear boundaries but rather are a transition that involves a gradual changeover as dominance is passed from one stage to another. Adapting this model for creating an ISC, an organisation has to start (the first phase) by ending its old way of doing things. This will include persuading people to let go of the past and acquire new ways of doing things. The next phase, the neutral zone, is characterised by confusion and lack of direction. Finally, the third phase, the new beginning, is characterised by accepting the new way of doing things.

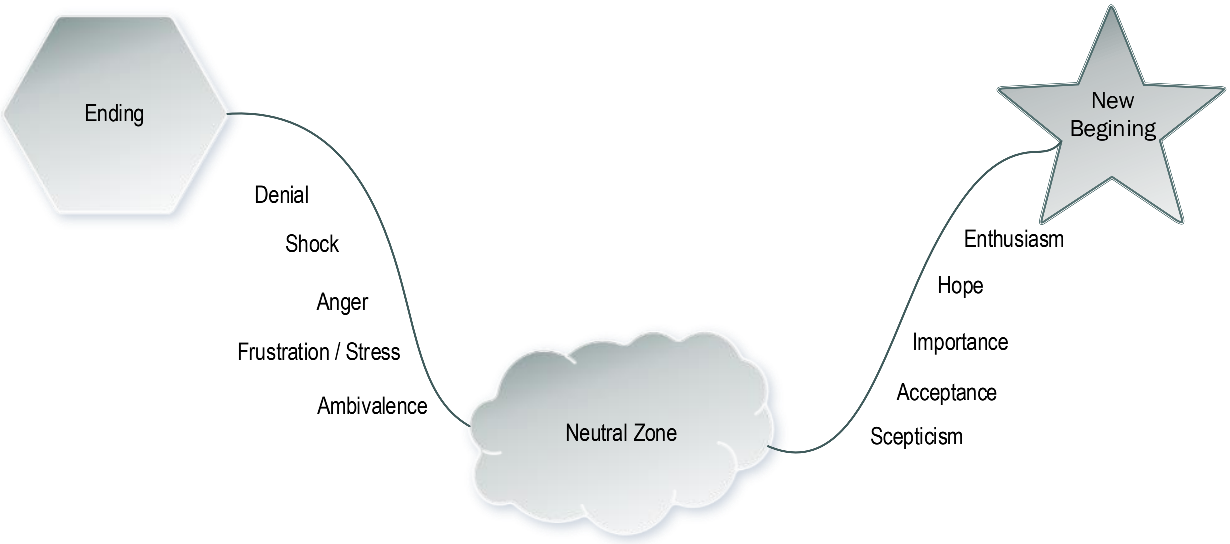


Figure 24. Three-phase Transition Process

Source: Bridges (1987)

Understanding these phases will assist organisations in giving the appropriate focus to building an ISC around BYOD. Building an ISC will only be possible if the proper acceptance base is made by propagating the appropriate mind set in the people who are driving the process (Ngo et al., 2005). Chapter 5 will discuss how to build an ISC. The next section will examine some of the models for building an ISC and will randomly select theories and examine them to set the basis for the model in building an ISC around BYOD.

4.11 Existing Frameworks Representing Information Security Culture

Frameworks are used to form the basis of a model. The Oxford University (2015) business dictionary defines a framework as a "broad overview, outline, or skeleton of interlinked items which supports a particular approach to a specific objective, and serves as a guide that can be modified as required by adding or deleting items". Nilsen (2015) defines theories as "a set of analytical principles or statements designed to structure our observation, understanding and explanation of the world" (p. 1). Nilsen (2015) further differentiates a theory from a framework by pointing out that a framework usually denotes the overview of a structure, system plan, outline, or schema composed of various descriptive categories without providing explanations.

Several scholars have proposed frameworks in order to assist organisations in establishing an ISC. A literature review on the concept of ISC conducted by Alhogail and Mirza (2014) concluded that most publications did not present a framework but rather addressed general terms of information security. This explains why the creation of a model for building an ISC for BYOD becomes an important research focus area. This section will explore various frameworks that discuss different issues related to ISC.

Based on Schein's corporate framework, Schlienger and Teufel (2003) presented a framework that addresses the internal marketing aspects of ISC. The framework is centred on five main phases:

i. **Pre-evaluation.** This is where the main gap between security and policy is examined, leading to the identification of areas that need improvement.
ii. **Strategic planning**. This includes the setting up of a clear culture that is supported by policy.
iii. **Operative planning**. This addresses field aspects like management buy-in, internal communication, security training as well as a training programme.
iv. **Implementation.** This section addresses four phases, namely, internal communication, management commitment, knowledge transfer, and employee commitment.
v. **Post-evaluation**. This addresses the post-implementation review.

Zakaria (2004) proposed another framework related to Schein's studies but this time based on the model of OC. In this study, Zakaria (2004) posits the use of interpretive epistemological research that includes semi-structured interviews, questionnaires, direct observation and observation for data collection.

Da Veiga and Eloff (2008) present the Comprehensive Information Security Framework (CISF) for cultivating an ISC within an organisation. The CISF is a set of information security components to be implemented by organisations in order to address the human processes and technical threats that would deter the establishment of an acceptable ISC.

Van Niekerk and Von Solms (2005) created a model that integrated Bloom's learning taxonomy and e-learning as an educational design and delivery backbone for the organisational change process. In the model, they make use of Schein's perspective on OC. They also suggest that information security knowledge is a prerequisite for an effective ISC and is also a key component in building an ISC. If employees have knowledge of information security, building a culture will be easy and less tedious.

Another conceptual framework for classifying and organising the characteristics is proposed by Alfawaz and Nelson (2010). Their work, as explained in section 4.3, focuses on the national culture and OC classified into different modes of not knowing–not doing, not knowing–doing, knowing–not doing mode, and knowing–doing mode.

Several other frameworks were put forward from the literature study, some of which touched on human aspects such as training but did not put any special focus on the employee and the means by which to influence his/her behaviour. Alhogail and Mirza (2014) argue that the existing frameworks lack a comprehensive analysis that integrates the employee, the organisation and the technology. The table below contains a comprehensive list of frameworks and the aspect of information security that they address.

Table 8. An Overview of Information Security Frameworks

Study	Goal of the Framework Presented by the Study
Chia, Maynard, and Ruighaver (2002)	Study the effect of organisational culture on the information security culture
Schlienger and Teufel (2003 a)	Analyse the security culture of an organisation in order to create. change and maintain information security culture
Zakaria (2004)	Data collection in information security culture research
Koh,Ruighaver, Maynard, and Ahmad (2005)	Analyse how security governance influences the security culture
Chang and Lin (2007)	Quantify the effects of organisational culture factors on the effectiveness of implementing information security management
Ruighaver, Maynard, and Chang (2007)	Define the concept of information security culture.
Dojkovski et al. (2007. 2010)	Fostering an information security culture in SMEs in a national setting
Lim et al (2009)	Determining to what extent the information security culture is embedded in organisational culture
Alnatheer, (2014)	Understanding information security culture in the Saudi context
Alfawaz et al. (2010)	Classifying and organising the characteristics of organisational subjects involved in information security practices
Da Veiga and Eloff (2010)	Comprehensive framework to establish information security culture

Van Niekerk and Von Solms (2005, 2006, 2010)	Foster an information security culture in the organisation through e-learning

Source: Al Hogail and Mirza, (2014)

4.12 Relationship between Organisational Culture and Information Security Culture

For years, ISC has remained one of the top-ranked concerns of academic researchers and industry practitioners, as evidenced by the fact that the Organisation for Economic Co-operation and Development (OECD) has introduced guidelines for a culture of information security (Lim et al., 2009).

In order to examine ISC properly, there is a need to understand OC. Lim et al. (2009) argue this by stating that there are three types of relationships between OC and ISC, namely, a standalone culture separate from OC; a subculture or a subset of OC; and part of the OC embedded within. This study will take the view of ISC as a subculture of OC.

4.13 Conclusion

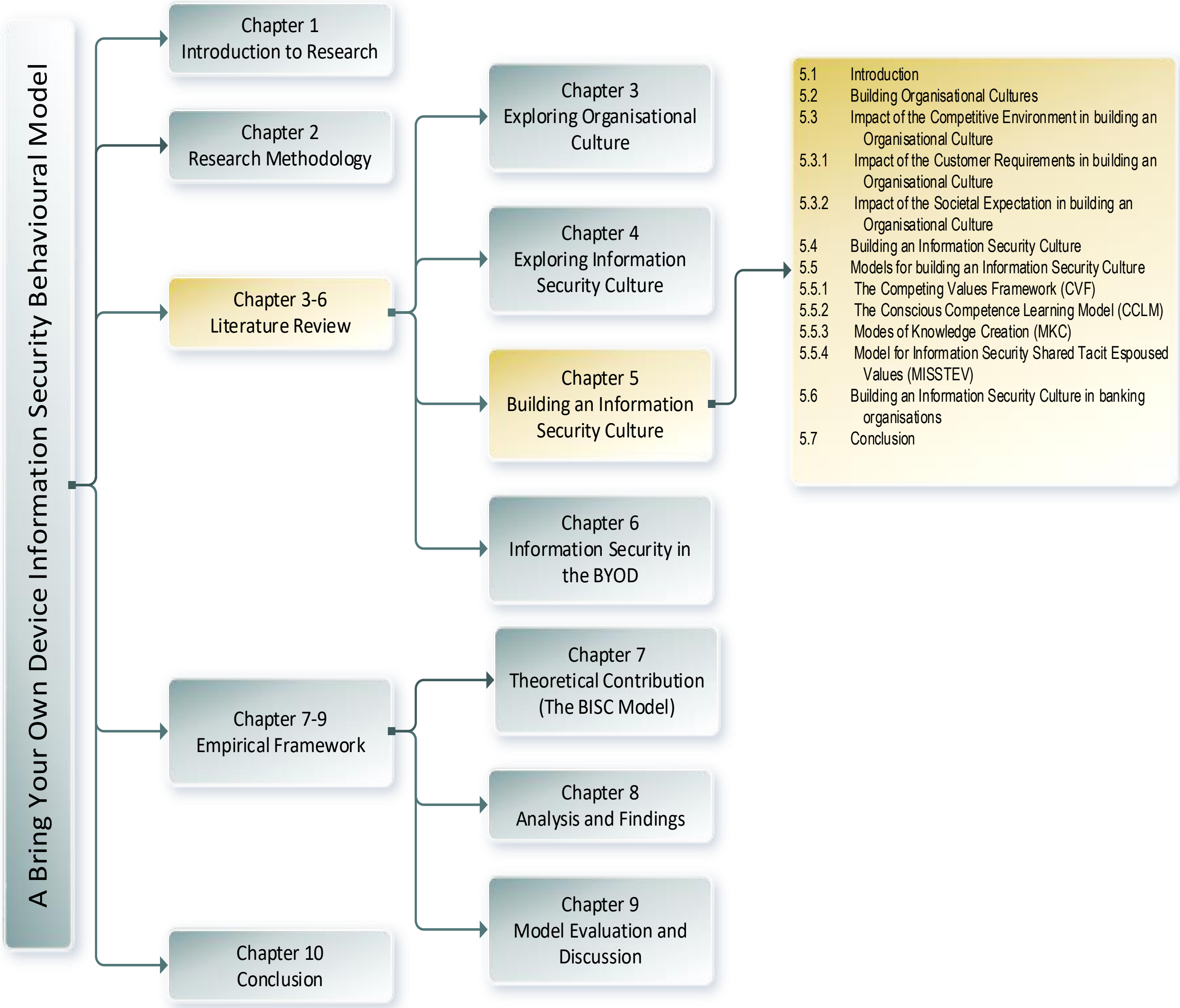
ISC has gained importance, resulting in many researchers working to understand it comprehensively. Von Solms (2000) suggests that it is “a culture of Information Security to be created in a company by instilling the aspects of information security to every employee as a natural way of performing his or her daily job” (p. 618). In a related finding, Schlienger and Teufel (2002) propose that “security culture should support all activities in such a way that information security becomes a natural aspect in daily activities of every employee” (p. 7). Several authors also argue that information security, as a culture, is vital in ensuring organisational information security (Vroom & Von Solms, 2004).

This chapter began by positioning ISC as subculture of OC. This led to ISC being defined in terms of the way it is managed in a given organisation. The chapter further explored human behaviour by examining theories that explain how human behaviour is created. The TRA maintains that individual behaviour is driven by behavioural intentions which are a function of an individual's attitude toward the behaviour and the subjective norms surrounding the performance of the behaviour. TPB, on the other hand, works best when the behaviour is NOT perceived to be under the person’s control. TPB maintains that intentions are the precursors of behaviour. In terms of the TRA, constructs are motivational and depend on the strength of the intent to perform the behaviour. These theories support the creation of a BYOD ISC by bringing rigour to one of the constructs of the model that address attitude habit and knowledge. All these combined will form part of the answer to the research statement which seeks to mitigate the risks posed by the unintended administrator created by the BYOD phenomenon in the Zimbabwean commercial banking sector. The unintended administrator poses a major information security risk for organisations if not properly controlled.

The chapter proceeds by exploring prior studies to see how an ISC can be created. The same approach is followed in exploring the relationship between OC and ISC. From the insights gathered from Chapters 2 and 3, strong OC and ISC are the key imperatives for modern-day business environments. Accordingly, businesses have to embark on strategies that ensure their safety as they leverage on the modern trends in technology. In support of this, Von Solms and Von Solms (2006) confirm that information security is the fourth wave of change that businesses have to focus on for competitive advantage. The next chapter will examine the means by which this fourth wave of information security can be built as a culture in organisations.

Chapter 5 : Building an Organisational Information Security Culture

"A culture is like an immune system. It operates through the laws of systems, just like a body. If a body has an infection, the immune system deals with it. Similarly, a group enforces its norms, either actively or passively." – Henry Cloud


A Bring Your Own Device Information Security Behavioural Model
Chapter 1
Introduction to Research
Chapter 2
Research Methodology
Chapter 3-6
Literature Review
Chapter 3
Exploring Organisational Culture
Chapter 4
Exploring Information Security Culture
Chapter 5
Building an Information Security Culture
Chapter 6
Information Security in the BYOD
Chapter 7-9
Empirical Framework
Chapter 7
Theoretical Contribution (The BISC Model)
Chapter 8
Analysis and Findings
Chapter 9
Model Evaluation and Discussion
Chapter 10
Conclusion
5.1 Introduction
5.2 Building Organisational Cultures
5.3 Impact of the Competitive Environment in building an Organisational Culture
5.3.1 Impact of the Customer Requirements in building an Organisational Culture
5.3.2 Impact of the Societal Expectation in building an Organisational Culture
5.4 Building an Information Security Culture
5.5 Models for building an Information Security Culture
5.5.1 The Competing Values Framework (CVF)
5.5.2 The Conscious Competence Learning Model (CCLM)
5.5.3 Modes of Knowledge Creation (MKC)
5.5.4 Model for Information Security Shared Tacit Espoused Values (MISSTEV)
5.6 Building an Information Security Culture in banking organisations
5.7 Conclusion

5.1 Introduction

Mohanty (2015) argues that an organisational culture (OC) is built from organisational characteristics that influence the employees' performance, as well as the overall effectiveness of the organisation in relation to competition and the operating environment. In agreement with this perspective, Munteanu and Fotache (2015) remark that building an information security culture (ISC) entails a process of introducing a new concept that involves human behaviour and attitudes. Process flow management tools and methodologies, like the plan-do-check-act model (PDCA) introduced by the ISO/IEC, provide a means for measuring transformational processes such as culture change in an organisation (Roer, 2015). In a related finding, a report on information security from Cisco Systems (2016) observed that "[t]he threat to information assets has never been so great. Vulnerabilities range from eavesdropping on a phone call to a stolen laptop or even a misconfigured password. Yet, small changes in behaviour can have a huge upside for information security" (p. 1). Considering that behaviour is an acquired characteristic of human existence, this observation suggests that there is a need to rethink behaviour at the organisational level.

Tharp (2009) states that culture grows and can be built through either the active or passive participation of the organisational stakeholders, bearing in mind that the employee is the first step in building the culture of an organisation. Cultural changes are planned changes that do not happen by accident but rather require careful change management (Haworth, 2015). This chapter will examine how an OC can be built. The study will then examine how a BYOD ISC can be built. Considering that an ISC is a subculture to OC, the study will explore the way ISC is built. The chapter will also investigate banking examples of how ISCs can be created as part of a successful OC.

It is important to recognise the differences between cultural profiles because organisations always have a dominant culture and may also contain many different subcultures (Bibb, 2010). By understanding and accepting various cultures, organisations can harness the differences to successfully build an organisational ISC. The OC is strongly influenced by the characteristics of the industry in which the organisation operates and that the individual organisation requires for survival, such that within industries, certain cultural features will be widespread among organisations, and these most likely will be quite different from the characteristics found in other industries (O'Donovan, 2004).

5.2 Building an Organisational Culture

Haworth (2014) states that OC change requires a planned change management process and cannot happen by accident, whilst Cameron and Quinn (2006) argue that building an OC is an intra-organisational process which organisations require in order to survive. OC studies have shown that the primary reason why most culture changes fail is that they are usually implemented drastically without receiving employee buy-in and they demand too much too quickly. Earlier studies by Gordon (1991) concluded that whilst culture is unique to a given organisation, the industry that the organisation operates under exerts influences that direct certain cultures in that industry. Because of this relationship, the potential for changing an organisation's culture is limited to actions that are neutral to, or directionally consistent with, industry demands. Organisations usually have a main OC which consists of many corresponding, or sometimes totally conflicting, subcultures (Bibb, 2010). Khatib (1997) views a subculture as being part of a culture that has similar elements to the main OC of shared values and norms, but differing from the dominant cultural factors because of the differing experiences faced by employees, their job profiles or even the changing environment. Examples of subcultures can include the recruitment culture inherent in human resources, the remuneration culture, the reward culture and many others. Haworth (2014) highlights that OC change arises from the following three basic factors:

- **Evolutionary change.** This is when a culture is built by letting change happen gradually and often naturally over time, observing organisation-wide transformations. This is often well understood by the employees, will receive the greatest employee buy-in, and often results in the dominant cultures growing. Evolutionary change has traceable and clearly marked stage gates which will be observed as maturity phases in the change process. Proper change management processes are usually followed and result in the creation of the organisation's main culture.
- **Focused change.** This happens when measures for change are exacted upon only certain fundamentals or subcultures. This approach also observes a predefined change management process and is often measured by meeting the targets set. Focused change is often rigorous and is focused on results. This type of change sometimes disregards the values and beliefs among the employees.
- **Revolutionary change.** This happens when an organisation forces employees to change the OC drastically. This is usually a turbulent method that often faces resistance. Revolutionary

change does meet the expectations of the management and is viewed as a somewhat tyrannical or draconian approach to building a culture.

Some authors suggest that organisations do not necessarily build cultures from the roots, but rather organisations transition from one culture to another. This process is often met with challenges if proper change management processes are not followed. The way employees receive the change management process will depend on the industry type as well as the way the management introduces the change process (Mohanty, 2015).

Based on industry-specific assumptions, Gordon (1991) identified three classes of industry variables that have an impact on how organisations build their culture. Topmost among these expectations is the assumption that: "If the solution works, and the group has a shared perception of that success, the value gradually starts a process of cognitive transformation into a belief and, ultimately, an assumption" (Gordon, 1991, p. 7).

The three classes are:

- Competitive environment
- Customer requirements
- Societal expectations.

Figure 26 is a schematic model for industry-driven culture formation showing the way in which the three subclasses influence the building of a culture in an industry.

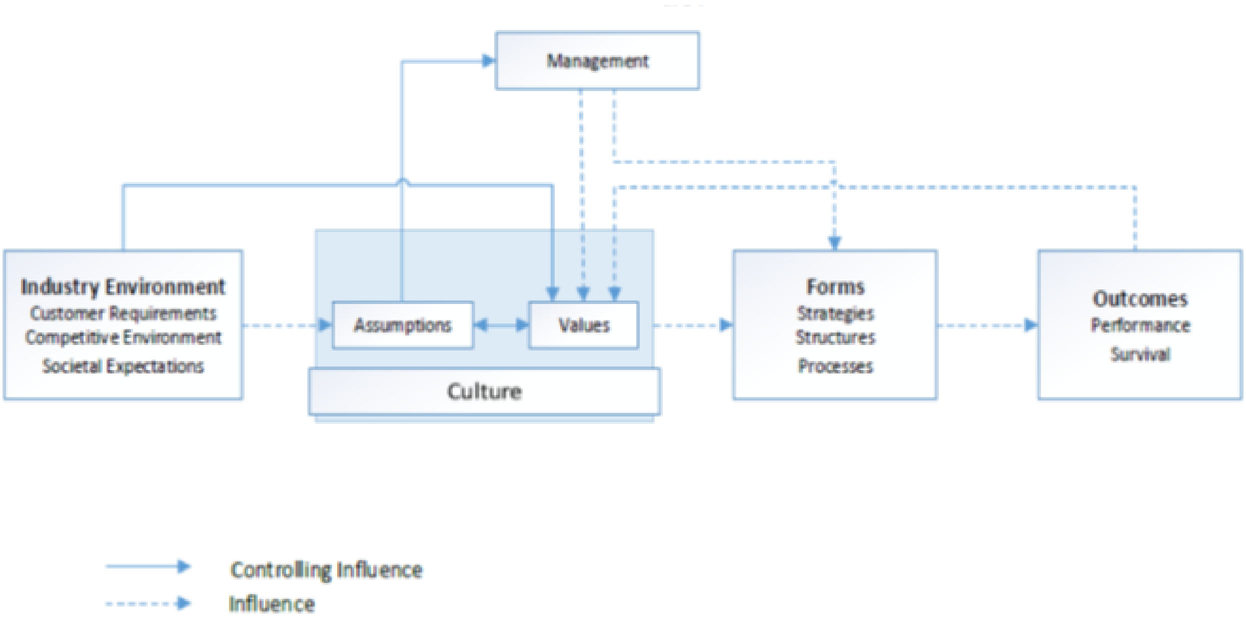


Figure 25. A Model for Industry-driven Culture Formation

Source: Gordon (1991)

At the core of the model of industry-driven culture formation is the belief that regardless of the inherent cultures within organisations, the industry trends play a pivotal role in building an OC. The model shows that the industry environment characterised by customer requirements, the competitive environment and the societal expectations have a controlling influence on the assumptions and values that the organisations uphold. These will, in turn, influence the formation of a particular culture within the industry. Strategies, structures and processes, as well as performance and survival, influence the overall culture formation process but do not necessarily have a controlling stake. The next section addresses in detail the three classes of industry variables that influence the way cultures can be created. The section ends by examining cases related to the banking industry to identify the way in which the industry influences the formation of culture. The analysis will also examine cases where a technology culture has been implemented in the banking industry, thereby giving impetus to a study on how banks in developing countries develop cultures around the implementation of technology taking into account the competitive environment, customer requirements, and societal expectations.

5.3 Impact of the Competitive Environment on Building an Organisational Culture

Assumptions that form the basis of an OC originate from the competitive environment within which the organisation operates. The competitiveness of the environment can be viewed in terms of a legislated monopoly where there is no contention at all to competitiveness where there are several players participating in the same industry. Studies have been conducted on the topic of the dimensionality of the competitive environment by various scholars including Sharfman and Dean (1991), Strang and Aldrich, (2002), and Aldrich and Auster (1986), who have all been consistent in pointing out the following three dimensions:

i. **Complexity or product market concentration.** This refers to the number and variability of firms in the competitive environment. The amount of variability determines the complexity of the market.

ii. **Stability or dynamism.** This addresses the rate of environmental change that will determine whether the product will reach maturity or will be overtaken by newer products before the product finishes the growth process. In the case of enterprise mobility, this dimension will be instrumental in explaining how Bring Your Own Device (BYOD) has changed the traditional Use What You are Told (UWYT) model. The rate of change in the enterprise mobility information security standards will be examined from this perspective. This chapter will also address the change associated with the ISC for the commercial bank in Zimbabwe, which will be the basis for this study.

iii. **Munificence.** This speaks to the extent to which the environment can sustain the growth of a service or product. For this study, this dimension will be instrumental in exploring the extent to which the banking environment can sustain the building of an ISC around BYOD, considering that ISC is always playing catch-up to changes in technology (Leavitt, 2011).

The complexity of the environment determines the players' competitiveness. Early studies by Duncan (1972) showed that the complexity of the environment and its dynamism cause uncertainty in management's decision-making. When it comes to culture, it is reasonable to anticipate that the more complex and competitive the environment is, the more it will affect the uncertainty resulting from the variety of competitors and the evolution in products, technology and trends. A highly dynamic environment is characterised by complex competitive practices where an employee finds derivative values that correspond to institutionalising the means by which the organisations conduct their business. Smith and Levins (1970) argue that specialised structures are most appropriate in a stable environment, whereas Rumelt, Schendel, and Teece (1991) found that increasing diversification in organisations leads to decentralised structures. Pfeffer and Salancik (2003) argue that efforts to eliminate uncertainty emanate from greater uncertainty through coordination and centralisation, resulting in the creation of larger organisations operating in highly regulated and politically controlled environments. However, this will only apply in an environment of low munificence (case of resource scarcity). In Chapter 7 of this thesis, environment is discussed in detail as one the key traits that determine behavioural intention towards information security.

Munificence has a direct influence on culture. Gordon (1991) posited as follows:

> "Industries that can support considerable growth usually develop values around risk taking and innovation in order to try to take advantage of the growth opportunities. A basic assumption of the computer industry is that better technologies will continue to be developed and will supplant older ones. If, however, there were few buyers for computers of any type, that assumption would be less true, because companies would not be able to invest heavily in R&D efforts. Thus, munificence also may have a direct effect on industry-driven assumptions" (p. 404).

The next section explores the impact of the customer requirements on the building of an OC. Customers have a tendency to dictate the trends that technologies follow mainly because of their preferences.

5.3.1 Impact of Customer Requirements in Building an Organisational Culture

The pre-eminence of property rights has been replaced by the pre-eminence of human rights, giving rise to an era by which cultures in organisations are largely dictated by societal values and expectations. Gordon (1991) states that, prior to 1960, societies' primarily expected organisations to provide services, jobs and products without any restrictions on their operations. Today, customer requirements largely command the way the OC is built. For instance, in building a culture around BYOD, the type of device being used is dictated by the quest to satisfy customer preferences. King (2012) confirms this, stating that "[on] the Web and on Mobile the customer isn't king, he is a dictator, highly impatient, skeptical and cynical" (p. 34). Customer needs can be categorised as demands for either reliability or innovation, displaying a close relationship with the stability-dynamism concept of competition (Gordon, 1985). This view contrasts OCs in high technology manufacturers and utilities, representing two ends of a continuum, reaching from highly dynamic or novel to static and reliable marketplaces. In terms of this dynamic, products, technologies and buyer preferences change frequently, whereas in the static dimension, products, technologies and consumer preferences change very slowly, if at all.

The same study by Gordon (1991) highlights that "culture formation is neither a random event nor an action dependent solely on the personalities of founders or current leaders, but it is, to a significant degree, an internal reaction to external imperatives" (p. 9). Gordon (1991) further suggests that "a dimension of external demand is the degree to which the industry's customers emphasise the need for reliability or novelty in the industry's offerings" (p. 12).

From this study it can be deduced that the influence of customer requirements in building an ISC can be summarised as the reliability of the technology required as well as the novelty or differentiation that the product brings on to the market as a competitive advantage. Reliability addresses the dependency associated with the quality of service or product offered, which has a domino effect on the quality of service that customers will be enjoying. For instance, when it comes to BYOD in the banking sector, staff members will likely be inclined to a device and service that will enable them to perform their duties reliably. Whilst reliability is a desirable feature, it is not necessarily the basis upon which the business will be built.

The differentiation of the product and services offering or the novelty also has an effect on the creation of a culture. Novelty will address such aspects as the availability of new technologies with desired features. In the information and communication industry, the assumption is that the new product will supplant older ones. Novelty will drive the culture by ensuring that the organisation will remain up to date. In the case of ICT consumerisation, various technology providers supply their own novelty, which in turn informs the culture that a business will build in order to remain relevant. Singh and Phil (2012) argue that enterprise mobility is now the rule rather than the exception, and organisations have to keep up with the competition in order to remain relevant players in the industry. Whilst information security is a key component, it is now playing catch-up in most organisations and it is against this background that organisations must have a culture for managing their information security (Leavitt, 2011).

From the discussion above, it can be concluded that customer expectations form the endogenous factors that influence the building of an OC around information security; on the other hand, societal expectations play an exogenous role. The next section will explore how societal expectations affect the way an OC is built.

5.3.2 Impact of the Societal Expectations on Building an Organisational Culture

Organisations exist in all national and international societies. Crowley-Henry (2005) remarks that the extent of their geographical reach plays a significant role in the way that societal expectations influence the formulation of an OC. Organisations that are present in one society, or in societies with similar expectations, usually find it relatively easy to build an OC (Atikomtrirat, Pongpayaklert, & Lundgren, 2011). Conglomerates usually have widespread presence and can at times have multiple societies to deal with resulting in multiple cultures existing within one organisation (Ghemawat & Reiche, 2011).

The consumerisation of technology presents a practical example of societies directing the culture in the use of technology in organisations. The phenomenon of consumerisation is characterised by the redefinition of OC through employee preferences. Twinomurinzi and Mawela (2014) point out that enterprise mobility has become entrenched in societies such that organisations are compelled to formalise or consider embracing enterprise mobility, with BYOD being at the forefront. As a result of employees increasingly opting to use their personal devices for work-related functions, organisations have had to redesign their policies and standards (Afreen, 2014). The rise of ICT consumerisation has gained momentum because of employees' ability to work anywhere anytime. Moreover, Blount (2011) suggests that the increase in the relevance of social media in both work and social life, complemented by the increase in the power of ubiquity, has given impetus to the growth of a culture of mobile technology in organisations. From an evolution perspective, societies are now composed of a workforce that grew up with technology and the Internet, thereby influencing a culture of technology (D'Arcy, 2011). French, Guo, and Shim (2014) state that the requirement of societies to have interoperability between home and work has compelled organisations to embrace the shift in IT culture brought about by BYOD.

The next section will explore the way organisations build an ISC. The consumerisation of technology has inadvertently influenced the traditional information security standards in organisations such that organisations are compelled to rebuild their ISCs or change from one culture to another (Schlienger & Teufel, 2003).

5.4 Building an Information Security Culture

Considering the relationship between OC and ISC, where ISC is a subculture to OC, it is obvious that the factors that affect the building of OC also influence ISC (Al Hogail & Mirza, 2014). Studies on user security behaviour conducted by Alfawaz and Nelson (2010) suggest that significant security gains for organisations can be achieved through the strengthening of their employees' security behaviours. Addressing information security at OC level will assist in addressing some of the breaches that exist within organisations (Dojkovski et al., 2010). Unlike other subcultures, ISC is visibly driven by IT which in turn is usually driven by external forces driving the evolution of technology (Belani, 2014).

Thomson et al. (2006) suggest that the management in any organisation play a critical role in building an ISC through their articulation of organisational information security goals and expected employee security behaviours. In Chapter 7 this is viewed as the organisational environment which makes up one of the six key traits in determining behavioural intention towards information security. If management take proactive roles in the formulation of an ISC, the building of an effective ISC will be less difficult

Schein (2009) argues that the first step in building an ISC is for employees to unlearn their old beliefs and ways relating to their work. Organisations can achieve this though comprehensive training programmes. This is often received with great anxiety and resistance and thus require proper change management in order to be implemented. In agreement with this viewpoint, Thomson et al. (2006) state that employee values, attitudes and norms should change in order for them to contribute to a "right" and healthy ISC in the organisation. Another perspective from Thomson and Von Solms (2005) holds that information security obedience should be the key starting point. These researchers define information security obedience as the amalgamation of the OC, information security, and corporate governance, observed in organisations as the behaviour by which users comply with the security policy. The management in the organisation have to create the environment and make provision for the governance structures to support information security obedience.

In building an ISC for the BYOD unintended administrator, this study followed Schein's perspective. From the literature review carried out in Chapters 3 and 4, it is clear that the three levels, that is, artefacts, espoused values and shared tacit assumptions, are an important basis for building culture in organisations (Schein, 1999). The next section will explore an extended model of Schein's model known as the model for information security shared tacit espoused values (MISSTEV), which was proposed by Thomson et al. (2006). In this model, which is essentially an application of Schein's perspective on OC applied to ISC, ISC is presented as a result of information security obedience. The MISSTEV model will be explored in detail together with the conscious competence learning model (CCLM) and the modes of knowledge creation (MKC).

5.5 Models for Building an Information Security Culture

This section will examine two generic models of behavioural science and apply them to building an ISC. The section starts by examining the competing values framework (CVF) and the MISSTEV. In order to apply the MISSTEV model to building an ISC for the BYOD unintended administrator, an exploration of the CCLM as well as the MKC will be conducted in that order. The CVF framework provides a simple way for characterising culture whilst the MISSTEV model puts forward the notion that employee behaviour towards information security is informed by the quest to comply with the senior management's vision.

5.5.1 The Competing Values Framework (CVF)

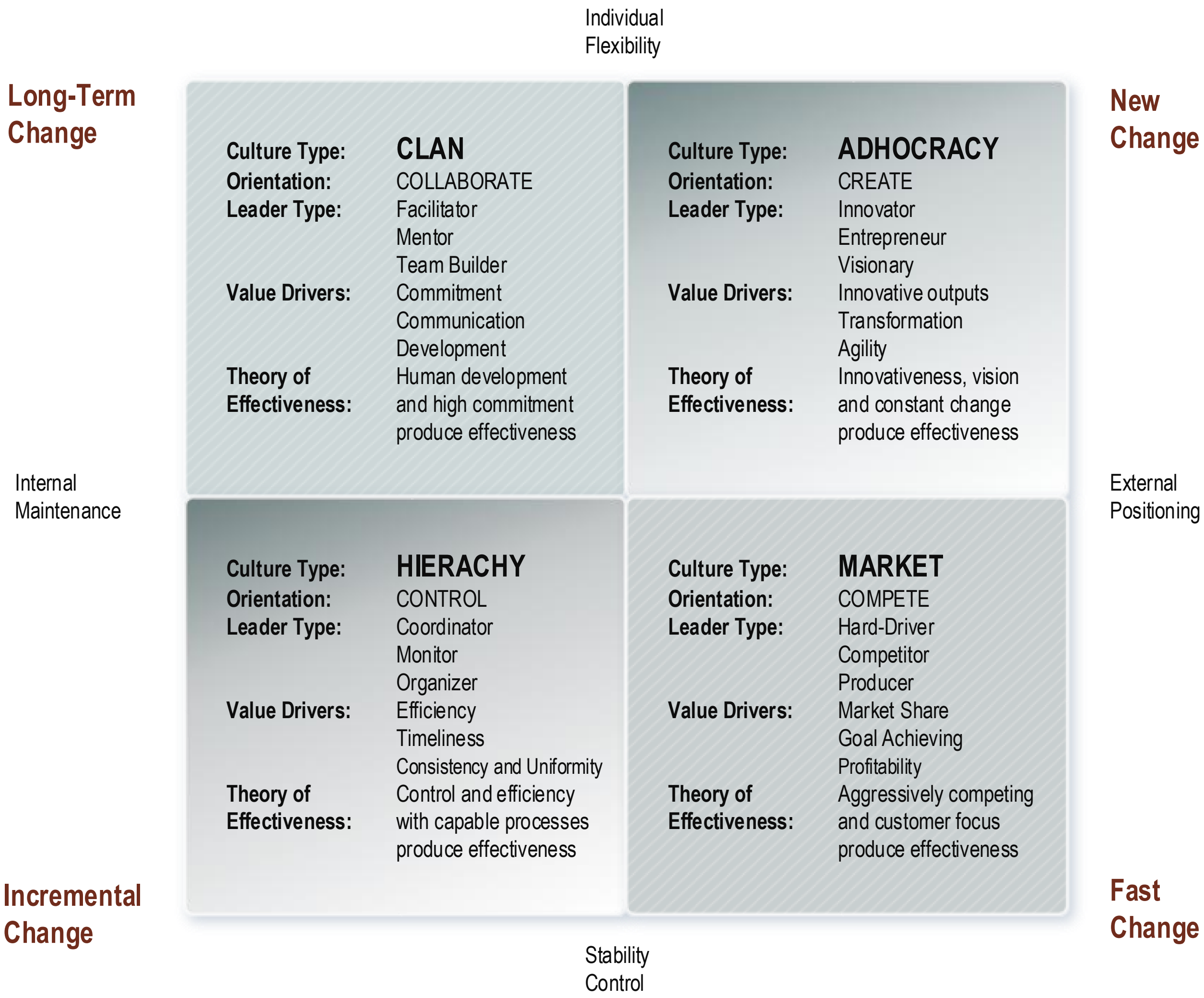
Cameron and Quinn (2006) diagnosed the changes in OC using the CVF and discovered that it provides a means for characterising OC in a way that is easy to construe. The CVF was formulated on the basis of a study on the major indicators of organisational performance carried out by the University of Michigan (Cameron, 2009). The CVF was subsequently found to be instrumental in understanding the wide varieties of organisations and individual cultural phenomena. Haworth (2014) further explains that the framework is based on the notion that there are countless activities that organisations engage in to create value and that form their culture, and these activities can be placed into the following four quadrants:

i. **Collaborate (clan).** This quadrant addresses all the organisational aspects of building human competencies within the organisation. Reliance is placed upon the employee's willing cooperation resulting mainly in satisfaction and teamwork. This also highlights the human capital development which is associated with organisational effectiveness.

ii. **Control (hierarchy).** This quadrant covers pursuit for improvements in efficiency through better processes. The hallmark for this quadrant is the achievement of a high degree of statistical predictability of the outcomes in risk management, auditing, planning and so forth.

iii. **Compete (market).** Value-enhancing activities are the hallmark of this quadrant, at the same time involving the monitoring of market signals and the interactions with external stakeholders like customers and competitors. The mantra for this quadrant is “compete hard, move fast and play to win”, that is, is organisational effectiveness.

iv. **Create (adhocracy).** This quadrant addresses the creation of value-adding activities through the ability to handle discontinuity, change and risk. This is a forward-looking quadrant whose mantra is “create, innovate and envision the future”.



Individual
Flexibility

Long-Term
Change

Culture Type: CLAN
Orientation: COLLABORATE
Leader Type: Facilitator
Mentor
Team Builder
Value Drivers: Commitment
Communication
Development
Theory of Effectiveness: Human development and high commitment produce effectiveness

Culture Type: ADHOCRACY
Orientation: CREATE
Leader Type: Innovator
Entrepreneur
Visionary
Value Drivers: Innovative outputs
Transformation
Agility
Theory of Effectiveness: Innovativeness, vision and constant change produce effectiveness

New
Change

Internal
Maintenance

External
Positioning

Culture Type: HIERACHY
Orientation: CONTROL
Leader Type: Coordinator
Monitor
Organizer
Value Drivers: Efficiency
Timeliness
Consistency and Uniformity
Theory of Effectiveness: Control and efficiency with capable processes produce effectiveness

Culture Type: MARKET
Orientation: COMPETE
Leader Type: Hard-Driver
Competitor
Producer
Value Drivers: Market Share
Goal Achieving
Profitability
Theory of Effectiveness: Aggressively competing and customer focus produce effectiveness

Incremental
Change

Fast
Change

Stability
Control

Figure 26. The Competing Values Framework

Source: Cameron and Quinn (2006)

When an organisation selects its own culture, it is essentially choosing its relative degree of emphasis in the four quadrants of the CVF. A close examination of the similarities and differences between the various quadrants of the CVF helps in understanding the strategic alignment of any organisation (Maximini, 2015). In this context we will use a banking organisation to examine the CVF. The collaborate and control quadrants stand on the side of internal control, whilst compete and create stand on the side with an external focus. The quadrants also address the dimension of stability and control versus individuality and flexibility. The CVF diagram, which is constructed on the basis of a survey of employees in an organisation

- can be used to communicate the organisation's culture to all key stakeholders
- clarifies the way the organisation will allocate resources to execute its growth strategy
- is a useful guide for the organisation's hiring, development and retention processes, and
- serves as a mechanism for coordinating belief and guiding day-to-day decision-making.

The CVF can also be used to analyse the overall culture that supports the growth strategy of the organisation and at the same time analyse the overall culture, including the ISC, of the organisation. Applying the CVF to building an ISC in the bank on this case study can be adapted by examining ISC on the basis of how employees can willingly learn information security concepts and apply them to ensure the bank's security. In view of the argument by Eschelbeck and Schwartzberg (2012) that BYOD is now the rule rather than exception, the CVF compete quadrant will provide a means for banks to compete by having a clean record on information security with no security breaches. Through the CVF quadrant of adhocracy, banks will create, innovate and envision the future which is full of security requirements. This resonates with the assertion by King (2012) that the Internet and mobile banking will characterise banking and therefore banks have to make the necessary adjustments to their ISC in order to become relevant. The next section discusses the CCLM and the knowledge creation model that will both lead to the MISSTEV model.

5.5.2 The Conscious Competence Learning Model (CCLM)

The CCLM divides the learning of a new skill or behaviour into four phases, forming a progression from unconscious incompetence to conscious competence (Businessballs, 2013). The four stages are as follows:

i. **Stage 1: Unconscious incompetence.** This is when employees are unaware of the existing particular skill that is required of them. Applying the stage to this study, employees may not be aware of the information security behaviours that could protect them. For instance, employees participating in BYOD may download games and applications that are malicious, ignorant of the impact they will have on the organisational data contained on the device they are using. At times, employees may deny the practicality and usefulness of the recommendations.

ii. **Stage 2: Conscious incompetence.** At this level, employees become cognisant of the relevant information security skills. This stems from the realisation of the skills and competencies they require for information security. In the case of BYOD, when employees become aware of the dangers such as the information security attacks they are vulnerable to in the absence of a functional ISC. This stage is often the turning point at which the employees will begin to learn survival means.

iii. **Stage 3: Conscious competence.** At this stage, employees will have acquired the security culture but will require concentration to apply it. Employees have to think of the ISC benefits before they can implement the culture. Employees will not reliably perform the security checks unless they are thinking about them, therefore they have to practise implementing them continuously until they become second nature.

iv. **Stage 4: Unconscious competence.** At this stage the skills and culture with regard to security inculcated at the conscious competent stage become second nature. Employees can now teach other employees about information security concepts and best practices. For instance, employees can easily make use of their BYOD devices in a secure way; they will not download and install malicious applications or leave the devices without basic security like passwords or updates on software patches.

Table 9. Conscious Competence Matrix

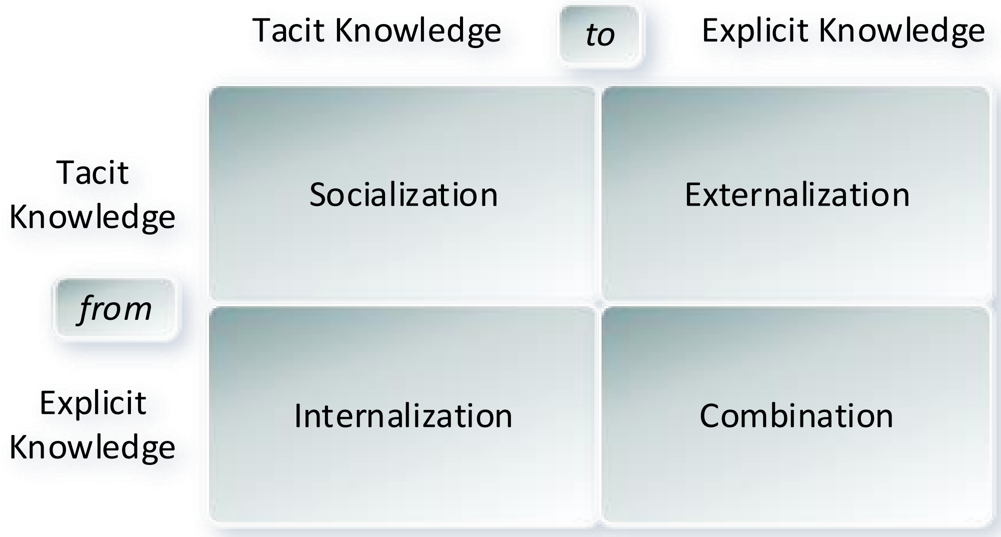
	Competence	Incompetence
Conscious	3 -Conscious Competence • The person achieves “conscious competence” in a skill when they can perform it reliably at will • The person will need to concentrate and think in order to perform the skill • The person can perform the skill without assistance • The person will not reliably perform the skill unless thinking about it – the skill is not yet “second nature” or “automatic” • The person should be able to demonstrate the skill to another, but is unlikely to be able to teach it well to another person • The person should ideally continue to practise the new skill, and if appropriate commit to becoming “unconsciously competent” at the new skill • **Practise** is the single most effective way to move from stage 3 to 4 P	2 -Conscious Incompetence The person becomes aware of the existence and relevance of the skill. • The person is therefore also aware of their deficiency in this area, ideally by attempting or trying to use the skill • The person realises that by improving their skill or ability in this area their effectiveness will improve • Ideally the person has a measure of the extent of their deficiency in the relevant skill, and a measure of what level of skill is required for their own competence • The person ideally makes a commitment to learn and practise the new skill, and to move to the “conscious competence” stage
Unconscious	4 -Unconscious Competence • The skill becomes so practised that it enters the unconscious parts of the brain -it becomes “second nature” • Common examples are driving, sports activities, typing, manual dexterity tasks, listening and communicating • It becomes possible for certain skills to be performed while doing something else, for example, knitting while reading a book • The person might now be able to teach others in the skill concerned, although after some time of being unconsciously competent the person might actually have difficulty in explaining exactly how they do it -the skill has become largely instinctual • This arguably gives rise to the need for long-standing unconscious competence to be checked periodically against new standards	1 -Unconscious Incompetence • The person is not aware of the existence or relevance of the skill area • The person is not aware that they have a particular deficiency in the area concerned • The person might deny the relevance or usefulness of the new skill • The person must become conscious of their incompetence before development of the new skill or learning can begin • The aim of the trainee or learner and the trainer or teacher is to move the person into the “conscious competence” stage, by demonstrating the skill or ability and the benefit that it will bring to the person's effectiveness

Source: Businessballs (2013)

The application of the CCLM in developing an ISC resonates with findings by Bransford (2000) on how people learn. This study by Branford (2000) argues that people usually learn by following what the leadership views as best ways of doing things in the organisations they are linked to. In the next section, modes of knowledge creation (MKC), as proposed by Nonaka (1994), will be explored. The combination of the MKC and the CCLM will culminate in the formation of the MISSTEV model. It is noteworthy that all these models confirm the six traits influencing the behavioural intention towards an information security culture, as discussed in detail under Chapter 7

5.5.3 Modes of Knowledge Creation (MKC)

Building a culture around information security can be viewed as knowledge creation, considering that this will result in the creation of a new way of doing things. Nonaka (1994) argues that in any organisation, knowledge is created through a continuous dialogue between tacit and explicit knowledge. The MKC model proposes four modes of knowledge creation: externalisation, combination, socialisation and internalisation.



from / *to*	Tacit Knowledge	Explicit Knowledge
Tacit Knowledge	Socialization	Externalization
Explicit Knowledge	Internalization	Combination

Figure 27. Nonaka's Modes of Knowledge Creation

Source: Thomson et al. (2006)

This model is based on the notion that there are two dimensions of knowledge creation – implicit and tacit knowledge creation – which are experience based and therefore subjective. Tacit knowledge is the training that is associated with a personality, thereby making it hard to formalise and communicate it. It is the knowledge that is unwritten knowledge held by practically every normal human being, based on his or her experiences, understandings, intuition, interpretations and assumed information. Explicit knowledge is codified knowledge; that is, knowledge that can be transferred by means of formal systematic language. At the core of Nonaka's model is the identification of existing knowledge, which can be converted into four new modes of knowledge based on the assumption that knowledge can be created through conversion between tacit and explicit knowledge (Nonaka, 1994). In Figure 27, the four modes of knowledge creation are (1) from tacit knowledge to tacit knowledge, (2) from explicit knowledge to explicit knowledge, (3) from tacit knowledge to explicit knowledge, and (4) from explicit knowledge to tacit knowledge.

An application of this to building an organisational ISC would be characterised by the conversion of existing cultures to security aware cultures. Applying this concept of knowledge creation to the BYOD ISC, organisations will have to create new knowledge for their employees which will promote a culture that meets the organisational expectations. The most practical way for creating knowledge it for organisations to create an environment that is governed in a manner that promotes information security. The organisation will then be required to harness employee attitudes and habits by means of training programmes that create the knowledge that ISC is central to the organisation.

5.5.4 Model for Information Security Shared Tacit Espoused Values (MISSTEV)

The MISSTEV model is based on the notion that information security can be developed into a culture by using training to address appropriate policies. The model presents organisational information security as a combination of organisational information security policy complemented by awareness and training programmes that promote knowledge creation within the organisation, which will ultimately result in corporate information security obedience (Thomson, 2007). The model builds a culture by creating new knowledge about information security, which is then implemented through training and awareness programmes.

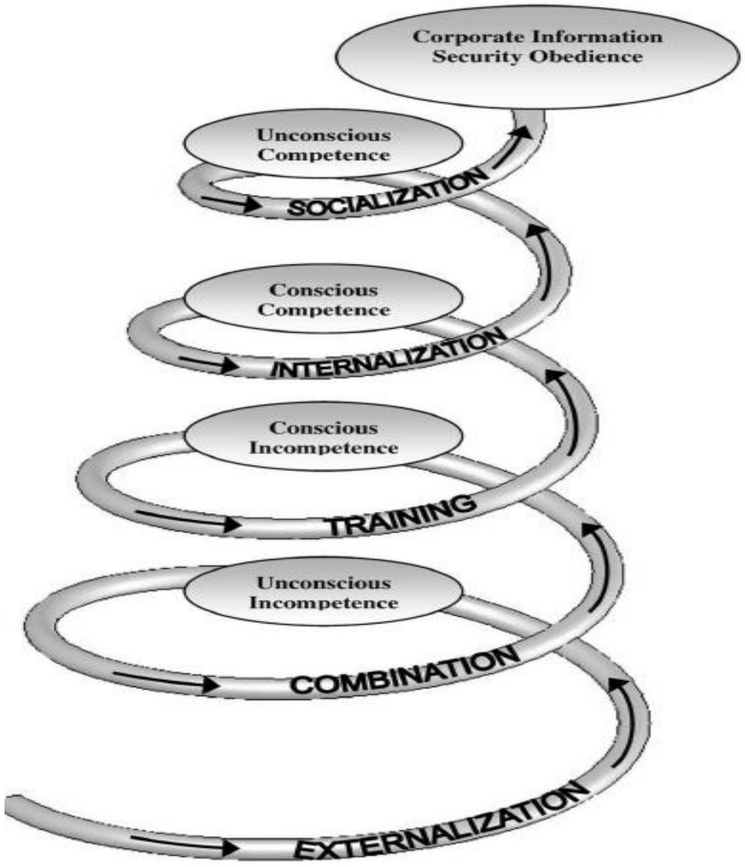


Figure 28. MISSTEV Model

Source: Thomson (2007)

By means of training programmes, employees will realise their inadequacies when it comes to security and the skills they are required to attain in order to protect the organisational information assets. The employees' learning process will include moving from the unconscious incompetence stage, where they will not know the risks they are exposing the organisation to by not having certain skills and knowledge about information security. Subsequently, training and awareness will help employees to become conscious of the security risks that the organisation will face as a result of their incompetence. The next stage is conscious competence where training and awareness will make employees aware and equip them with the skills required to protect information assets consciously. The last phase of the model is unconscious competence, where employees are aware of the security and it has become second nature to them. At this level, information security becomes a culture among the employees. The knowledge creation approach followed by the MISSTEV model resonates well with Al Hogail and Mirza's (2014) perspective, which suggests that people's attitudes and absence of training on security challenges are among the majors contributors to security incidents. Chapter 7, training is highlighted as one of the key traits influences the behavioural intention towards information security.

The following section will explore how an ISC can be built by applying the MISSTEV model findings. Bearing in mind that building a culture is also creating new knowledge, the next section will discuss how organisations conduct training and awareness in building an ISC. For the purposes of this study, the focus will be on studies of how banks train and provide awareness to their employees on information security issues around the BYOD unintended administrator.

5.6 Building an Information Security Culture in Banking Organisations

Lucca et al. (2014) state that banking organisations operate in highly regulated environments regardless of the country or continent in which they are based. Studies conducted by Davis (2004) show that culture operates more effectively where there is regulation and control. Childress (2011) argues that banking should focus on culture now more than ever. He attributes this viewpoint to the fact that "culture cannot be managed but it can be led" (p. 10). Thus, focusing on culture will enable banks to follow regulations seamlessly. Magdalena et al. (2009) note that behaviours follow culture which, in turn, follows regulation. In this section, models and frameworks for building culture will be cited and conclusions will be drawn along those lines of classification.

Barrett (2006) proposes a means by which culture entropy could be measured based on Maslow's hierarchy of needs. In his study he formulated a way of measuring the culture entropy for an organisation by carrying out what is called the Barrett survey. On carrying out this survey in a number of organisations, he concluded that:

> "The culture of an organisation is defined by the values that are lived by the leaders, managers and supervisors. These are not necessarily the espoused values—the values that the organisation says it wants to embrace—but the values that exist in reality and show up in the everyday interactions between leaders, managers and employees, and between employees and customers and suppliers. The conclusion I have reached is that if you want to build a high performing organisation with superior financial returns, then you will need to focus on satisfying the needs of all your stakeholders, especially the needs of your employees—their basic needs and their growth needs" (Barrett, 2006, p. 12).

Barrett (2013) conclusion confirms the fact that in order for culture to be built there is a need for stakeholder participation. To highlight the fact that OC as a concept has often been ignored in the banking sector, Thakor (2015) states in this regard:

> "It is easy to see why culture has not been a big part of banking regulation. Variables like capital ratios and executive compensation are tangible and visible, so it is easy to target them in the formulation of regulations. Culture, by contrast, is a nebulous concept that often means different things to different people. And because it is nebulous, it tends to be unattended to. Moreover, we have a vast body of research on capital requirements and incentive compensation, but precious little on culture, at least in Economics. This too adds to the reasons why culture has received relatively scant attention until recently in regulatory discourse. Yet, the inattention to culture due to the paucity of knowledge about how culture in Banks should be diagnosed and the levers that should be pulled to change it has limited the ability to design regulations that proactively cope with foreseeable problems rather than react to problems after they occur. It is unlikely, however, that future Banking regulation will operate in a culture vacuum " (p. 2).

After carrying out studies in the Indonesian banking sector, Ula et al. (2011) explained that Information Systems has become the heart of modern banking in our world today. Any mishandling of confidential information assets can cause huge financial loss, and the reputation of the bank will be severely damaged. Building an ISC in banking organisations is a key imperative, which can be linked to building any other culture in banks that involve employee participation. Certain theories that are applicable to building OC provide significant insights on how organisations can build an ISC. Studies conducted by Marjani and Forouzanfar (2012) on the Saderat Bank and Eghtesad Novin Bank in Iran based on Denison's model concluded that banking organisations operating in the same regulatory environment can have different levels of staff cooperation, adherence to policy and procedures, adaptability, and clarity of organisational objectives regarding their culture. Denison' model explains that an OC is built on employee participation (involvement), adaptability, mission and consistency.

From the conclusion of the Saderat Bank study cited above, it can be deduced that employee participation is a key component for building a culture in an organisation. A study by Coetzee et al. (2007) in the South African banking sector also placed emphasis on employee participation as an equally important aspect in building OC. In this case, the models used to build OC are independent of the continent, as the employee is the key player.

After carrying out a study in the Nigerian banking setting, Selamat and Babatunde (2014) concluded that information security activities need to be observed in order for an organisation to be able to implement an efficient ISC. This corresponds closely with the emphasis given in Schein's perspective on OC. In his model, Schein (2009) gave three classifications of culture – visible artefacts, espoused values and shared tacit assumptions. The information security activities in Selamat and Babatunde's (2014) study operate at the level of visible artefact. In another study, (Renaud, Flowerday, Othmane, and Volkamer, (2015) proposes an African digital security culture (ADSC) which puts forward the human collective identity as a key to any organisation's culture. The ADSC suggested an approach for fostering security in African societies based on the African wisdom of "Ubuntu", which is based on the understanding that "I am because we are".

The study of ISC will be best explained by examining the consumerisation of technology and also by understanding that technical solutions fail if the people do not know how to use them (Keyes, 2013). In investigating ISC in banking organisations, this study focused on the BYOD phenomenon. The four major areas in the financial industry that require change are the regulatory environment, security of the device, policy changes or updates, as well as the financial implications of voice and data usage. Banking organisations must optimise their strategies to embrace BYOD in a secure way (Lund & Silva, 2015).

Based on a study on the ISC in the Ethiopian banking sector, Woretaw and Lessa (2012) identified certain factors that influence ISC. These factors are information security policy, information security risk analysis, information security management standardisation, information security compliance, and top management support. This research evaluated the level of ISC that can be built through an auditing process (Woretaw & Lessa, 2012), using Martins' (2010) ISC framework. The research found that an ISC in the banking sector is a prerequisite for good governance and the application of an effective regulatory framework. The study also pointed out that employees are at the centre of the organisation's ability to build an effective ISC. This corresponds closely with findings of Sidek (2011) in Indonesia and studies by Marjani and Forouzanfar (2012) in Iran and (Babatunde et al., 2014) Babatunde et al. (2014) in Nigeria.

Thakor's (2015) conclusion that culture is an aspect that has been neglected in the banking context implies that the BYOD ISC in the banking sector is not directly addressed in the literature. The application of ISC in BYOD will thus be addressed as a derivative of OC.

5.7 Conclusion

Building an ISC in any organisation, like the building of any other culture, is a social aspect, which will be driven by employee involvement. The best way to build an ISC is to examine it from the perspective of the consumerisation of technology. Information security in most businesses is viewed as a specialised area confined to the ICT function of the business. To that effect, this study has taken an approach in which it addresses enterprise mobility through BYOD as the basis for creating a BYOD ISC.

Various scholars believe that organisations do not build a culture but rather transition from one culture to another (Gordon, 1991; Thakor, 2015). Other scholars believe that organisations have a main culture as well as subcultures that are built because of the changing business environment or introduction of new technologies to foster the business strategy (Boisnier and Chatman, 2003; (Khatib, 1997), 1997; Oliver, 2011). From the two viewpoints, it is evident that OC is not static and that ISC as a subculture of OC is indeed dynamic. The cases from the banking sector on the ISC examined here single out the employee as the key initiator of the culture change or growth. Ula et al.'s (2011) conducted in the banking sector in Malaysia confirmed this and ten years later Selamat and Babatunde (2014) came to the same conclusion after carrying out a similar study in Nigeria. The same finding on employee participation was also confirmed by Davidson et al. (2007) for the South African banking sector.

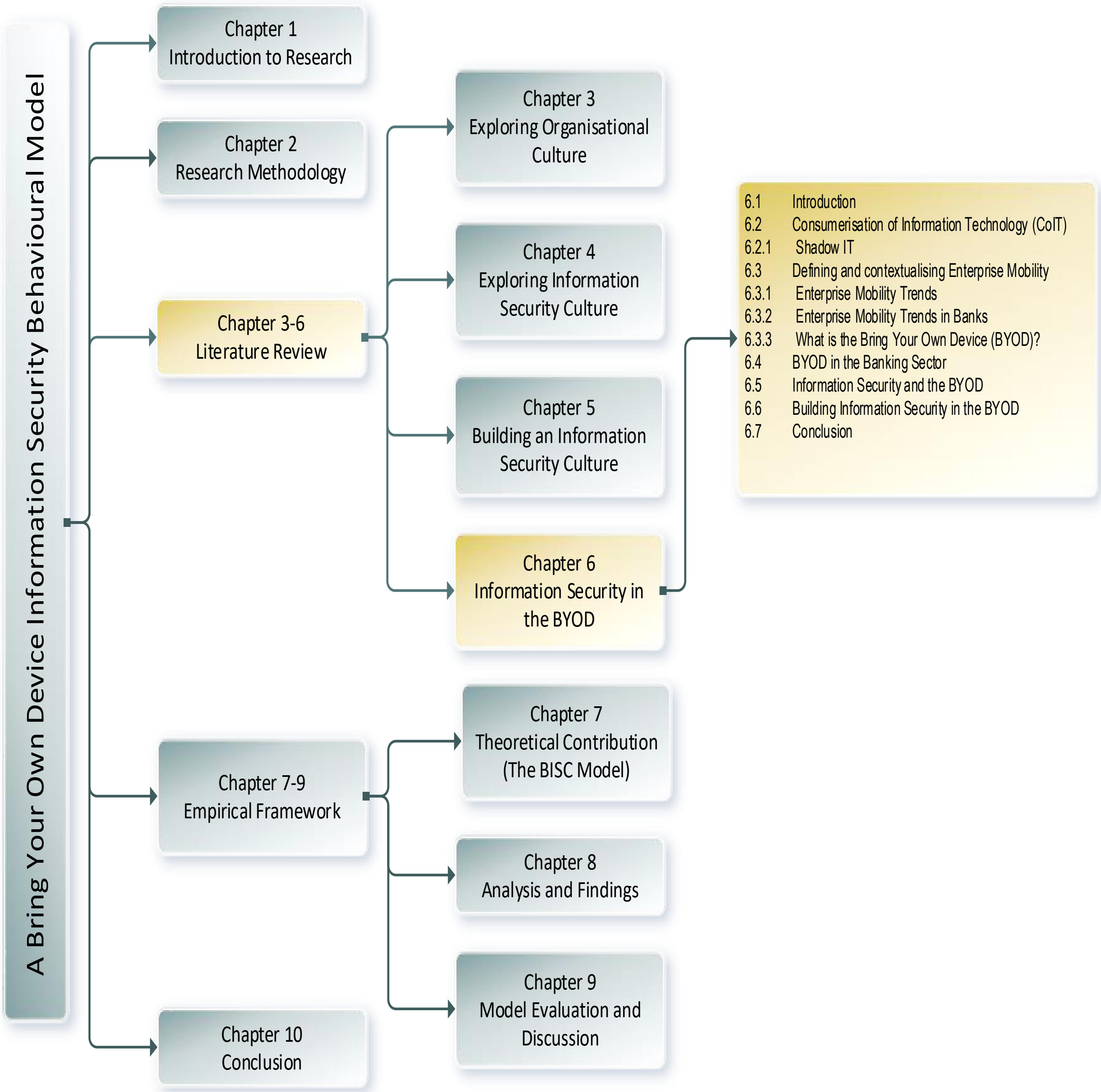
The chapter also explored some models for building an ISC based on prior studies. The CVF by Cameron and Quinn (2006) is based on the notion that there are countless activities that organisations engage in to create values that formulate their culture, and these activities can be placed in four quadrants, which cover the aspects of collaborate, control, compete and create. The CCLM divides the learning of a new skill or behaviour into four phases in the form of a progression from unconscious, incompetence to conscious competence. The MKC postulated by Nonaka (1994) argues that knowledge is created through a continuous dialogue between tacit and explicit knowledge within any organisation. This is based on the realisation that building a culture around information security can be viewed as knowledge creation; considering that this will result in the creation of a new way of doing things. Based on Schein’s perspective discussed in Chapter 3, MISSTEV model is based on the notion that information security can through training be developed into a culture by addressing appropriate policies.

From the literature above, Denison et al.'s (2006) perspective remains visible across different continents. In this study, the banking sector will be the industry of focus for the survey on building an ISC around the BYOD unintended administrator. The next chapter will explore the ISC in the BYOD.

The focus will be mainly on the banking sector in developing countries. Cases from other regions will be explored where relevant to come up with comparisons on how the BYOD has changed information security practices in banks, which demand the building of an ISC.

Chapter 6 : Information Security in the BYOD

"The boundaries between working in the office, on the road or at home have been blurred by the untethered power of smartphones, tablets, and other portable devices." IBM


A Bring Your Own Device Information Security Behavioural Model
Chapter 1
Introduction to Research
Chapter 2
Research Methodology
Chapter 3-6
Literature Review
Chapter 3
Exploring Organisational Culture
Chapter 4
Exploring Information Security Culture
Chapter 5
Building an Information Security Culture
Chapter 6
Information Security in the BYOD
6.1 Introduction
6.2 Consumerisation of Information Technology (CoIT)
6.2.1 Shadow IT
6.3 Defining and contextualising Enterprise Mobility
6.3.1 Enterprise Mobility Trends
6.3.2 Enterprise Mobility Trends in Banks
6.3.3 What is the Bring Your Own Device (BYOD)?
6.4 BYOD in the Banking Sector
6.5 Information Security and the BYOD
6.6 Building Information Security in the BYOD
6.7 Conclusion
Chapter 7-9
Empirical Framework
Chapter 7
Theoretical Contribution (The BISC Model)
Chapter 8
Analysis and Findings
Chapter 9
Model Evaluation and Discussion
Chapter 10
Conclusion

6.1 Introduction

The consumerisation of information technology (CoIT) has changed information security management in organisations, mainly as a result of the introduction of enterprise mobility (Ullman, 2011). Gartner (2012) predicted that by 2017 the primary focus of endpoint breaches would shift to smartphones and tablets. Organisations also worry that they underestimate risk because they focus on the device rather than their enterprise's entire enterprise mobility landscape. A study conducted by PWC (2015) concluded that Bring Your Own Device (BYOD) has brought numerous lessons to organisations across various industries including the retail, transportation, manufacturing and healthcare industries, as well as the banking industry. Sathyan, Anoop, Narayan, and Vallathai (2016) argue that enterprise mobility has been adopted by organisations to enhance their marketing channels, improve productivity in the office, boost customer satisfaction, as well as offer shopping experiences or to process sales through the mobile devices. A customer survey report by Norton (2012) on cybersecurity and enterprise mobility found that half of respondents use their personal devices for work, but they do not take basic security precautions – a fact made more worrying from a risk management perspective because 27% of those users reported having had their device lost or stolen.

Independent findings by Scarfo (2012) and Eschelbeck and Schwartzberg (2012) suggest that across all industries it is no longer an option for organisations to adopt BYOD but rather a must, as its benefits outweigh the cost of securing its operations. The employee is now driven more by the ability to work from anywhere, anyhow and at any time. The exponential growth in bandwidth and the massive entry of smart devices has given impetus to enterprise mobility (Musarurwa & Jazri, 2015). With these trends, BYOD information security has become paramount for organisations if they are to remain operational and retain the ability to attract high performing employees.

Whilst enterprise mobility trends have affected several industries, the focus of this study will be the banking sector where governance is a primary performance indicator. Enterprise mobility has changed the way of doing business in banks the world over. After carrying out a study on mobile money and payments trends, Shrier, Canale, and Pentland (2016) pointed out that the evolution of mobile money is the key driver for financial inclusion. The same study indicated that, in 2012, about 2.5 billion people out of the then world population of about 7 billion did not have a bank account. Of the 2.5 billion, that was unbanked, 1.7 billion had a smartphone, and in the same year there were more mobile money accounts than traditional bank accounts in developing countries like Kenya, Tanzania, Madagascar and

Uganda. Enterprise mobility has brought a separate form of money exchange called mobile money, which does not necessarily require a bank account. GSMA (2010) define mobile money as "the broad spectrum of financial services which can be accessed through a mobile phone" (p. 15). In contrast, mobile banking can be defined as "the mobile processed financial services associated with a bank account such as deposits, withdrawals or bill payments" (GSMA, 2010, p. 5). In order to explore the impact of the enterprise mobility trends in banking, the study will examine all the terminology related to CoIT as well as enterprise mobility, which will later be referred to interchangeably with BYOD.

This chapter will begin by exploring CoIT and enterprise mobility. It will then build up the concept of BYOD from an enterprise mobility definition and extend this to its application to organisations. Key terminologies in relation to BYOD, as well as the various names by which it is referred to, will be examined. A comparison of the risks and benefits as cited by other scholars will also be presented. The chapter will proceed by examining how the BYOD information security culture (ISC) is applied in the banking sector and conclude with an evaluation of how other banking organisations can build a culture of BYOD information security.

In order to understand information security in the BYOD clearly, the next section will examine CoIT as well as enterprise mobility. Among the existing enterprise mobility trends, the study will then focus on the impact of BYOD on information security. According to the definition adopted from Singh and Phil (2012), information security refers to the standards for guarding data and information from illegal access. The chapter will conclude by examining means for building information security in BYOD.

6.2 Consumerisation of Information Technology (CoIT)

Organisations across industries have begun to understand the need to adapt to the CoIT in order to gain competitive advantage. Thomson (2012) describes the CoIT as "enabling the chaos" and as the introduction and adoption of consumer devices in enterprise organisations. Gartner (2016) views CoIT as

> "… the specific impact that consumer-originated technologies can have on enterprises. It reflects how enterprises will be affected by, and can take advantage of, new technologies and models that originate and develop in the consumer space, rather than in the enterprise IT sector. Consumerisation is not a strategy or something to be "adopted". Consumerisation can be embraced and it must be dealt with, but it cannot be stopped" (p. 1).

According to this view, the CoIT is the increasing trend for new IT to emerge in consumer markets and then spread into business. A report by PWC (2011) defines CoIT as "[t]he use of technologies that can easily be provisioned by non-technologists" (p. 2). The same report argues that CoIT has redefined the relationship between the employers and their employees who use IT devices. Niehaves, Köffer, and Ortbach (2012) view CoIT as the use of privately owned IT resources like devices and software for business purposes.

In a different study related to enterprise mobility, Niehaves, Köffer, and Ortbach (2013) speak of a reverse technology adoption life sequence, meaning that more and more employees prompt IT innovation in a bottom-up fashion. Experts in CoIT like Banerjee (2016) point out that there is a change in the direction of technology absorption whereby the adoption of IT used to start with defence and government followed by the business enterprises. Banerjee explains that CoIT does not mean that IT has become a consumer product but rather that consumers have reversed the way organisations used to implement IT strategies by influencing the types of device to be used in the enterprise network.

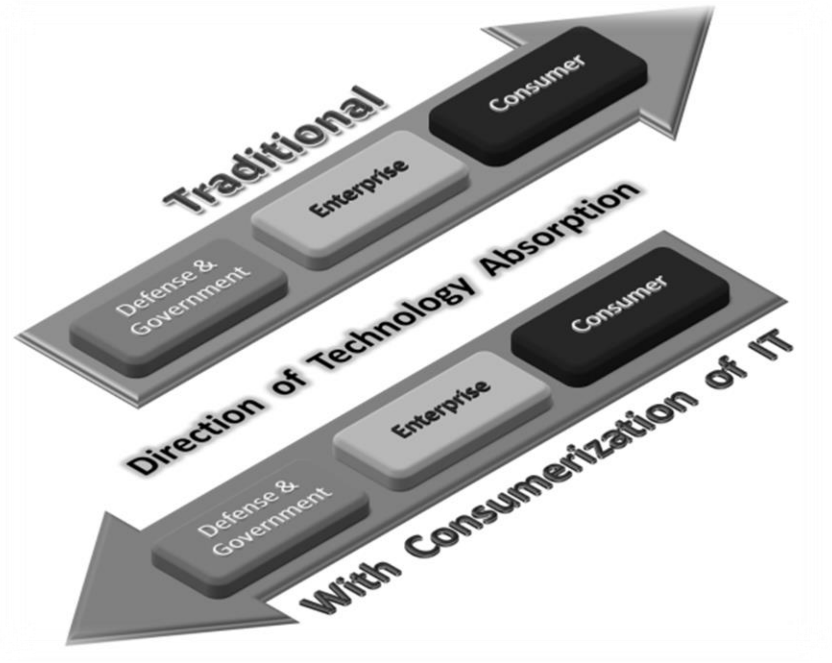


Figure 29. Direction of Technology Absorption

Source: Banerjee (2016)

According to a research conducted by AMCTO (2012) at the University of Ontario, the term CoIT came into being in 2001 when it was introduced by Neal and Taylor. The first academic publication on CoIT was by Moschella, Neal, Opperman, and Taylor (2004). PWC (2011) believe that CoIT emanated from the social upheaval of the 1960s and 1970s which introduced the notion that diversity is a key strategic advantage for both employees and businesses. The same report believes these trends gave rise to the corporate structures, as well as styles in management and workplace ethos, that have endured today. The aspect of consumerisation emerges from the fact that modern-day employees have become "nomads" who prefer to work from anywhere, anytime and on anything. Some even prefer to work as contractors who only get paid for certain tasks within organisations, working from the comfort of their own homes or offices.

Russo (2011) states that CoIT is made possible by consumer-driven IT innovations, the consumer market scale and lower business margins, smarter workforce, the emergence of a reliable global network, as well as the introduction of infrastructure variable cost services. Microsoft (2016) argues that what drives the CoIT is cloud computing, data explosion, social computing, browser-based apps, and the ecosystem of computers, personal devices in the workplace, ubiquitous connectivity, and natural interaction. As a result of these CoIT drivers, not all organisations implement and update their policies to ensure security. Driven by their preferences, employees have begun bringing their "shadow" devices of preference to the workplace, resulting in the rise of "Shadow IT". TrendMicro and McCafferty (2011) state in this regard: "As consumerization proves to be irreversible, and threatens to become an IT nightmare by increasing security risk, data loss and financial exposure, it's clear that a lack of strategy could prove devastating. The best approach to effectively managing a consumerised workforce is to embrace consumerisation in order to unlock its benefits and reap its full business potential" (p. 1).

Brodin (2016b) argues that whilst Shadow IT is a problem brought about by the CoIT, the issue of rogue devices has been around for a while. According to Gartner (2012) security analysts, the use of rogue devices has been around since the introduction of iPods, flash disks and all movable data transferring media in organisations. While organisations have had endpoint security systems like antiviruses and intrusion detection systems, these data transferring devices have always exposed organisational data to insider threats of data theft and transportation of viruses and malware. The only protection that the organisational data have in this instance is an information security aware employee. The main focus of this study is thus to create a model for building an ISC for the unintended administrator in enterprise mobility. The study is based on the realisation that whilst the organisation can invest massively in the technologies that give security, the effectiveness of these technologies is as good as the strength of the security culture of the employees using them. The next section will explore Shadow IT, which is an indication of the fact that the culture of information security is not yet very strong in organisations, as findings from the literature show that employees still use personal devices for work and, where they are not officially allowed, they may even bring them in without getting clearance (Silic & Back, 2014).

6.2.1 Shadow IT

Gartner (2016) defines Shadow IT as devices, software and services outside the ownership or control of IT organisations, whilst Johnson (2013) views it as a term used to describe the use of unauthorised applications within a corporate environment, as well as the processing or storage of business information on devices that are not approved by the information security department. Shadow IT emanated from the CoIT and it is a currently misunderstood and relatively unexplored phenomena (Silic & Back, 2014). This study will ultimately show that Shadow IT is a consequence of the absence of a strong ISC in the organisation. Shadow IT exists as a consequence of CoIT; it is not formalised by the IT functions for a given organisation and it often undermines the organisation’s main IT systems. Highly regulated industries like the banking industry are less susceptible to Shadow IT-related attacks as they have tight security systems. Considering that the banking environment is highly regulated, it follows that a culture of control is already in existence among the employees (Lucca et al., 2014b).

Employees place more reliance on their Shadow IT systems since they give them the results they want at the same time offering the convenience they require. Shadow IT is also referred to Black IT and employees extensively use Shadow IT products that leverage their efficiency and allow faster and improved cooperation and communication (Silic & Back, 2014). Moreover, employees believe that they are not doing anything wrong, and therefore simple naivety is motivating their behaviours. Considering that Shadow IT comes without the formal approval of organisations’ IT divisions, it poses serious information security risks. In order to explore Shadow IT on mobile devices, the next section will explore enterprise mobility which basically defines the exposure that enterprise organisations face as a result of the advent of mobile devices which are remotely connected to the enterprise network.

6.3 Defining and Contextualising Enterprise Mobility

Enterprise mobile technology as we know it today evolved over time. Sathyan et al. (2016) attribute the evolution of enterprise mobility to advancements in three significant areas: the development in web standards, advances in wireless networking technology, and innovations in the mobile device platforms. One area that was possibly left out of this list and that may be a fourth attribute is change in employee behavioural patterns as a result of the entrance into the working environment by the Millennials cohort of staff members in the workplace. The Generational Differences Chart list defines Millennials, or Generation-Y, as that age cohort of 34 years and below who grew up with mobile technology (Dole, 2009). This generation was born with the technology and they work efficiently on the devices of their choice.

According to research by IBM (2015) "the boundaries between working 'in the office', 'on the road', or 'at home' have been blurred by the untethered power of smartphones, tablets, and other portable devices" (p. 3). The same research points out that employees now prefer to work on devices they choose and employers have come to expect employees always to be online. Barnes (2003) defines enterprise mobility as "the degree to which an organisation's operations address the information needs, typically supporting the employee activities in a geographically independent way" (p. 3). Enterprise mobility can also be viewed as the application of complex combinations of the computing capabilities embedded in mobile and ubiquitous IT (Carden, 2007).

From the literature it can be deduced that CoIT and enterprise mobility have shaped the modern-day mobile computing trends. Whilst CoIT is described as the use of personal devices, enterprise mobility is the ability of those personal devices to access organisational information through virtual private connections remotely. The best way to explain enterprise mobility is to define it in the context of the evolution of mobile devices, as well as their ability to connect to the office networks remotely (Hazelton, Kingstone, Mckee, & Analyst, 2016). Organisations are taking their time in embracing enterprise mobility fully. Enterprise mobility is being driven by the fact that the era for personal computers is coming to an end and there is massive growth in the mobile content as well as the Internet of Things (IoT) (Mobile Iron, 2014). Further, the increase in the number of device agnostic operating systems has also fuelled this trend (Mobile Iron, 2014). Figure 31 shows Schadler, Yeats, and Wang's (2013) findings of "anytime, anywhere users". Blatt and Gallagher (2014) observed the same trend and describe it as "Mobilocracy". Mobilocracy refers to "a powerful class of worker who relies on mobile devices for greater productivity; as well as the common worker, especially, as a mobile workforce within corporations, or as mobile employees' behaviours and preferences increasingly play a larger role in IT decisions and directions" (Blatt & Gallagher, 2014, p. 275).

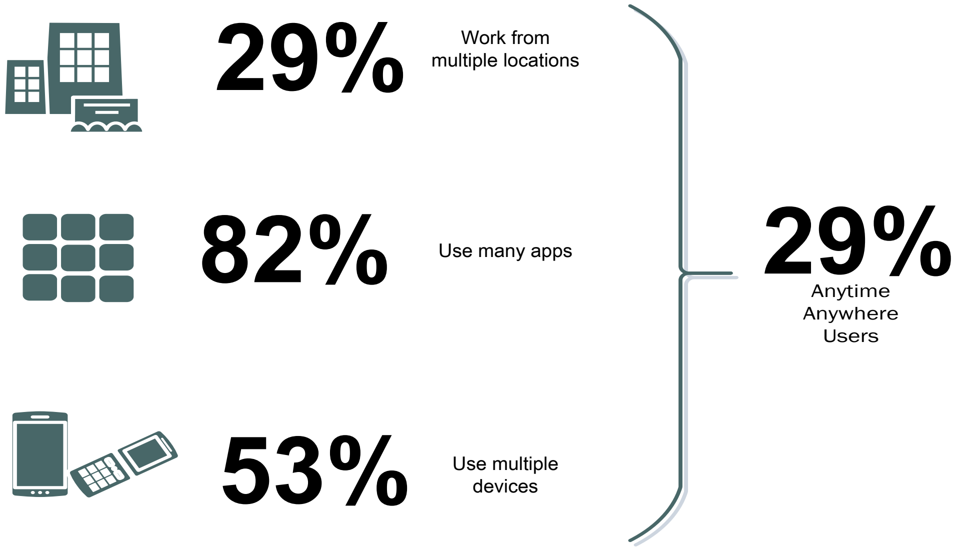


Figure 30. Mobile Workforce Adoption Trends 2013

Source: Schadler et al. (2013)

A report by Citrix (2015) showed that seventy-two out of every hundred devices owned by employees in 2015 were enabled to access organisational information. This ownership of mobile devices coupled with the massive growth in broadband penetration has compelled organisations to revisit their strategies on CoIT and enterprise mobility.

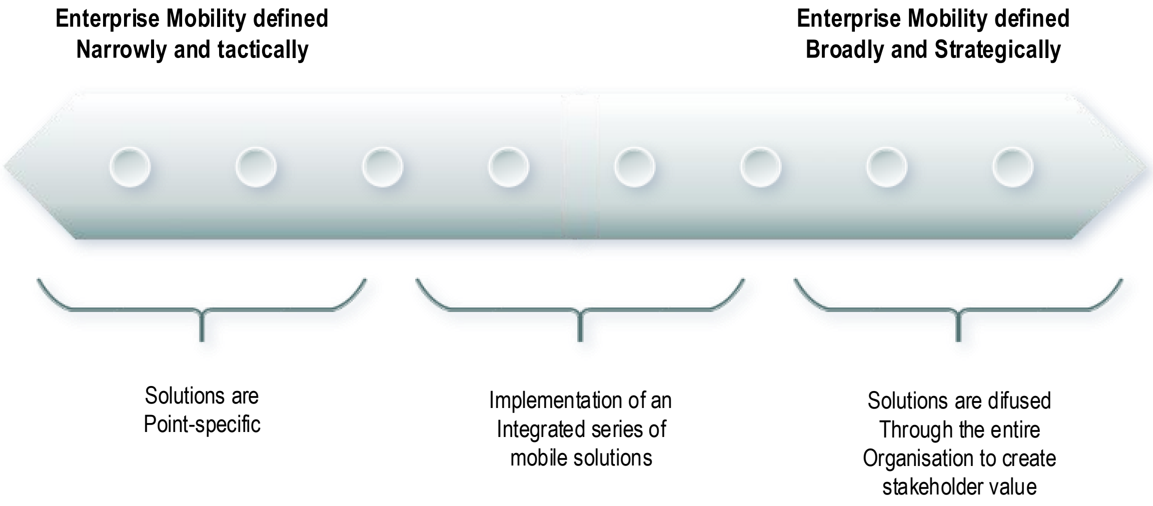


Figure 31. Enterprise Mobility Continuum

Source: Basole (2008)

Figure 31 shows the enterprise mobility continuum, which is essentially a summation of the technology readiness of organisations measured together. According to Basole's (2008) enterprise mobility continuum model, different organisations across all industries have adopted enterprise mobility and are at various stages of maturity. The next section will explore the trends in enterprise mobility with a special focus on the banking industry, which is the industry of focus in this study.

6.3.1 Enterprise Mobility Trends

According to studies, executives need to keep up to date with office dynamics, which is necessitated by the trend of enterprise mobility. MaaS360 (2015) states:

> "In the beginning there was darkness, especially for those who needed to get work done on the road or at home. Workers left their data and productivity programs on their cumbersome desktops. Laptops made it possible to work outside the office, but connectivity was costly and inconsistent. Also, the minute you closed your laptop, you entered an information black hole of nothingness" (p. 3).

With the arrival of technologies like Blackberry that allowed connection to the office, executives in corporate leadership became connected to their offices remotely. The entrance of smartphones led to the "spread of the light", which was then followed by the tablet which had a larger screen making it easier for employees to do work more comfortably. Employees embraced the technology as it made their working hours flexible, whilst the guardians of the information systems, the IT team, remained in the shadows, not convinced that the devices could connect in a safe way.

A global executive overview report findings by Hazelton et al. (2016) points out that enterprise mobility continues to gain traction in business despite the IT teams' security concerns. The report identifies seven trends where mobile devices continue to gain traction in the enterprise. The seven areas identified are listed in Table 10, which further classifies the trends in terms of their impact both on ICT and business by identifying losers and winners for each trend.

Table 10. Enterprise Mobility Trends

	Winners	**Losers**
IT decision-makers will shift to a mobile-first mind-set	IT vendors that enable the movement of workflows to mobile devices as a core capability; mobile-first and mobile-only vendors	Mobile laggards and companies that don't engage their customers through mobile
Culture, not costs, will be the biggest barrier to wider enterprise loT adoption	Vendors that can put the loT into the proper business context for the vertical markets they serve with solutions and partners that can enable their customers' digital transformation of data into business insights	Pure-play loT technology companies
Technology boundaries will increasingly blur across the enterprise mobile application lifecycle	Vendors that place data at the heart of their product	Pure plays that decide to go it alone

Ecosystem partnerships will drive further consolidation in the enterprise mobile market space	Emerging vendors with proven solutions and market traction	Stand-alone solutions with limited capabilities for integration
Mobility issues will gain heightened operator focus	Mobile operators willing to discount but also understand customer concerns	Mobile software providers pushing enterprise solutions
Strong Apple Pay adoption will further distance iOS from Android in mobile payments	Apple Pay partners; iOS-first commerce companies	Vendors that don't hedge their bets and those that haven't developed contactless-compatible solutions
Businesses will need to plan for rapidly increasing mobile commerce demand	Vendors that offer mobile engagement tools for line-of-business users	Web commerce providers that only provide responsive design strategies for mobile

Source: Hazelton et al. (2016)

The key findings from Table 10 above are as follows:

i. **Culture, not costs, will be the biggest barrier to wider enterprise loT adoption**: Vendors that can put the loT into the proper business context for the vertical markets they serve, with solutions and partners that can enable their customers' digital transformation of data into business insights, will take their businesses to the next level.

ii. **More IT decision-makers are now thinking mobile first:** The report noted that 40% of organisations had started prioritising mobile since the beginning of 2015.

iii. **The IoT interest for enterprises is growing despite the existing cultural barriers:** The report noted that in the first quarter of 2016, 19% of enterprises were planning to use or were already using IoT – up from 16% in 2015.

There is a wide spectrum of benefits and risks as well as challenges associated with enterprise mobility. IBM (2015) lists and quantifies the benefits of enterprise mobility as shown in Table 11 below, as well as the risks and challenges as shown in Table 12.

Table 11. Enterprise Mobility Benefits to Organisations

Allows flexible remote working	86%
Increases staff productivity	64%
Cost saving	39%
Access to cloud services	30%
Staff manage their own devices (unintended administrators) so reduce IT admin	29%
Attract young and energetic staff to organisation	13%

Source: Adapted from IBM (2015)

Whilst there are benefits associated with enterprise mobility, there is also a whole list of risks and challenges associated with the same trend.

Table 12. Biggest Risks and Challenges for Enterprise Mobility

Device loss leading to security issues	61%
Lack of control over corporate data access	49%
Requirement for IT to help users with numerous devices and platforms	48%
Staff (unintended administrators) accessing consumer services for work purposes	28%
Cost of supporting mobile devices	25%
Requirement for IT to create apps for multiple platforms	201%
Lack of transparency in use of services	19%

Source: IBM (2015)

Enterprise mobility trends are so imperative that organisations have to find means to fit them into their IT systems if they are to remain relevant. Hill (2014) states in this regard:

> “BYOD and business security don't have to be a challenge, no matter what size your business is. Establish a policy on the acceptable use of mobile devices, and make clear to employees the ways in which the company will secure corporate information if it resides on an employee's tablet or smartphone. There is much to gain from empowering employees to work from anywhere. With a little planning, you can make the experience both productive and secure” (p.1).

Gordon (2015) observed three trends in enterprise mobility: firstly, it will take the form of security and manageability, secondly, application development, distribution and management, and finally, threat management. An infographic by Fliplet (2016) illustrates that in 2015, the number of mobile workers worldwide surpassed 1.3 billion, which translates to an additional 240 hours per employee per year. The infographic predicts that about 3 billion mobile devices will be sold by 2017 based on a year on year growth of 70% on tablet shipments observed since 2013. By the year 2014, there was a 731% increase in custom-built enterprise apps. As such, companies were compelled to embrace mobile apps resulting in a continuous growth in app usage. In order to move the study on towards the industry of choice in this study, the next section will explore how the effect that enterprise mobility has had on banks.

6.3.2 Enterprise Mobility Trends in Banks

Online banking followed by mobile banking constituted the first waves of digital disruption in the banking industry, as customers realised the availability of more convenient ways of managing their finances than the brick-and-mortar branches. The capabilities have developed over time from being objectively elementary to highly intuitive and unrestricted by location. The industry is yet to leverage the full potential of mobile technologies, and must soon begin to think beyond the traditional transaction-based restrictions of their business models if they are to grow and improve ahead of their competitors (Westacott, 2014). Notable trends in the banking sector include Mobile Money and mobile banking apps. Westacott (2014) notes that “[a]round 40% of people worldwide now use mobile technology in banking and finance, most often in the form of specialist apps, on a weekly basis (or more) to monitor their accounts, transfer funds and pay their bills” (p. 1). The major challenge faced by banks in implementing enterprise mobility is that they are being primarily transaction-led instead of customer-centric, and they do not believe in collaboration and infrastructure sharing to leverage on a wider product set and reach distant customers.

The evolution of the mobile wireless systems through the use of virtual private networks (VPN) has driven the mobility of banking applications to benefit both the employee and the customer. Figure 32 gives a diagram of the way a model bank now manages to connect its employees and customers by riding on cellular Internet or Wifi.

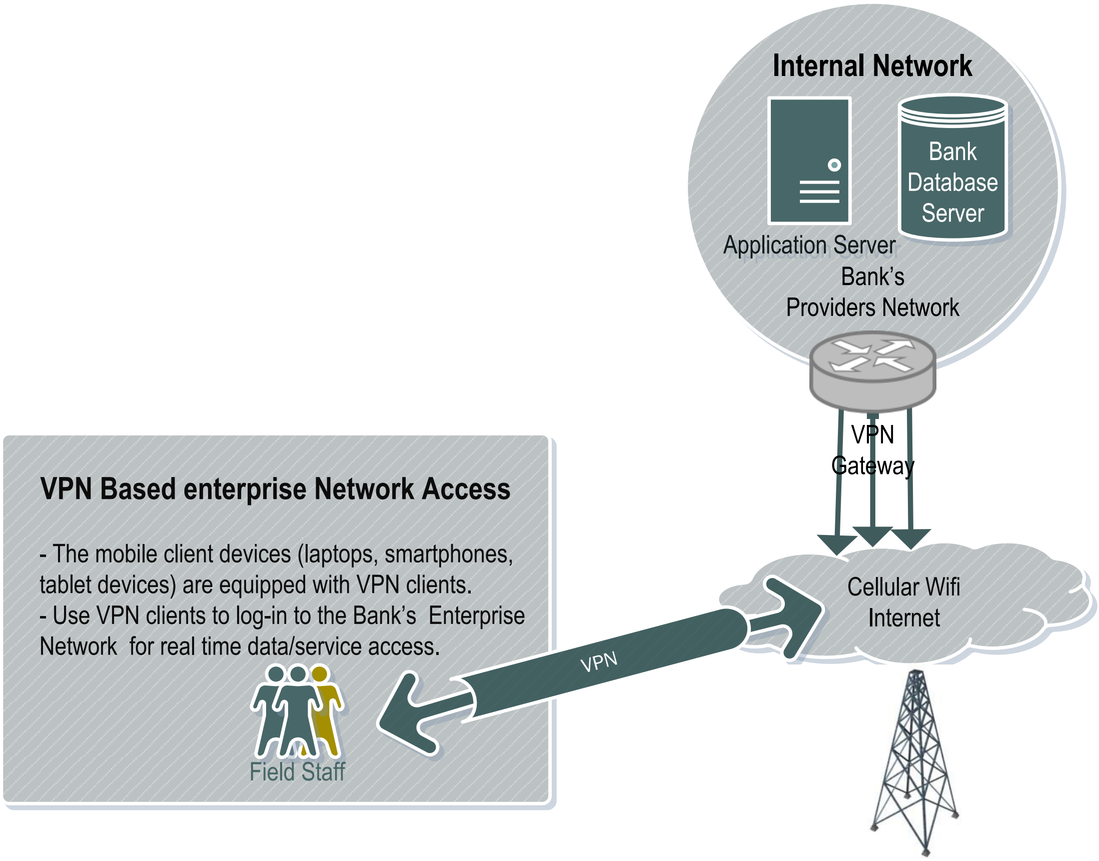

Internal Network
Bank Database Server
Application Server
Bank's Providers Network
VPN Gateway
Cellular Wifi Internet
VPN
VPN Based enterprise Network Access
- The mobile client devices (laptops, smartphones, tablet devices) are equipped with VPN clients.
- Use VPN clients to log-in to the Bank's Enterprise Network for real time data/service access.
Field Staff

Figure 32. VPN-based Enterprise Access

Source: Sathyan et al. (2016)

A significant trend taking shape and shifting banking further towards a mobile ecosystem is the introduction of mobile wallets and payments. Accordingly, the banking industry is a modest, developing marketplace with great opportunities for mobility.

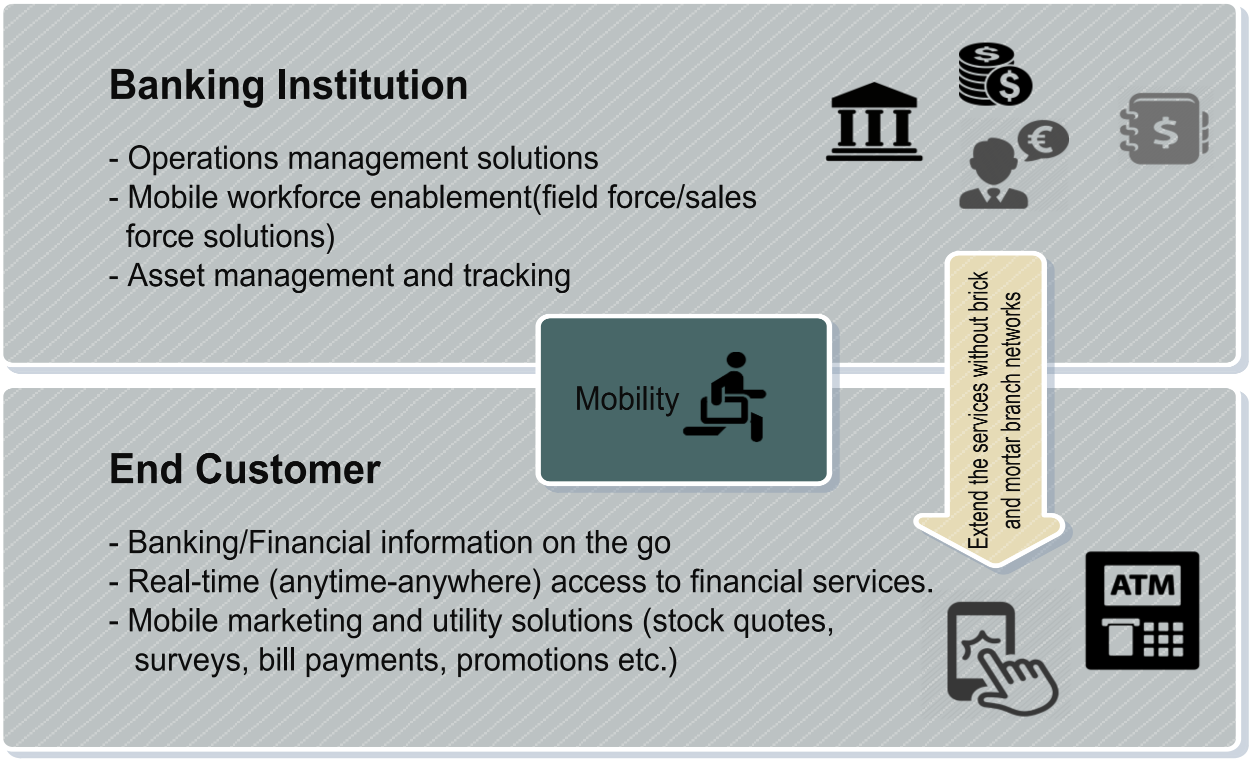

Banking Institution
- Operations management solutions
- Mobile workforce enablement(field force/sales force solutions)
- Asset management and tracking
Mobility
Extend the services without brick and mortar branch networks
End Customer
- Banking/Financial information on the go
- Real-time (anytime-anywhere) access to financial services.
- Mobile marketing and utility solutions (stock quotes, surveys, bill payments, promotions etc.)
ATM

Figure 33. Scope for Mobility Solutions in the Banking Industry

Source: Sathyan et al. (2016)

Sohal (2014) observed ten trends in enterprise mobility and among them is better and improved BYOD. IBM (2015) observed the same trends and described them as approaches to enterprise mobility as BYOD was not acceptable in the banking industry because of the challenge of having to secure multiple operating systems that moved in and out of the protected environment. Regarding this trend, they recommend that CIOs have to start considering platform agnostic solutions since BYOD has become imperative in the industry. From championing the cause of financial inclusion to servicing customers effectively in remote locations, enterprise mobility through the use of smartphones is proving to be a powerful tool in the banking and finance sector. The mobile channel is indispensable if a bank wants to grow the loyalty of its customers and drive positive experiences for them. By catering to the mobile expectations of new customers, the bank can attract, delight and engage them. If used efficiently, the mobile channel can emerge as the single most important touchpoint in their entire banking experience.

(Kaufman (2014)lists the following top five trends in enterprise mobility in banking:

i. **Mobile payment streamlining informal personal payments**. This includes P2P (person-to-person) payments, which are on the rise. Forrester (2013) predicted that the mobile payment market would grow from $12.8 billion in 2012 to $90 billion in 2017. However, this mode of payment is not new; a market for financial transactions between individuals has always existed. With the growth in mobile phones, the market once handled informally has now become a reliable dissemination channel (Bodine & Dorsey, 2013).

   In the African market, M-PESA was the initial such offering made open to Kenya society in 2007. Since then, upwards of 17 million Kenyans have been using the service to access money as and when required. In other developed markets like Europe and America, PayPal is perhaps a more popular example of mobile payments in the First World with a global outreach (Kershenbaum, 2012). While there are many existing independent services like Ecocash in Zimbabwe, iMali in Namibia Cash that facilitate P2P payments, Arwa (2014) argues that big banks are only beginning to understand the potential of mobile payments. Banks can increase user engagement by offering their end users a service that is fast, easy and most notably secure.

ii. **Mobile wallet – reducing time taken at checkout lines**. The traditional pocket wallet is progressively being substituted by the mobile wallet. To avoid the trouble of handling cash and change, debit and credit cards came into being. Just when people thought that going cashless was the new normal, the mobile wave disrupted the financial industry and presented the concept of a mobile wallet. While going cashless may be the new normal, going digital is certainly the future. With the Ecocash wallet in Zimbabwe, MobiKash Wallet in Kenya and Apple Pay in the USA with global outreach, this mode of payment has only been projected to acceptance. A mobile wallet can store information about your credit and debit cards, coupons and loyalty programmes. It can be used to transact at any point-of-sale terminal. Mobile wallets are being increasingly adopted by the current generation to facilitate app-driven payments and other utility payments. While mobile wallets may have opened exciting possibilities for people, it has also given rise to numerous security concerns. This is both a challenge and an opportunity for big banks. Currently, digital wallet services are only being offered by non-banking organisations like telecommunication companies in Africa, such as Safaricom in Kenya, Econet Wireless in Zimbabwe, and Apple, Google and Amazon in the USA. If banks can securely integrate this mode of payment into their existing suite of service offerings, they can capture a good share of the market. In Zimbabwe, Ecocash recently partnered with banks to bring interoperability within the mobile payments space (Kufandirimbwa, Zanamwe, Hapanyengwi, & Kabanda, 2013).

iii. **Cross selling products – personalising customer experiences.** This entails presenting a wide spectrum of products and services that is known to have a unique gain over other players in any industry. Ashwani Mishra (2016) remarks that the banking industry is also trying to provide end-to-end solutions to its customers to increase their level of satisfaction. Instead of merely offering the conventional banking services through a mobile app, banks are also using it to promote various other products and services like home loans, car, health or life insurance. The entire basis of cross selling rests on being able to push the right service or the right product at the right time. Through the use of predictive analytics and customer relationship monitoring (CRM) tools, banks are able to map customers' behaviour and buying patterns (Deloitte, 2015). Based on the data, the most context-relevant offer is made. This targeted method of advertising generates more qualified leads than pushing general offers through an email. With location-based services like Wifi and beacons gaining traction, targeting customers and providing them with hyperlocal content will only become easier. Gantz and Reinsel (2012) point out that leveraging mobile devices as an additional channel to cross sell products and services can provide the much needed velocity to customers' mobile strategy.

iv. **Wearable technology – affording improved convenience**. All business organisations constantly grapple with the means by which they can differentiate themselves from competitors in the same industry (IBM, 2015). In the same vein, Michalow (2016) remarks that to enjoy competitive advantage in the market, banks have to embrace the newest wave of technology that excites and benefits the customers. The current crop of users enjoys the ease and expediency of accessing information through wearable devices and it irrefutably presents an outstanding opportunity to achieve best customer experience. The customer can make financial information like bank statements and account information available through apps for smartwatches or other wearable devices (AMCTO, 2012). Although they may still be considered a novelty, the market for wearable electronics is definitely expected to cross US$8 billion level in 2018, increasing at a healthy compound annual growth rate (CAGR) of 17.7% from 2013 to 2018 (Sathyan et al., 2016). Studies show that a few banks in Spain like La Caixa and Banco Sabadell are already experimenting with the use of Google Glass (Clark & Lee, 2009). By being an early mover in this space, banks can uniquely position themselves as financial enterprises aligned with the latest in technological trends.

v. **Biometric authentication – reducing risk and security concerns**. Security is a big priority where money is involved and the inability to provide strong security measures can prove to be a deal breaker in the banking sector. Passwords are a weak and no longer effective measure of verification in accessing critical financial information (Sathyan et al., 2016). To address the challenges of authentication, banks are now turning to biometrics since biometric identifiers are almost impossible to fake. A distinguishing biological factor such as fingerprints can be used to accurately identify a user. Fingerprint authentication is also easier and more user friendly because unlike a password there is no hassle of remembering it. As a means to boost security for its mobile banking platform, US-based Montgomery County Employees Federal Credit Union incorporated fingerprint authentication for users accessing their mobile app (Bradbury, 2007). Another American credit union requires its customers to authenticate themselves through retina scans which can be seen through the camera of a mobile phone. Such impenetrable layers of security can augment the image of one's brand and can have profound implications for the business.

Regarding the impact of enterprise mobility in banking, Ernst and Young (2013) states that "[t]he Digital transformation and a proliferation of data are fundamentally changing the relationship between businesses and their customers businesses" (p. 12). Applying these comments to the studies by Sohal (2014) on banking mobility trends, it is interesting to note that mobility trends exist in various forms. Several terms like Choose Your Own Device (COYD), Here's Your Own Device (HOYD) and others have been introduced to describe enterprise mobility trends. As a result of the wide array of enterprise mobility options, there is an XYOD, whilst the Ovum survey referred to this wider array as the BYOX (Cavoukian, 2013). The next section will examine this wider array of enterprise mobility trends.

6.3.3 What is the BYOD?

A variety of acronyms and their definitions exist to describe the various BYOD categories. Bring your own software (BYOS) exists where the same technologies driving BYOD also allow users to access non-organisation software (Eschelbeck & Schwartzberg, 2012). The term BYOS can also be used to describe "bring your own services". This is where employees supply their own technological services of choice to the organisation (French et al., 2014). Bring Your Own Apps (BYOA) is another variation of the BYOD phenomenon, where employees use their own applications to access and support corporate functions and services. The Ovum survey concluded that there is a Bring Your Own Anything (BYOX) phenomenon which describes the particular function under use in the BYOD (Eddy, 2013). For the purpose of this study, only the BYOD phenomena will be discussed in detail. There are different strategies for enterprise mobility and BYOD is one them (Absalom, 2012). BYOD is defined as "a program that involves employees using their own mobile electronic communication devices to carry out work for their employer through remote access to the organization's intranet" (Cavoukian, 2013, p.5). Singh and Phil (2012) define BYOD as a new business trend in terms of which the business policy adopted by management allows employees to use their own devices for work-related duties and to connect to the office network remotely. Under the BYOD trend, employees own and are free to choose a device that suits their preferences, enabling them to be more productive. However, if the information security standards of the BYOD are not observed properly, it will create a security challenge for organisations, which Larryfurst (2013) escribes as the "Bring Your Own Disaster".

6.4 BYOD in the Banking Sector

BYOD challenges in today's banks are characterised by high data security requirements and management risk requirements (Lund & Silva, 2015). Consequently, a study by BankingTech (2016) pointed out that BYOD has transformed the way banking is now being conducted such that banks have to weigh possible gains in productivity against the security risks. VMware (2016) reveals four reasons why bank IT leaders are driving the change from traditional banking to BYOD as follows:

i. **It's all about apps.** The proliferation of new and legacy applications makes managing, updating, delivering and consuming applications on a multitude of devices more difficult. For instance, banks can help eliminate the pain of application packaging with instant delivery, update and retirement of applications and user environment settings.

ii. **Mobility and secure digital workspaces.** As mobile devices continue to proliferate in the workplace for efficiency, productivity and customer service, there is a great deal of interest from customers to provide a single workspace. This digital workspace, powered by a simple and secure enterprise platform, delivers and manages any app on any device with conditional access policies.

iii. **Advent of the Windows 10 Operating System**. This was Microsoft's first truly mobile operating system that delivers a seamless user experience across tablets, desktops and laptops.

iv. **Data security**. The challenge in the financial services ecosystem is that no chain is stronger than its weakest link and sometimes the weakest link happens to be the employee.

Considering that the BYOD is an enterprise mobility trend, it is logical to conclude that the literature on enterprise mobility trends in the banking industry will address the application of BYOD in the banking industry to a greater extent. After carrying out a study on the adoption of BYOD in enhancing customer service delivery at the Kenya Commercial Bank (KCB), Arwa (2014) concluded that 100% of the employees used their smartphones while 16% used tablets for customer support. The reason for smartphone and tablet prevalence was convenience and quick service in response to customer instructions and queries – each at 100%. According to the respondents, the current level of usage of personally owned devices had an overall effect on their productivity and improved the quality of customer service. Consequently, the Hong Kong Monetary Authority issued a statement in which they lifted the ban on the use of BYOD in banks (Cheng, 2014).

6.5 Information Security and the BYOD

Information security is the greatest challenge in BYOD across all industries. Brien et al. (2013) maintain that an "organisational culture that is information security aware will minimise risks to information assets and specifically reduce the risk of employee misbehaviour and harmful interaction with information assets" (p. 2). Whilst BYOD brings advantages and benefits to the organisations, it will have disastrous consequences for the organisations' information security if not properly managed. In the BYOD environment, the employee is the unintended administrator, as no endpoint security management policies are enforced by the organisation's IT. Two major issues thus arise for BYOD training and pose a serious information security risk; namely, the consequences of not keeping the device secure by the unintended administrator and the fact that the device connects to multiple issued networks.

Olalere, Abdullah, Mahmod, and Abdullah (2015) argue that the biggest BYOD challenge is that organisational data are being delivered and managed to devices that are not managed by IT departments. They believe that these have security implications for data leakage, data theft and regulatory compliance, especially in the case of the banking industry. Inspired by inconsistencies in the current research on BYOD information security, Downer and Bhattacharya (2016) introduced a new taxonomy for classifying BYOD security challenges. This taxonomy divides BYOD information security challenges into two dimensions:

i. **Dimension 1**. Security challenges are categorised according to the areas of the organisations they affect most like the hardware or the software security as well as human resources.

ii. **Dimension 2**. This classifies challenges by primary concern, key common characteristics and inferred relationships. For instance, equipment challenges are classified into deployment challenges and technical challenges. Deployment challenges are experienced at pre-implementation whereas technical challenges are experienced during the entire BYOD lifecycle. The human resource challenge is divided into policy and regulation challenges.

In order to understand BYOD information security, all of the dimensions observed by Downer and Bhattacharya (2016) should be analysed at their various stages. Several attempts to address BYOD information security concentrate on either one of the two dimensions stated above. Figure 34 shows the proposed categories for BYOD security challenges.

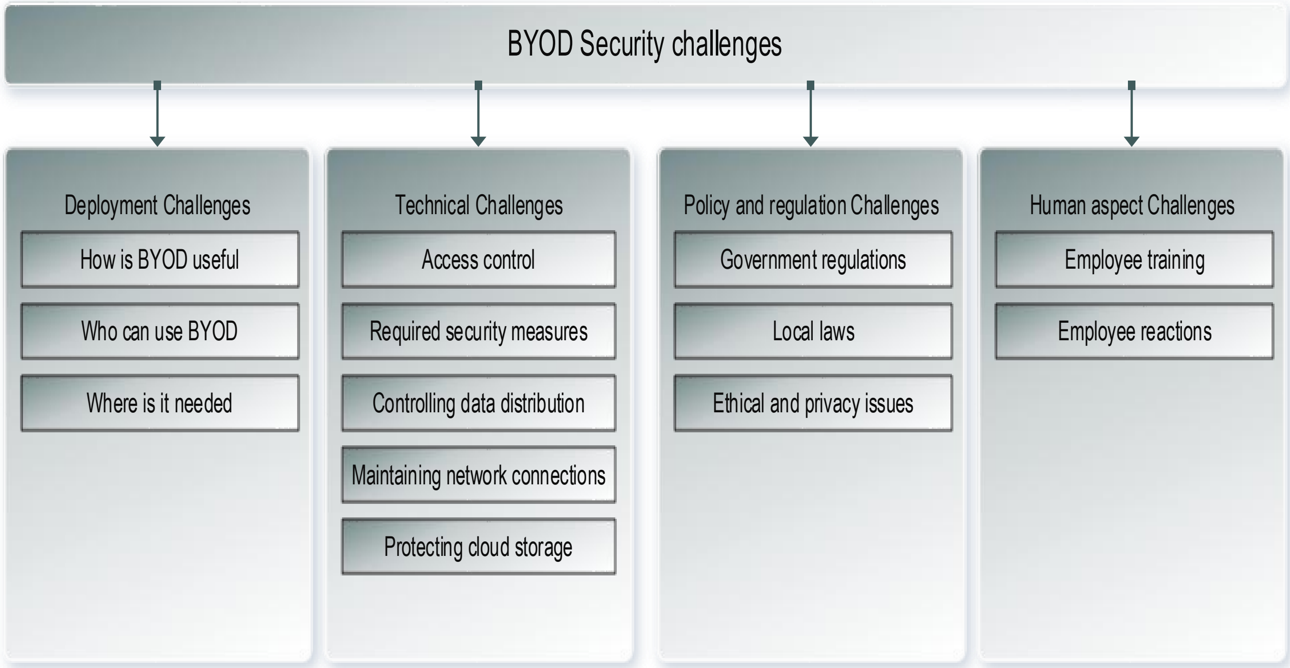


Figure 34. Categories of BYOD Security Challenges

Source: Downer and Bhattacharya (2016)

Whilst the approach cited in Figure 34 addresses all the facets of BYOD, this study proposes that there is a need to concentrate more on the challenges related to the human aspect. Employee behaviour is something that needs to be attended to first, as it determines how the employee will implement all the other sections. Whilst training is important, employee behaviour is also important in combating BYOD-related security challenges. Human actions are guided by predicting the occurrence of a particular behaviour, provided that behaviour is intentional (Ajzen, 1991). Therefore, it can be concluded that an ISC is probably the additional component of a model for organisations to conclusively deal with BYOD information security challenges. The next section discusses how BYOD information security can be built.

6.6 Building Information Security in the BYOD

BYOD information security can be built by exploring the two dimensions as proposed by Downer and Bhattacharya (2016). Regarding the technical dimension, existing security measures on the BYOD include the following:

i. **Virtual Private Networks (VPN).** Gessner et al. (2013) argue that VPNs ensure selective access to information over public networks.

ii. **Network Access Control (NAC).** This is a network solution that limits the number of devices, as well as their access privileges to the organisational network. Sathyan et al. (2016) note that NAC provides reliable network access control.

iii. **Mobile Device Management (MDM).** This refers to a multifunctional framework which grants businesses the ability to strictly manage mobile devices connecting to its network. Hillard (2014) argues that MDM paves the way for the mobilisation of apps, content and entire businesses. He describes it as a mechanism to "defend and contend".

iv. **Mobile Application Management (MAM)**. This is viewed as a lighter version of the MDM or a flexible option to MDM by which organisations can strictly control a specific application on the device.

v. **Mobile Information Management (MIM)**. This is security relating to BYOD that targets data integrity, synchronisation and personnel access to the device. Murthy (2009) argue that MIM is similar to a bank safety deposit box where enterprises can safely deposit their secure and sensitive data.

Technical solutions to the BYOD are specific to the BYOD solution that the employee uses. Android has Aurasium, and VMware has introduced AirWatch, which supports BYOD programmes. The Cisco BYOD Smart Solution is a BYOD solution which is specific to Cisco (Wang, Wei, & Vangury, 2014). Whilst these solutions exist, they all usually connect to the same enterprise network, making it difficult for the organisations to manage all the technologies. There is thus a need for a platform agnostic solution to BYOD information security challenges (Diogenes & Gilbert, 2015). This study proposes the employee as the source of all BYOD information security challenges. Therefore, there is need to build an ISC with the unintended administrator of the BYOD.

Chapter 4 examined the way in which an ISC can be built. It was noted that an ISC is a subculture of OC, therefore psychological theories can be applied in building an ISC. Schein (2009) argues that in order to build an ISC, employees need to unlearn their old beliefs and ways relating to their work. Thomson and Von Solms (2005) point out that there is a need for information security obedience as a starting point in building an ISC. Information security obedience is defined as the amalgamation of the OC, information security and corporate governance observed within organisations and as the behaviour with which users comply with the security policy. In building BYOD information security, there is a need for organisations to work towards information security obedience which then translates to an ISC. This is achievable through a combination of training and understanding the employees' behaviour and attitudes towards information security.

6.7 Conclusion

BYOD emerges as a phenomenon or new business policy implemented by management, which gives employees the privilege of using their own individual mobile devices for work-related tasks (Singh & Phil, 2012). BYOD has given rise to an "unintended administrator" who has total control of their own device. By 2017, it has been predicted that after all companies embrace mobile, 100% of customer-facing devices will be running on apps and 75% of employee apps will be built on mobile first (Mobile Iron, 2014). Further, by 2018, enterprises the world over will have invested upwards of 60 billion dollars in enterprise mobile apps, making enterprise mobility as big as the Internet (Basole, 2008).

This chapter identified employees as being the drivers of technological trends in modern-day business. The first wave for this drive in executing their duties started with the CoIT. The advent of broadband Internet as well as the massive proliferation of smart mobile devices brought mobility to the CoIT, leading to the introduction of enterprise mobility. Information security standards in organisations have remained targeted on endpoint solutions liked antivirus software as well as intrusion detection systems (Chen, 2014). Enterprise mobility has experienced different trends like the BYOD, CYOD, HYOD and BYOT (French et al., 2014). BYOD is the most popular and prevalent of these trends in enterprise mobility. The focus of this study is mainly on BYOD. While enterprise mobility trends exist across all industries, the industry of focus for this study is the banking industry.

It is also evident that employee behaviour and attitude are key focus areas when studying how BYOD information security can be built. Whilst technical solutions to BYOD information security exist, the permanent solution to this challenge for many CIOs is to address the employee. Studies from psychology have shown that human beings are social beings who respect their values and cultures (Montesdioca & Maçada, 2015). Schein (2009) remarks that in order to build an ISC, employees need to unlearn their old beliefs and ways of relating to their work. Thomson and Von Solms (2005) point out that there is a need for information security obedience as a starting point in building an ISC. Therefore, this study applies these theories in building an ISC for the unintended administrator for a commercial bank in Zimbabwe.

Summation of Literature Review

From the literature review that was conducted for this study, it can be concluded that BYOD information security is becoming vital for organisations, such that they have to invest in it appropriately and at the right level of the organisation. Clearly, mobile device manufacturers have proffered technical solutions to manage information security but these solutions are specific to the manufacturers' devices. What is required is a platform agnostic solution that ensures BYOD information security regardless of the model of the device connecting to the OC.

The literature review identified that information security is in fact a subculture of OC. In order to understand OC, psychological theories pinpointed several aspects regarding employee contribution to the overall functioning of the organisation that come into play when building a culture. According to Schein (1991), OC can be categorised on three levels – artefacts, espoused values and the shared tacit assumptions in an organisation. However, this perspective merely positioned OC without necessarily giving the existing types of OC. Hofstede (2011) classifies OC into six types without providing means for measuring it, and Denison (1990) measures OC in line with four factors – mission, adaptability, involvement and consistency.

In order to understand how an ISC can be built, it is evident in the literature that employee behaviour and attitudes play a central role in the process. Ajzen (2002) argues that an employee's behaviour is driven by behavioural intentions which are closely related to the individual's attitude towards subjective norms, which he referred to as the theory of reasoned action. The consequences of carrying a particular behaviour at the individual's volition determines if the action is carried out or not. Ajzen's (2002) theory of planned behaviour (TPB) dictates that an individual's behaviour or action is not based on his/her own volition. Understanding these cognitive aspects of human behaviour assists in creating the basis for building an ISC.

The literature also identified that the real challenge with BYOD is not necessarily the impact that it has on organisations but rather how organisations have adapted to it. Similarly, it can also be inferred that an organisation's information security is not necessarily built from the beginning but organisations transition such a culture. The banking industry is a highly regulated environment such that creating an ISC is a fairly easy task as employees are used to having the organisation regulating and controlling how they operate their information systems.

The CoIT together with enterprise mobility have influenced organisations' technology culture. BYOD is emerging as one of the prominent trends in enterprise mobility, which have disrupted organisations' information security management. The banking industry, which is the main focus of this study, appears to be one of the industries where much of this disruption has occurred. The entrance of young generation employees to the workplace has also given impetus to these disruptions. Young generation employees grew up with the technology and are more comfortable using their devices for work-related tasks. This has compelled banks to move away from traditional banking methods and adopt banking on the move through BYOD.

The last chapter in literature review confirmed that building an ISC, even in the banks, is an imperative competitive advantage. Inasmuch as technical solutions to BYOD security exist, the real, permanent answer lies in equipping employees with a BYOD ISC. The additional following findings emerged from the literature:

1. The adoption of the BYOD in the workplace, especially in banks, is imperative for gaining competitive advantage.
2. Organisations across several industries have a dominant culture which is supported by subcultures that involve certain ways of managing the business environment. ISC is one such subculture of the dominant OC.
3. Human psychology theories play a central role in building cultures in organisations.
4. Employees play a central role in building an ISC around the BYOD in organisations.

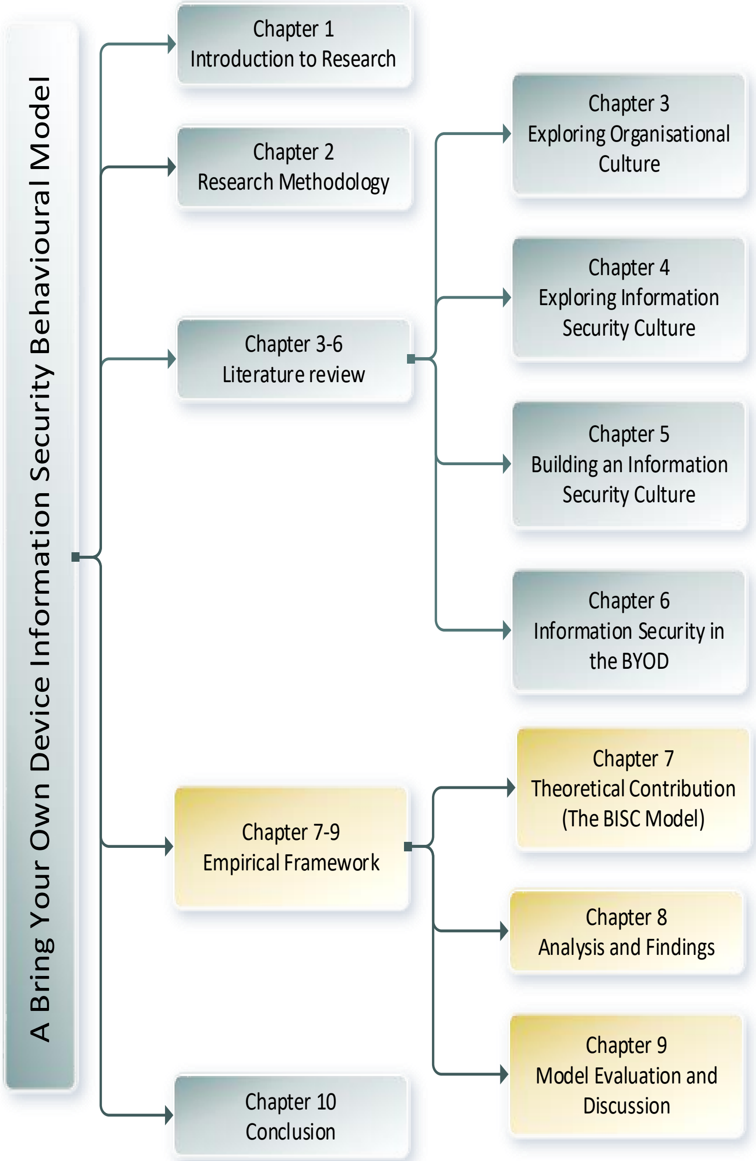
Bring Your Own Anything (BYOX)

CYOD is an enterprise mobility trend whereby employees choose a device to use from a set of devices that the organisation offers and the device remains an organisational asset controlled by the organisation's IT. CYOD is similar to Corporate Owned, Personally Enabled (COPE) in that the organisation owns the device (Leclercg-Vandelannoitte, 2015). The only difference between the two is that in COPE the employee is not necessarily controlled by the organisation's IT and is at liberty to operate under the conditions of BYOD on an organisation's device (Ovum, 2014). CYOD is also similar to Here's Your Own Device (HYOD) where IT departments acquire and configure mobile devices for use by employees for a particular organisation. Company Owned Business Only (COBO) is another trend in enterprise mobility whereby the employee is given a device strictly for business use. The term "COBO" is often used interchangeably with "HYOD". Further, BYOA is another trend by which employees use their own applications for business-related functions. This is very common among employees who work as consultants. Ackerman and Krupp (2012) believe that there is a Bring Your Own Technology (BYOT) culture among employees who work as consultants, whereby they bring their own technology for use at work and these often work remotely and connect to the organisational network using the VPN.

Whilst there is a wide array on enterprise mobility trends, this study will focus on BYOD. The main objective of this study is to create a model for building an ISC for the BYOD unintended administrator. This study will take the form of a case study for a commercial bank in Zimbabwe. In order to achieve this objective, the next section will explore the application of BYOD in the banking sector with a focus on the information security aspects of the BYOD. The next section will explore how a BYOD ISC can be built in a bank. Theories of human behaviour will be applied in engaging with the literature and an inductive approach will be used to identify how the existing ISC factors concerning BYOD have been built from the literature.

EMPIRICAL FRAMEWORK

An Empirical Examination into the Model for Building an Information Security Culture around the BYOD Unintended Administrator


A Bring Your Own Device Information Security Behavioural Model
Chapter 1
Introduction to Research
Chapter 2
Research Methodology
Chapter 3-6
Literature review
Chapter 3
Exploring Organisational Culture
Chapter 4
Exploring Information Security Culture
Chapter 5
Building an Information Security Culture
Chapter 6
Information Security in the BYOD
Chapter 7-9
Empirical Framework
Chapter 7
Theoretical Contribution (The BISC Model)
Chapter 8
Analysis and Findings
Chapter 9
Model Evaluation and Discussion
Chapter 10
Conclusion

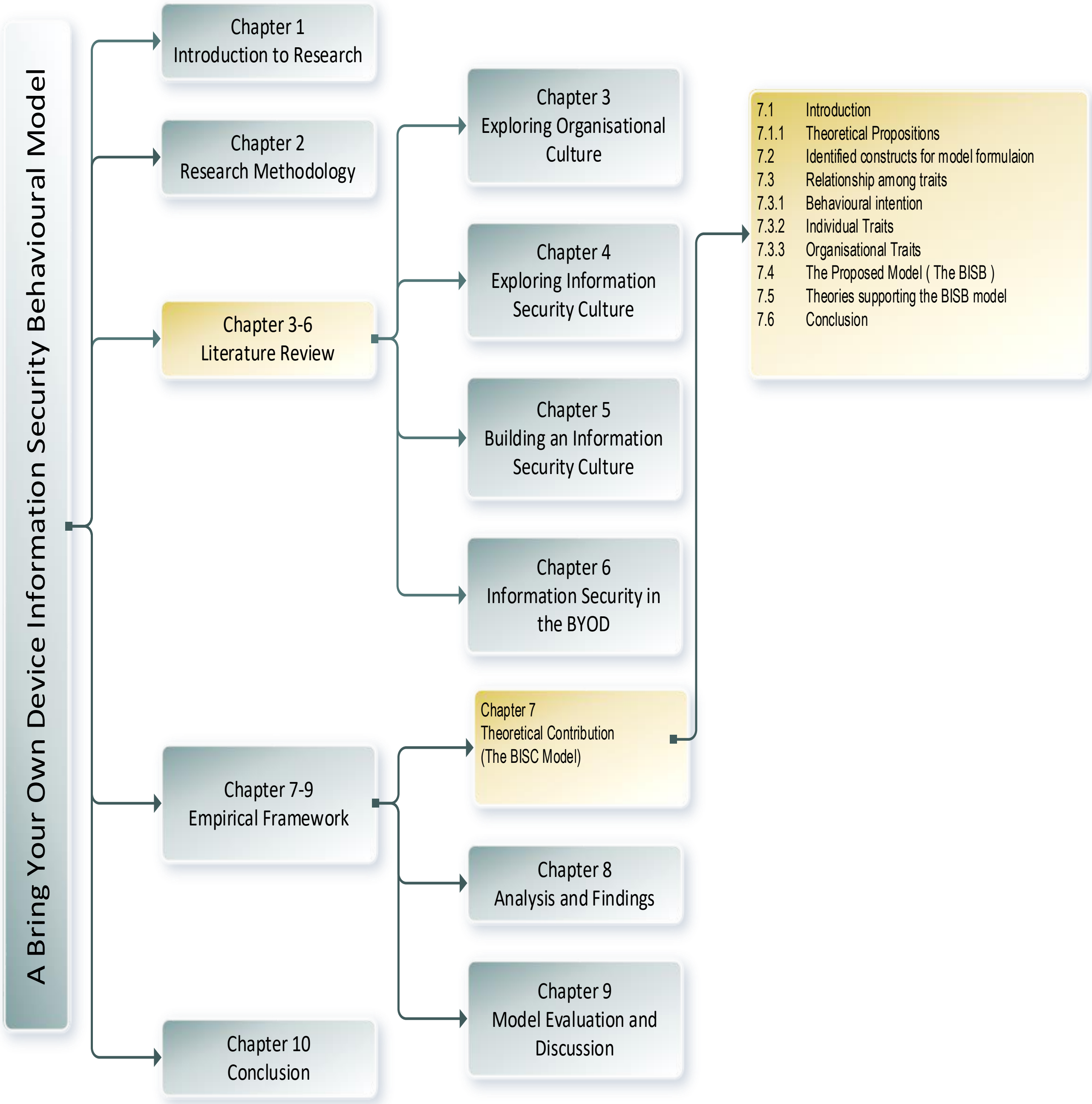
Overview of the Empirical Framework Section

This section contains an empirical review of the way in which this study attempts to secure the BYOD unintended administrator. The aim of this study is to create a model for building an information security culture (ISC) for the BYOD unintended administrator in a commercial bank in Zimbabwe. The study takes the form of a literature review to come up inductively with propositions and constructs for the model. Social science theories for building organisational and human behaviour were used in Chapters 3 and 4 to bring about rigour regarding the traits which were identified as relevant for building an ISC. The aim of this study is to prove that while there are technical solutions to BYOD, the real solution lies in building an ISC within the employees of a particular organisation. The methodical approach used to provide answers to research questions was discussed in detail in Chapter 2. The empirical framework applied in this study will now be discussed followed by the presentation of the findings of the empirical framework. A critical discussion of the research findings as well as the theoretical contribution based on the findings will also be presented.

The empirical framework is divided into three sections: the theoretical contribution, the analysis and findings, and the model evaluation and discussion. The section begins by introducing the research artefact – the BYOD ISC model for the unintended administrator. The model is made up of both individual and organisational traits. The individual traits are further broken down into attitude, knowledge and habit, while the organisational traits are broken down into environment, governance and training. These traits are subsequently explored, resulting in the formulation of theoretical propositions that will be tested in Chapter 8. Chapter 8 addresses the analysis of the survey results and the conclusions formulated based on the analysis process. Statistical tests of factor analysis, correlation between variables as well as multiple regression were conducted. These statistical findings were used to evaluate the theoretical propositions introduced in Chapter 7. An expert evaluation process was also used to evaluate the refined research model. The next section examines the theoretical contribution.

Chapter 7 : Theoretical Contribution (The BISB Model)

“Every problem can be solved as long as they use common sense and apply the right research and techniques.” Daymond John


A Bring Your Own Device Information Security Behavioural Model
Chapter 1 Introduction to Research
Chapter 2 Research Methodology
Chapter 3-6 Literature Review
Chapter 7-9 Empirical Framework
Chapter 10 Conclusion
Chapter 3 Exploring Organisational Culture
Chapter 4 Exploring Information Security Culture
Chapter 5 Building an Information Security Culture
Chapter 6 Information Security in the BYOD
Chapter 7 Theoretical Contribution (The BISC Model)
Chapter 8 Analysis and Findings
Chapter 9 Model Evaluation and Discussion
7.1 Introduction
7.1.1 Theoretical Propositions
7.2 Identified constructs for model formulaion
7.3 Relationship among traits
7.3.1 Behavioural intention
7.3.2 Individual Traits
7.3.3 Organisational Traits
7.4 The Proposed Model (The BISB)
7.5 Theories supporting the BISB model
7.6 Conclusion

7.1 Introduction

This chapter introduces the model that is at the centre of this study and concludes by establishing the link with social science theories, showing how they support the constructs of the proposed model. Human behaviour theories and models stem from social science disciplines (Morris et al., 2012). Disciplinary frontiers simply serve to delineate the types and contexts of human behaviour in which researchers are interested. The way in which behaviour is attained, including the methods through which it can be studied, is another area of focus.

The literature review section was made up of four chapters, which included Chapters 3 to 6. Chapter 3 focused on exploring OC, and was followed by an exploration of ISC in Chapter 4, where it was viewed as a subculture of OC. Chapter 5 examined the way organisations can build an ISC and concluded with an examination of BYOD information security in Chapter 6. The research model introduced in this chapter makes use of relevant literature (as discussed from Chapters 3 to 6) to set the foundation on which to build the model constructs. The research approach took the form of a single case study on a commercial bank in Zimbabwe. A research instrument in the form of a questionnaire was used to conduct a survey, and observations and interviews and an expert review process were also applied.

The survey findings help quantify the findings of the literature study. The results from the research instrument and the empirical study are discussed in Chapter 8, which constitutes an analysis of the findings of the study.

This chapter starts by outlining the way the model constructs were identified from the literature review. The identification process and the model are further supported by theories on organisational behaviour and human behaviour. The identified constructs will then be grouped as individual and organisational traits. The relationships between the constructs will then be examined culminating in the creation of a model for building an ISC for the BYOD unintended administrator. It is should be reiterated at this point that this research is based on the banking sector. Theoretical propositions were used to evaluate the model and these theoretical propositions were then enlisted in section 7.3 of Chapter 7 and later evaluated in section 9.4 in Chapter 9 of this thesis. The evaluation results of the theoretical proposition provided rigour to the model constructs. Section 9.5 in Chapter 9 presents the model which encompasses the test results for the constructs.

7.1.1 Theoretical Propositions

A theoretical proposition is a theory that explains both the occurrence and the phenomena which in essence are the data and what is actually happening. In this study, the three individual traits of knowledge, attitude and habit combined with the three organisational traits of environment, governance and training were formulated into theoretical propositions for evaluating the model. Statistical tests were conducted on the theoretical propositions as explained in section 9.4 (Chapter 9), consequently resulting in the formulation of a model

7.2 Identified Constructs for Model Formulation

As shown in Chapters 4 to 6, in every organisation, the ISC is influenced by individual employee characteristics and the OC. Supported by behavioural science theories, Chapter 3 discussed how organisational ISC management influences the way information security is managed in a given organisation.

Key individual traits of attitude, knowledge and habit and organisational traits of environment, governance and training were identified as constructs for the model. Figure 35 shows the steps followed in the model formulation process.

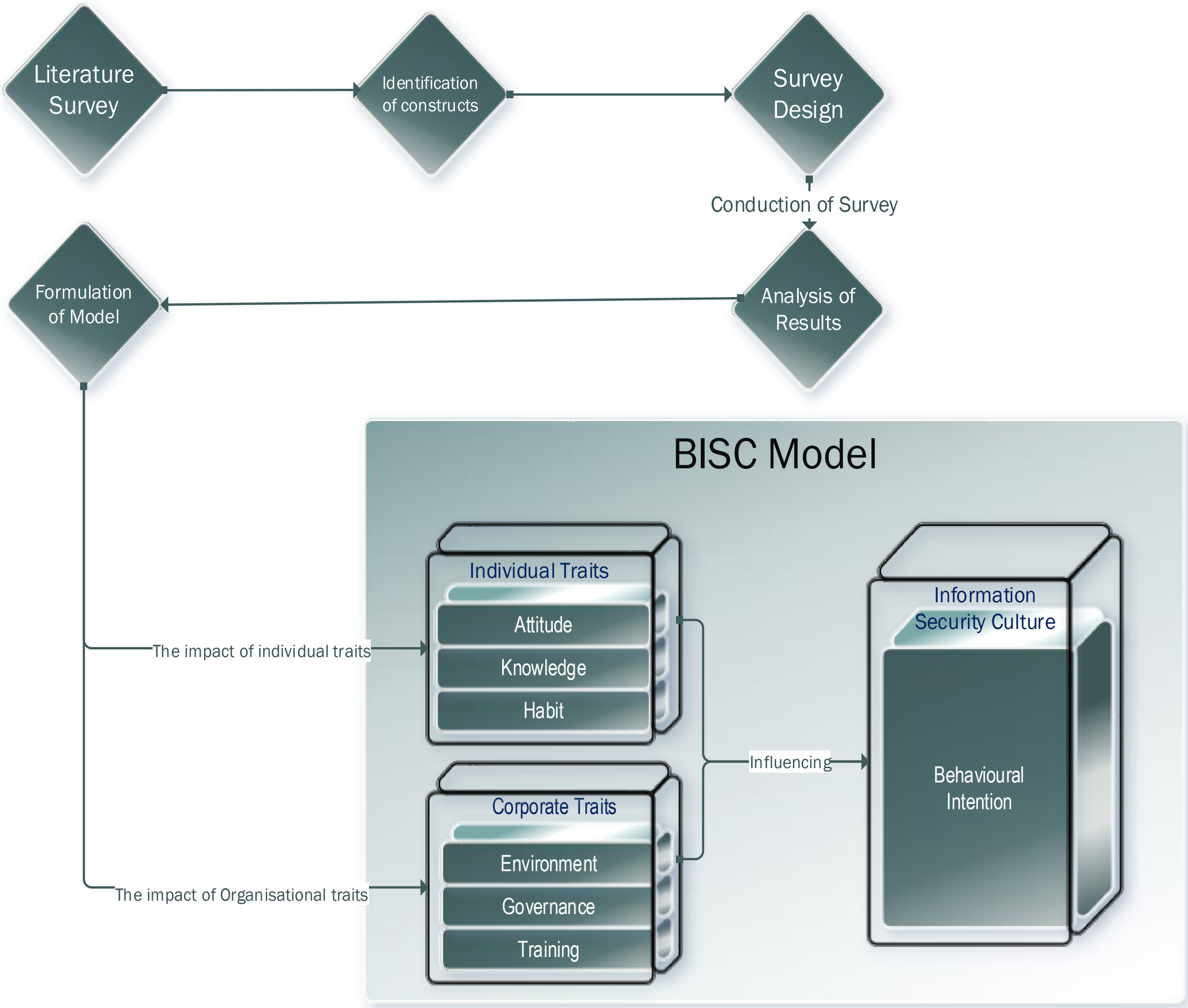


Figure 35. Identification of Model Constructs

While this chapter provides an overview of the model, the various elements of the model have been discussed thoroughly in the previous chapters. Chapter 2 detailed the way the research methodology was followed and the research instrument (refer to Appendix 1) based on the findings of the literature review. To that effect, this section then constitutes the part of the "whole" that is discussed throughout this research project, as explained by GST discussed in Chapters 1 and 4. The various constructs for the model will be discussed in the next section.

7.3 Relationship among Traits

The traits identified from the literature all share the common characteristic of influencing the behavioural intention to build an ISC for the BYOD unintended administrator. Notably, attitude, knowledge and habit are all characteristics related to human behaviour and are classified as individual traits. Environment, governance and training were identified as being related to an organisation and, in this study, these are grouped under organisational traits. Despite this classification, these six traits collectively influence the behavioural intention to build information security for the BYOD unintended administrator. Such behavioural intention is viewed as being the same as the ISC for the BYOD unintended administrator. The subsequent subsections detail the six traits that form the model constructs grouped as individual and organisational traits. Before discussing the six traits, behavioural intention will be introduced in the context of this research study in section 7.3.1. Theoretical propositions are then formulated to measure each trait, which in essence are the constructs for the model.

7.3.1 Behavioural Intention

A large number of studies within psychology focus directly on the individual as the locus of behaviour. According to Tharp (2009), the complex whole, which includes knowledge, belief, arts, morals, law, custom, and any other capabilities and habits, acquired by man as a member of society forms the behavioural intention which can be summed up as a culture. The findings of this study uncover links between ISC and information security behavioural intention, which translate to the security culture exhibited by employees in the bank where the study was conducted. In this study, behavioural intention represents ISC. The theory of planned behaviour (TPB), discussed in Chapter 4, provides a reliable reference for appreciating behaviour by introducing specific components of attitude, subjective norms and perceived behavioural control that directly influence employees' behavioural intentions. According to Fishbein and Ajzen (1992), the person's perceived, and not necessarily the actual, behavioural control is a sufficient motivator for influencing behavioural intention. In this study, the behavioural intention for employees to observe and implement information security traits was used to represent the ISC. The next section explores the individual employee traits that influence the BYOD ISC.

7.3.2 Individual Traits

Several research projects on information security focus on the human component, for instance information security training (Kruger & Kearney, 2006; Puhakainen & Siponen, 2010), employee insider computer crime (Leclercg-Vandelannoitte, 2015), as well as information security policy obedience (Pahnila, Siponen, & Mahmood, 2007; Vroom & Von Solms, 2004). All are aimed at minimising the threat that user behaviour poses to the protection of information assets. This research study identified and grouped three traits to represent individual traits, as shown in Figure 36.

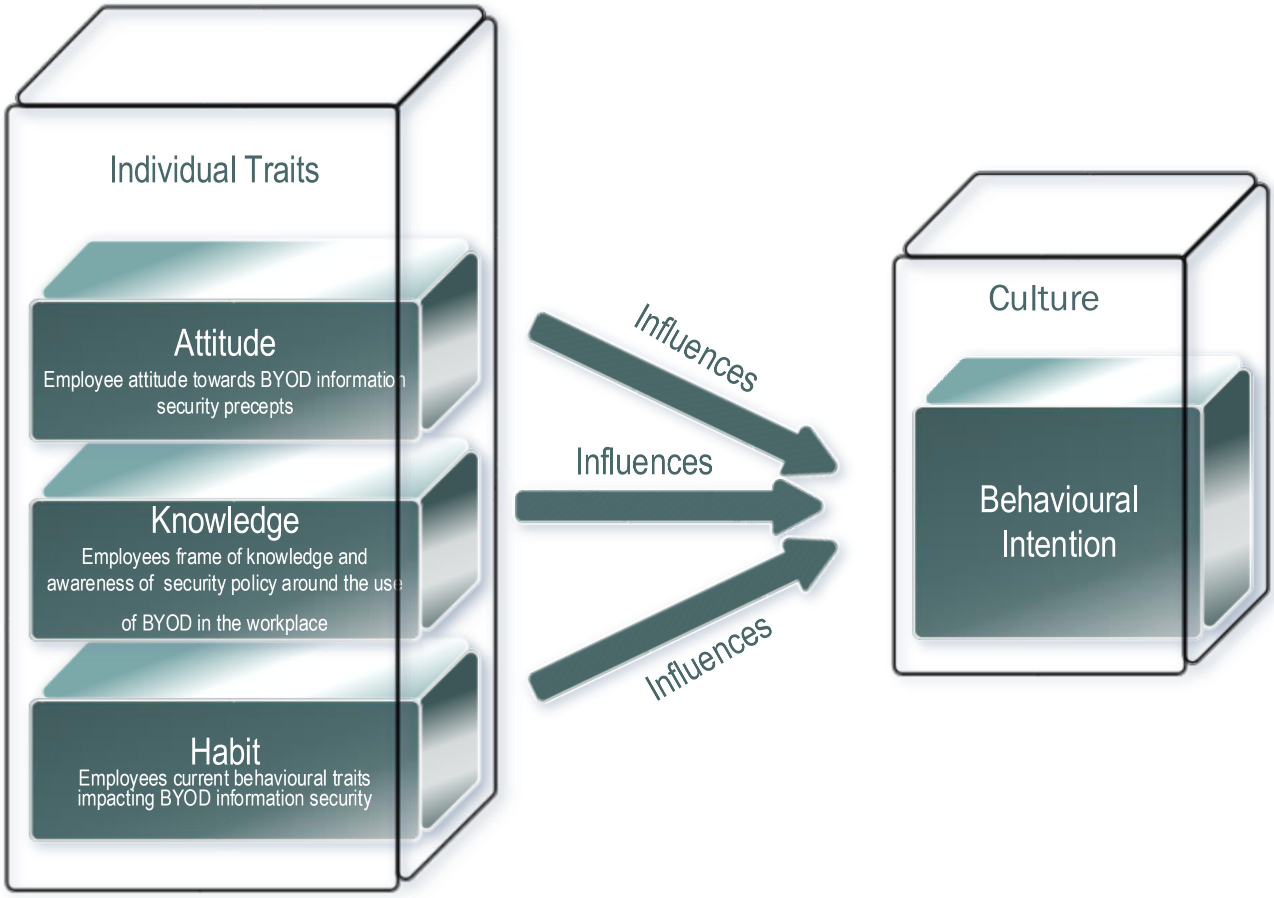

Individual Traits
Attitude
Employee attitude towards BYOD informatio
security precepts
Knowledge
Employees frame of knowledge and
awareness of security policy around the us
of BYOD in the workplace
Habit
Employees current behavioural traits
impacting BYOD information security
Influences
Influences
Influences
Culture
Behavioural
Intention

Figure 36. Individual Traits for the BISB Model

The three individual traits, attitude, knowledge and habit, were found to be capable of influencing the employee behavioural intention to observe information security. Their application was confirmed by theories discussed in Chapters 3 and 4. The various components of the model will now be introduced and discussed in more detail.

i. **Attitude**

Allam, Flowerday, and Flowerday (2014) remark that attitude is what people think. In this study, attitude is what employees think about BYOD information security, which includes the technology they use, the organisational policy framework they apply, and how they adhere to the policy. Attitude determines employee ISC as it influences the level at which they observe the policy frameworks and rules surrounding its implementation (Van Niekerk & Von Solms, 2010). According to Lennon (2012), attitude can be either positive or negative. In this study, the development of a positive attitude towards BYOD information security for the banks in Zimbabwe is explored.

The TPB claims that the intended behaviour influences the attitude towards that behaviour. If applied to this study, it points to the fact that the attitude that the employees have towards BYOD information security and the organisational policies determines how information security can be improved in the banks (Ajzen, 1991). With regard to the same trait of attitude, Da Veiga and Martins (2014) maintain that an ISC consists of employees' attitude and beliefs with respect to information security. Furthermore, ISC consists of knowledge of the organisation's information security policy as well as compliancy requirements. In agreement with this perspective, Alfawaz and Nelson (2010) propose IS behaviour modes that organisations must observe in building an ISC. Section 4.3 in Chapter 4 discussed these modes in detail. Chen et al. (2015) believe that ISC is an assemblage of shared security values, beliefs and assumptions in information security in the organisation and can lead to unconscious, continuous habits that formulate the behavioural intention toward ISC. (Lee, Lee, and Kim (2016) remarked that employee attitude to compliance with the information security policies and standards within an organisation mitigates work overload and invasion of privacy, which they formulated into an information security stress management model. In this study, attitude was thus identified as being a key member trait in formulating a BYOD ISC.
Based on this the following research proposition was made:

- ✓ ***Proposition P1**: The employee attitude towards information security is positively associated with the building of an information security culture in the BYOD phenomenon in a commercial bank in Zimbabwe.*

ii. Knowledge

Separate research studies define knowledge as what people know (Allam et al., 2014; Kruger & Kearney, 2006; Safa & Von Solms, 2016). In this context, knowledge can be defined as what employees know about BYOD information security in a bank in Zimbabwe. Furthermore, what the employees know about BYOD hardware, the software used to manage and drive the devices, the data contained in these devices, the policies and procedure required to optimally operate the BYOD devices, as well as the people who operate these devices. This knowledge is in essence the operational knowledge of the technical devices in use and how it fits within the organisation's IS policy framework. Operational knowledge of the devices ensures secure usage of the device; for instance, employees will need operational knowledge to understand the risks of downloading software that may be malicious to their operations (Twinomurinzi & Mawela, 2014). In a bank, operational knowledge of the organisational policy framework is central in implementing the BYOD information security (Mphahlele, 2016).

Banking organisations recruit and appoint employees based on some inherent knowledge they possess to hold certain job profiles. Ahmed, Ragsdell, and Olphert (2011) argue that knowledge underpins the success of knowledge management initiatives within an organisation and has been recognised as a vital activity for organisational transformation and success in implementing new solutions and standards within the business.

BYOD information security requires employees to be knowledgeable about the devices that they operate. In order for the BYOD information security to be implemented, there is a need for organisations (banks in this context) to invest in employee training and awareness on the consequences of not managing information security on their devices properly. D'Arcy (2011) argues that organisations require technology savvy employees who can operate the new technologies, which points to the requirement for technical knowledge. The attitude of the employees who are knowledgeable on the consequences of not observing an ISC and those that are not knowledgeable differs. Notably, an investment in knowledge and training on BYOD information security will encourage the right attitude and behaviour towards information security from employees.

Safa and Von Solms (2016) argue that knowledge plays an important role in the domain of information security owing to the positive effect it has in fostering employees' information security training. Knowledge of the information security risks makes it easy for banking organisations to implement attendant IS policies and encourage the sharing of best practices. Van Niekerk and Von Solms (2010) argue that lack of IS knowledge on the part of the employees is detrimental to the organisation; as such organisations have to invest in employee IS knowledge. Based on these literature review findings, the following proposition on knowledge as an individual trait influencing the improvement of an information security culture for the BYOD phenomenon was formulated and proposed as one of the three key individual traits that influence the employees' behavioural intention to implement BYOD information security.

- ✓ ***Proposition P2**: Employee knowledge is positively associated with the building of an information security culture in the BYOD phenomenon in a commercial bank in Zimbabwe.*

The next section discusses the third trait of habit, which completes the three identified traits constituting the constructs for the model under discussion.

iii. Habit

Social theorists have agreed that people generally act habitually in the world, not reflectively (Hopf, 2010). Vance, Siponen, and Pahnila (2012) define habit as a routinised form of past behaviour, while Pahnila et al. (2007) view habit as unconscious or automatic behaviour. The habits that the employees develop in using BYOD are part of the three individual traits identified in the literature. Banking organisations should consider employees' habits when dealing with BYOD information security (Chen et al., 2013). Employees develop certain routines in dealing with information assets that collectively have an influence on habitual perceptions which inform how the ISCs for an organisation can be improved. This is even more important with BYOD, as employees will also develop habits or routines on their private devices at home which will extend to the workplace. How employees secure their private phone with regard to physical access or authorisation to access the phone at home is unlikely to change when they enter the workplace. Following this lead, this study suggests that habitual behaviour explains the ISC for individuals in any banking organisation. The following research proposition was made:

- ✓ ***Proposition P3**: The employee's habits towards information security are positively associated with the building of an information security culture in the BYOD phenomenon in a commercial bank in Zimbabwe.*

7.3.3 Organisational Traits

Information security for BYOD in the organisations is also influenced by other organisational traits besides the individual traits. Leclercg-Vandelannoitte (2015) states that two contrasting perspectives exist for organisations' BYOD implementing security. The first perspective is that organisations build IT systems that users either want to use or not, while the second perspective maintains that users introduce IT systems that organisations want to incorporate or not. In this study, with its focus on the employee as an unintended administrator, the emphasis is on the second perspective. The organisational traits identified in this study cushion the resultant organisational traits that influence how the employee can make use of the BYOD securely.

The organisational traits were discussed in detail in Chapter 3, which explored OC. Notably, OC is the face of the organisation which to a large extent portrays the management inclination and appetite for information security. From the literature review conducted in Chapter 4, which explored information security regarding BYOD, it is also noted that the management tone on BYOD information security, the environment and the training and awareness given to the employees all influence the behavioural intention to implement information security. This, thus, informs the three organisational traits as portrayed in Figure 37. The combination of these three organisational traits culminates in organisational behavioural intention to implement security, which is viewed as an ISC in this study.

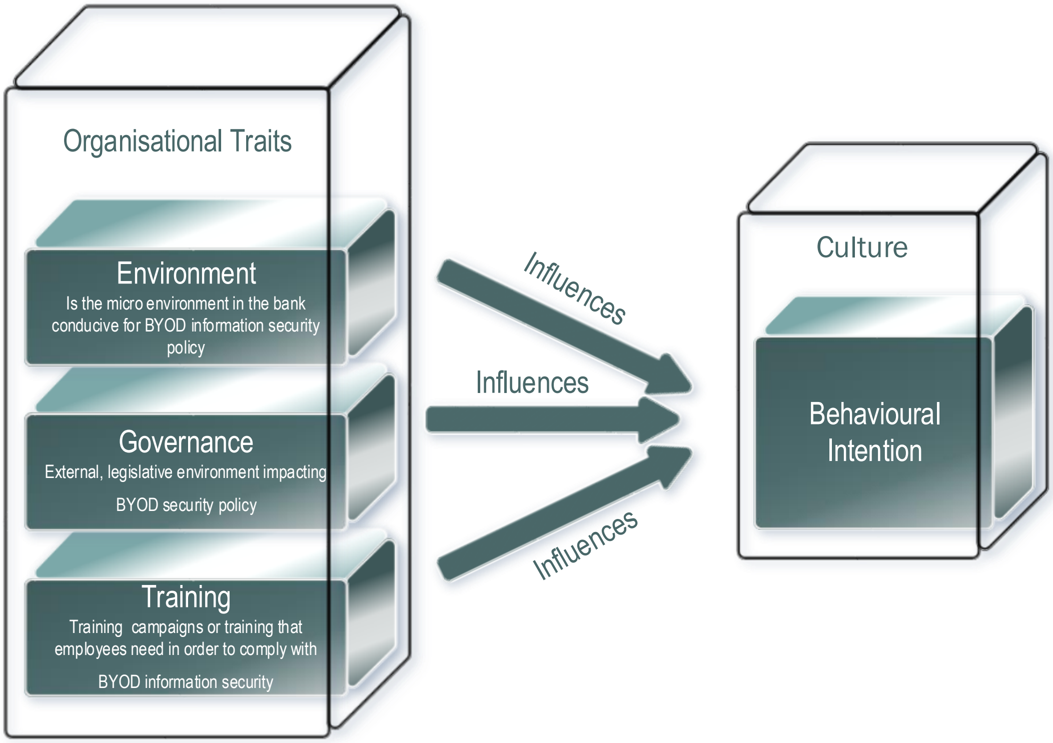

Organisational Traits
Environment
Is the micro environment in the bank conducive for BYOD information security policy
Governance
External, legislative environment impacting BYOD security policy
Training
Training campaigns or training that employees need in order to comply with BYOD information security
Influences
Influences
Influences
Culture
Behavioural Intention

Figure 37. Organisational traits for the BISB model

The next section discusses the three organisational traits that influence the OC for BYOD.

iv. Environment

Organisational traits include the microenvironment, which was identified as being one of the key role players in the formulation of employee behavioural intention (Gordon, 1991). According to Farooq and Amin (2017), a correct environment is associated with a better ISC. Vignesh and Asha (2015) state that the massive penetration of mobile devices, like smartphones, tablets and phablets, have changed the business environment. The highly dynamic banking environment is characterised by complex competitive practices, where an employee finds derivative values that correspond to institutionalising the means by which the organisations conduct their business. BYOD is one such derivative value that gives employees the latitude to work flexibly (Köffer & Fielt, 2015).

The environment determines the level of sophistication as well the rate at which BYOD security is propagated (Farooq & Amin, 2017). Chapters 3 and 4 give cases of environmental controls within banks and other organisations that influenced the manner in which BYOD information security is implemented. The absence of a uniform approach to adopting BYOD, as a consequence of the different environments that exist in organisations, is the major reason why organisations need to look at the environment when formulating information security (Singh & Phil, 2012). The environment in any organisation is closely related to how the organisation is managed and in this study the way an organisation is managed will be described as governance. This led to the research proposition below:

- ✓ ***Proposition P4:*** *The macro environment is positively associated with the building of an information security culture in the BYOD phenomenon in a commercial bank in Zimbabwe.*

The next section discusses organisational governance as one key member trait influencing the behavioural intention to comply with the set parameters of information security.

v. Governance

Organisational governance is another key component identified as having an impact on ISC. Information security management theorists assert that employee behaviour needs to be directed and censored to ensure that it is amenable to organisational information security standards (Dillon, Stahl, & Vossen, 2007; Rastogi & Von Solms, 2012; Vroom & Von Solms, 2004). An ISC in the banking sector is a prerequisite for good governance and the application of an effective regulatory framework (Da Veiga & Martins, 2014). Vignesh and Asha (2015) caution that there is an urgent need for organisations, including banks, to modify their information security governance policies so as to address the challenges that come with BYOD. Kufandirimbwa et al. (2013) consider governance to be a key organisational function that needs to be reinforced to ensure the functional integration of the systems and structures. In the context of BYOD for banks, a good governance system will improve information security, thereby forming an ISC for the BYOD unintended administrator. The literature reviews contained in Chapters 3 to 6 identified governance as a key function in the formulation of the behavioural intention to observe information security.

Section 4.3 notes that banks consider governance to be a central aspect of any bank's operation. Section 5.4 explains governance as a key function in behavioural intention to observe information security. In order for the governance standards to permeate down to the employees, this study identified training as another important organisational component for building an ISC. The following research proposition was thus formulated:

- ✓ ***Proposition P5:*** *Governance is positively associated with the building of an information security culture in the BYOD phenomenon in a commercial bank in Zimbabwe.*

vi. Training

Training on the information security plan for the organisation is another key component, which was identified in the literature review as a pillar in building an ISC. Because employees come from different backgrounds, most of them lack basic awareness of the consequences of breaching information security guidelines (Al-shehri, 2012). Information security training differs from awareness in that training is more formal and is confined to classrooms whereas training is more relaxed and very informational (Lim et al., 2010). Training teaches employees to be conscious about the ISC in an organisation while awareness conscientises them. Further, organisations may not achieve high levels of ISC if training is low among employees (Lim et al., 2010).

Banking organisations need to ensure that their employees are aware of the organisational standards on information security. This can be achieved through awareness campaigns, bulletins, as well as other available means to reach out to employees. Von Solms and Von Solms (2004) believe that there is need for a continuous information security training programme to ensure initial education, and also that regular updates and reminders should reach the employees. On the same construct of training, Brodin (2016a) states that information training is an area that requires improvement in many organisations. Organisations have to take proactive measures to make sure that their employees are aware of the organisational direction and position regarding information security (Brodin, 2016b). The following research proposition was formulated:

- ✓ ***Proposition P6:*** *Training is positively associated with the building of an information security culture in the BYOD phenomenon in a commercial bank in Zimbabwe.*

7.4 The Proposed Model (The BISB)

As mentioned in section 7.2, the "whole" consists of many parts. In this study, these parts, as well as the relationship between them, have been discussed throughout as sections or chapters with their own emergent properties. Thus, each chapter of the thesis is part of the whole presented in this research project, with the emergent property being a model to build an ISC for the BYOD unintended administrator. The emergent property will enable the development of more effective unintended administrators who are aware of information security risks.

Figure 38 illustrates the combination of individual and organisational traits culminating in a BYOD information security behavioural (BISB) model for the banking sector in Zimbabwe. The various components were described in detail in section 7.3 of this chapter. In the model, the individual and organisational traits complement each other as constructs for the BISB model. The traits were amalgamated from the literature study and funnelled into the behavioural intention construct which represents the BISB. The BISB model will be tested in Chapter 9 to confirm its applicability. This will follow the analysis and findings of the results discussed in Chapter 8.

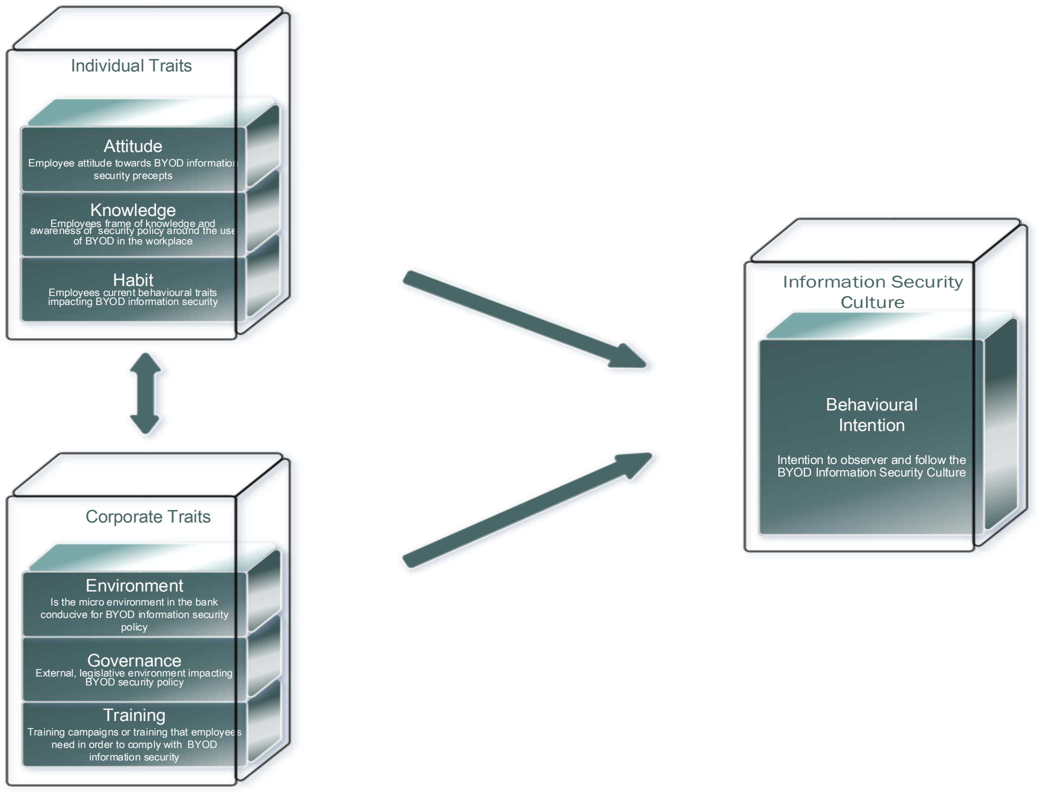

Individual Traits
Attitude
Employee attitude towards BYOD information security precepts
Knowledge
Employees frame of knowledge and awareness of security policy around the use of BYOD in the workplace
Habit
Employees current behavioural traits impacting BYOD information security
Corporate Traits
Environment
Is the micro environment in the bank conducive for BYOD information security policy
Governance
External, legislative environment impacting BYOD security policy
Training
Training campaigns or training that employees need in order to comply with BYOD information security
Information Security Culture
Behavioural Intention
Intention to observer and follow the BYOD Information Security Culture

Figure 38. The BYOD information security behaviour (BISB) model

The next section discusses the theories that support the model constructs.

7.5 Theories Supporting the BISB Model

Laszlo and Krippner (1998) state that a study of the relationship between theories and the perceptions of humankind helps in our understanding of the changing nature of human behaviour. In academic research, theories systematically order ideas and the phenomenon under study by assisting in the understanding of the concepts under research. OC theories help in viewing organisations through a cultural lens with attention being paid to values, beliefs, and attitudes of members. Human behaviour theories, on the other hand, focus squarely on the individual as the locus of behaviour. Theories and models spring from all disciplines of the social sciences (Morris et al., 2012). In many ways, disciplinary boundaries simply serve to demarcate the types and contexts of human behaviour in which scholars are interested, how behaviour is defined, and the methods via which it might be studied. In this study, human behaviour and OC theories were used to qualify the practicality and relevance of the model constructs.

Table 13. Theories supporting the research model

Classification	Theory Name and Description	Application to the Model
Human behaviour theories	**Theory of reasoned action (TRA):** Section 4.4.1 of Chapter 4 explains that human behaviour is under the person's volitional control**.** People think about the consequences of their actions and behaviour, making them decide whether or not to do something. The theory views behaviour as a function of the attitude towards specific actions or subjective norms regarding that action.	In the BYOD, employees act out of their own volition in choosing devices for use. Their attitude and knowledge as well as habits can be explained by TRA. Attitude and behaviour emerge as two of the three components of the BISB model.
	Theory of planned behaviour (TPB): this theory **w**orks best when the behaviour is NOT perceived to be under the person's control. The intentions are the precursors of behaviour as discussed in section 4.4.2 in chapter 4 of this thesis.	TPB is applicable to the BYOD in explaining the way that employees can be guided as well as the controls on the devices they use under the BYOD. This theory supports the forming of a habit that is guided by the employees' behaviour.
	Hofstede: Section 3.6.2 in Chapter 3 explains in details the cultural differences in the form of four levels of depth: symbols, heroes, rituals and values. There are shared perceptions among employees on daily practices which form the core of an organisation's culture. While practices are	This theory helps to explain the environment in a given organisation. A well-governed organisational environment forms the basis for the implementation of the BYOD ISC.

Organisational culture theories	the visible part of an organisation's culture, values are the invisible part.	
	Denison's organisational culture perspective: As discussed in section 3.6.6 of Chapter 3, this perspective argues that basic beliefs and assumptions are designed to measure specific aspects of an organisation's culture in terms of four factors: mission, adaptability, involvement and consistency.	The environment within an organisation can be best described by using the Denison's theory. A good environment for the development of a BYOD ISC is explained.
	Schein: Organisational culture may be analysed on three separate levels, namely: artefacts, espoused values, and basic underlying assumptions. The three levels are separated on the basis of the degree to which the cultural phenomenon is visible to the observer.	This model best explains the training trait for the BISB model. The three levels put forward in this model form a strong basis for the training construct in the model.

Table 13 contains an analysis of the way OC theories on human behaviour support the constructs resulting in the BISB model, which marks the end of the introductory part of the BISB model. The evaluation and testing of the BISB model will be conducted in Chapter 9.

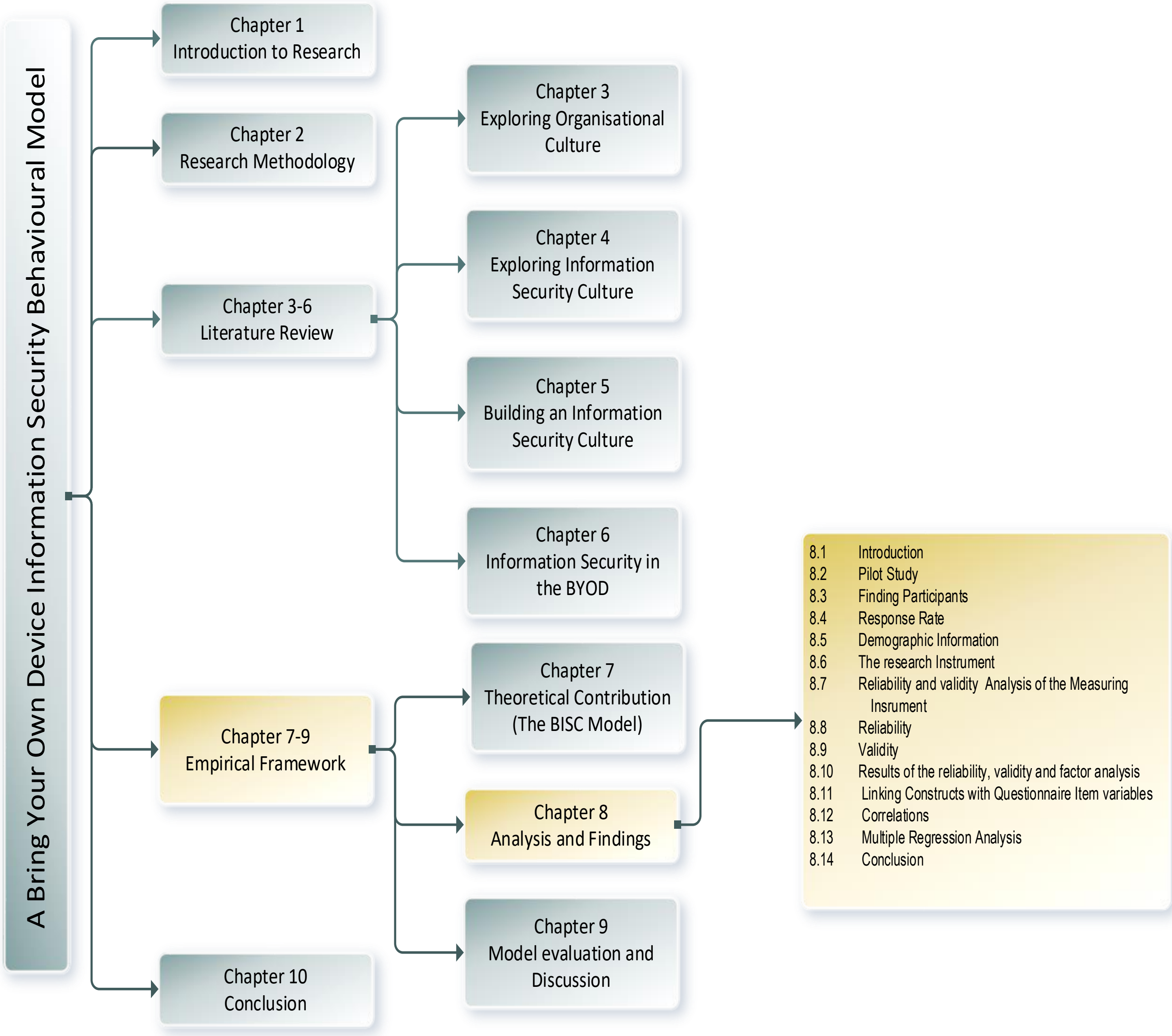
7.6 Conclusion

This chapter introduced the research artefact, which in this instance represents the BISB model. From the literature review, three traits of attitude, knowledge and habit were identified as individual traits for the BISB model (constructs), while three additional traits of environment, governance and training were identified as organisational constructs. The combination of the individual and organisational traits influence employees' behavioural intention to conform to BYOD information security. This relationship between the constructs was followed by a brief exploration of the relationship between the constructs.

The six traits were discussed in detail linking them to behavioural intention, which in this instance is OC. The BISB model was introduced followed by the discussion on how theories in the social sciences support these traits as constructs for the BISB model. Six theoretical propositions were formulated for each construct of the BISB model. The theoretical propositions were used to explain both the phenomenon and phenomena which in essence is the data and what is actually happening per construct. The tests on the suitability and application of the BISB model are discussed in Chapter 8, which constitutes the analysis and findings of the empirical work conducted. The research propositions formally introduced in this chapter will be evaluated in Chapter 9.

Chapter 8 : Analysis and Findings

Statistical literacy is necessary for members of society to critically evaluate the bombardment of charts, polls, graphs, and data that are presented on a daily basis. However, what can often pass for "statistical" analysis more closely resembles a lie." - H.G. Wells


A Bring Your Own Device Information Security Behavioural Model
Chapter 1
Introduction to Research
Chapter 2
Research Methodology
Chapter 3-6
Literature Review
Chapter 3
Exploring Organisational Culture
Chapter 4
Exploring Information Security Culture
Chapter 5
Building an Information Security Culture
Chapter 6
Information Security in the BYOD
Chapter 7-9
Empirical Framework
Chapter 7
Theoretical Contribution (The BISC Model)
Chapter 8
Analysis and Findings
Chapter 9
Model evaluation and Discussion
Chapter 10
Conclusion

8.1 Introduction
8.2 Pilot Study
8.3 Finding Participants
8.4 Response Rate
8.5 Demographic Information
8.6 The research Instrument
8.7 Reliability and validity Analysis of the Measuring Insrument
8.8 Reliability
8.9 Validity
8.10 Results of the reliability, validity and factor analysis
8.11 Linking Constructs with Questionnaire Item variables
8.12 Correlations
8.13 Multiple Regression Analysis
8.14 Conclusion

8.1 Introduction

This chapter presents the findings of the analysis carried out with the purpose of ensuring that the design artefact has been rigorously assessed to ensure its relevance, quality and efficacy. While there are a number of analysis methods (Ahmed & Sundaram, 2011), the analysis method selected is influenced by the design artefact (Hevner et al., 2004). The identified constructs discussed in the previous chapter were used to design a questionnaire for data collection. The questionnaire was distributed to 270 employees via an email link and 205 of these subsequently participated. A total of 170 completed the questionnaires with no missing data and the results obtained from the data collection were then loaded into the SPSS v23 application software. This chapter thus presents the analysis and findings from the data collection. The next section will present findings obtained from the questionnaire, starting with a discussion of the pilot study, the response rate and the demographics of the participants. This will be followed by a discussion on the validity and reliability of the research instrument, the descriptive statistical results; finally, the results of the additional analysis that was conducted will be presented as the findings. Six research theoretical propositions formulated in Chapter 7 will be evaluated in Chapter 9, using the analysis conducted in this chapter and the subsequent findings.

8.2 Pilot Study

In order to plan for the main survey, a pilot study was conducted to refine the research instrument. The questionnaire was formulated from the literature review. Different parts of the questionnaire were formulated from the six constructs identified. Whilst the results of the pilot study were not considered important to the data analysis in this study, the problems the users reported in respect of the data collection instrument were deemed important. The problems included misunderstood questions and unexpected responses from participants. The pilot study therefore involved a limited number of participants who were not included in the actual study. Twelve colleagues at the university participated in the pilot study where they were asked to complete the questionnaire and comment on both user-friendliness and the clarity of the questions. The comments received were used to refine the research instrument to elicit the appropriate responses.

It emerged from the pilot study that five of the questions were ambiguous and required further refinement if the expected responses were to be elicited. The recommended adjustments were accordingly included in the final research instrument. The next section discusses how the participants were selected for the survey.

8.3 Finding Participants

The research participants were employees of the commercial bank where the study was carried out. Approval was received from the University of Fort Hare and the bank (see Appendices 2 and 3) to conduct the survey and consequently a notification was sent to all employees soliciting their participation in the study. The e-mail sent to the employees had an option for employees to choose whether to complete the survey or to decline. The collected results were then loaded into SPSS V23 for analysis.

8.4 Response Rate

A total of 270 bank employees received the online questionnaire loaded in Survey Monkey. Of the population of 270, 205 employees participated, which represents a response rate of 76%. Of these responses, it was found that only 170 had completed the questionnaire, resulting in a response rate of 87% (refer Appendix 2: Questionnaire). Oates (2006) states that a response rate of 30% or higher is acceptable in a research project. Considering that the response rate was well above 30%, it was deemed acceptable. The next section discusses the demographics of the participants.

8.5 Demographic Information

It emerged from the survey results that about 60% of the respondents were males and 40% females. The majority of participants was between 30 and 40 years of age, constituting about 55% of the sample, followed by the 41 to 50 age group, which constituted about 21%. This suggests that the bank's active population is between 30 and 40 years with the majority participants being male. Most of the employees (89%) owned mobile devices. The majority of employees (92%) confirmed that they understood the distinction between personal and organisational data and were able to keep them wholly separate while using a personal device for work.

Table 14. Demographic Profile of the Respondents

Item	Category	Frequency	Percentage (%)
Gender			
	Male	106	59.2
	Female	72	40.4
	Did not indicate*	1	0.6
	Total	170	100
Age			
	<30	29	16.2
	30–40	99	55.3
	41–50	37	20.7
	>51	14	7.8
	Total	170	100
Employees who own a mobile device			
	Yes	159	88.8
	No	18	10.1
	Did not answer*	2	1.1
	Total	170	100
I understand the distinction between personal and organisational data and am able to keep them wholly separate while using a personal device for work			
	Yes	165	92.2
	No	11	6.1
	Did not answer*	3	1.7
	Total	179	100

**Respondents did not specify*

The next section discusses the questionnaire used in the data collection process. As discussed in Chapter 2, the constructs were included in this study as factors for building the BYOD ISC.

8.6 The Research Instrument

The purpose of analysing data is to create meaning from the raw data collected (Creswell, 2009). Comparing and evaluating the raw data and analysing the feedback received from the participants was the method used to report findings from the questionnaire. Chapter 2 contains the questionnaire formulation process in detail. Seven traits (attitude, knowledge, habit, environment, governance, training and behavioural intention) were identified from the literature which were then used to demarcate the questionnaire into sections that addressed these traits. These traits were discussed in the literature chapters and identified with propositions which formed the building blocks of the model. The identified constructs were then grouped into individual factors which impact on the BYOD information security and organisational factors that directly link to the influence that the organisation, or bank in this instance, has on BYOD information security. The survey questions were grouped according to the constructs identified in the literature and then loaded into Survey Monkey. The links were emailed to the employees and the responses were collected in the portal. These were subsequently cleaned, coded and exported for analysis.

8.7 Reliability and Validity Analysis of the Measuring Instrument

This section examines how well a measuring instrument evaluates the given variables. The first step in the data analysis process involves assessing the discriminant validity of the research instrument, which in this instance is the questionnaire. Factor analysis was used, specifically principal component analysis using an oblimin rotation method with Kaiser normalisation. The reliability of the questionnaire was tested using Cronbach's alpha. No exploratory factor analysis was conducted on the dependent factor, that is, the employees' behavioural intention. Notably, the behavioural intention in this study represents the ISC. It was decided that this would be of no significant value in view of the diversity of measures making up this construct. Consequently, it was expected that no underlying dimensions of this measure would exist.

Common exploratory factor analysis was used to identify the various factors measured by the variables, which were later classified into individual and organisational variables. This was done by extracting the combinations of variables that explained the greatest amount of variance. Based on the literature review discussed in Chapters 3 to 6, six independent factors were identified and grouped into individual and organisational factors. These factors were then subjected to a factor analysis process in order to verify their unidimensionality. The factors attitude, habit, knowledge, training, environment and governance were identified through six iterations. The variables that did not load higher than 0.300 were deleted. This cut-off point was based on the exploratory nature of the study. Since the aim of the study is to develop a model for building an ISC for the BYOD, it was deemed prudent not to make the cut-off point too high as possible variables that may have affected the model's success might have been omitted. The results will be tested using regression analysis to establish the significance of the factors identified in this section. Table 15 shows the rotated factor loadings in respect of the tested constructs.

Table 15. Rotated Factor Loading

	Factor					
Renamed	**1 = Attitude**	**2 = Environment**	**3 = Training**	**4 = Habit**	**5 = Governance**	**6 = Knowledge**
ATT1	.819					
ATT2	.818					
ATT3	.752					
ATT4	.723					
ATT5	.693					
ATT6	.612					
ATT7	.606					
ATT8	.514					
ATT9	.501					
ATT10	.466					
ATT11	.464					
ATT12	.410					
ENV1		.869				
ENV2		.796				
ENV3		.779				
ENV4		.613				

ENV5		.603				
ENV6		.460				
TRAN1			.851			
TRAN2			.801			
TRAN3			.644			
TRAN4			.520	-.432		
TRAN5			.405			
TRAN6			.400			
HAB1				.679		
HAB2				.551		
HAB3				-.536		
HAB4				.535		
HAB5				-.405		
GOV					.626	
GOV					.601	
GOV					.534	
GOV					.411	
KNOW1						.560
KNOW2						.509
KNOW3						.505
KNOW4						.402

The table indicates that a total of 37 items were grouped into six factors. Prior to the factor analysis, each of the items in the questionnaire was assigned a unique number. These numbers may be found in Table 15. After due consideration by the researcher, the six factors were classified as individual and organisational factors, according to the items that were loaded in each of the factors. A theoretical research proposition was created under each proposition. The individual and organisational factors were each classified as indicated in Table 16.

Table 16. Individual and Organisational Factor Groupings

Individual Factors	Organisational Factors
Attitude	Training
Habit	Environment
Knowledge	Governance

The next section discusses the reliability of the measuring instrument.

8.8 Reliability

Reliability addresses the dependability or repeatability of scores, which will be discussed in detail in section 8.5.3. Collis and Hussey (2013) view reliability as the consistency and accuracy with which a measure assesses a particular variable. They further argue that a measuring instrument is considered to be reliable when it is applied multiple times and consistently yields the same result (Collis & Hussey, 2013). Various authors recommend different reliability levels of the Cronbach's alpha coefficient. Zikmund (2012) indicates that good reliability is obtained with coefficients above 0.70, whilst Pallant (2011) recommends a reliability of 0.70 as being extensive and a reliability of 0.80 as exemplary. The higher the reliability coefficient the more reliable the factor. Pallant (2011) argues that values of 0.70 and above represent a good level of reliability, whereas values between 0.50 and 0.69 are considered to have an acceptable level of reliability.

8.9 Validity

In research, validity addresses whether an instrument or test actually measures what it is intended to measure (Tsoukas, 1989). According to Adams and Lawrence (2015), validity refers to the accuracy of the measurement instrument by evaluating how it gauges a given variable and the extent to which it enables the researcher to make assumptions which are based on the findings. Marczyk, DeMatteo, and Festinger (2010) believe that validity also relates to the research methodology, since the aim of validity is to increase the precision of research findings by eliminating confounding variables. They also believe that when the validity increases, the credibility of the findings correspondingly increase (Marczyk et al., 2005). The validity of the measuring instrument can also be categorised as internal and external validity (Copeland-Linder, 2009).

- **Internal validity.** This refers to the soundness of the components of a measure. Researchers use internal validity when exploring underlying relationships, which implies that internal validity directs the magnitude to which changes in one variable are caused by changes in another variable (Adams & Lawrence, 2015). Internal validity is often used by researchers when investigating causal relationships, which indicate the extent to which changes to one variable are caused by changes in another.
- **External validity.** Refers to the extent to which the results can be applied to the wider population.

According to Rees (2011), several basic approaches exist for researchers to test either internal or external validity. In this study, the following approaches will be briefly examined in no particular order of significance to bring out the application and significance of results:

i. Construct validity
ii. Content validity
iii. Criterion validity
iv. Face validity

Table 17 discusses the four approaches and what they measure.

Table 17. Four Basic Approaches to Validity

Construct Validity	Content Validity	Criterion Validity	Face Validity
Indicates how well the test measures the theoretical construct it was intended to measure. In order for researchers to warrant the validity of a construct, it is essential that they clearly define the construct, as well as hypothesise on its relationship with other variables.	The extent to which the items in the scale are representative of the theoretical content of the construct being measured. In other words, content validity ensures that the measure captures the full meaning of the concept under investigation.	The degree to which the measurement correlates with an external criterion or another instrument or test that is considered valid. It examines the correlation between two or more tests that appear to be similar. Thus, it only specifies whether or not it is related or unrelated to different tests.	The extent to which a measuring instrument measures what it was supposed to measure. Face validity is often used in quantitative research to ensure that the measuring instrument satisfactorily covers the particular topic in the study. Furthermore, face validity is a subjective assessment of the operationalisation of a concept.

For the purposes of this study, a cut-off point of 0.50 was chosen as the acceptable baseline measure of reliability. Watson and Flamez (2015) suggest that the validity of constructs is often measured using factor analysis. This is used to indicate how well items statistically group together, thereby specifying similarity and measuring a shared construct. In research there are three major ways in which factor analysis can be applied (Williams, Onsman, & Brown, 2012):

i. Providing construct validity. Factor analysis is used to provide construct validity to measuring scales during the research analysis process.

ii. Factor reduction. Reduces a large number of variables into a smaller set of factors with a minimum loss of information through data reduction.

iii. Dimension establishment. Establishes fundamental dimensions between measured variables and suppressed constructs, enabling the realisation of theory.

In addition to these tests, Williams, Onsman, and Brown (2010) explain that researchers use factor analysis to analyse interrelationships among a large number of variables. In this study, factor analysis was used to explore and check the relationships between the factors for the BISB obtained from the literature study. These factors were classified as individual (attitude, habit and knowledge) and organisational (training, macro environment and governance) factors.

The next section discusses the reliability and validity of ordinal scales which are made up of the constructs obtained from the literature review. The results also contain the results of the factor analysis leading to the creation of propositions used as the basis for formulating the research model. The six tables in section 8.5.3 each contain the results of the validity, reliability and factor analysis and are presented individually for each construct. These constructs are also classified as individual and organisational factors as previously discussed in Chapter 7.

8.10 Results of the Reliability, Validity and Factor Analysis

Reliability shadows validity and if research findings are valid, they are consequently regarded as reliable (Bayens & Roberson, 2011). However, research findings that are reliable are not necessarily valid. As discussed previously, six factors were identified in respect of the variables that form the baseline for building a BISB for the unintended administrator. These six factors will be discussed individually in the next section. Each factor also indicates the Cronbach's alpha coefficient values, eigenvalues, factor loading, item to total correlation and the Cronbach's alpha values after deletion. The factors were classified into individual and organisational factors.

8.10.1.1 Individual Factor Analysis

For this study, the individual factors for building a BISB revolved around the employee. The views on ISC from Schlienger and Teufel (2003) as well as Da Veiga and Eloff (2010) emphasise the employees' contribution in developing an ISC. Therefore, it can be concluded that the solution to the security challenges that BYOD poses should start at the employee level. From the literature study, the three major individual factors of attitude, knowledge and habit were identified to be key in building a BISB. The next section discusses these individual factors in detail. Propositions were formulated resulting from inductive reasoning guided by findings reported in the information security literature. These propositions were presented throughout the literature review and discussed in Chapter 8. The empirical analysis enabled the evaluation of these propositions through a case study of a commercial bank in Zimbabwe. The findings of these evaluations are discussed in the methodology section that follows.

i. The attitude factor

The attitude factor is one of the three individual factors identified during the literature survey. Attitude is defined as what people think (Allam et al., 2014; Kruger & Kearney, 2006). Van Niekerk and Von Solms (2010) believe that attitude determines the employees' ISC. An ISC consists of employees' attitudes and beliefs regarding information security, knowledge of the organisation's information security policy, as well as compliancy requirements (Da Veiga & Martins, 2014). Chen et al. (2015) believe that ISC is an assemblage of shared security values, beliefs and assumptions about information security in the organisation and can lead to unconscious and continuous habits that form the behavioural intention toward ISC. Table 18 contains test results conducted on the attitude factor.

Table 18. The Attitude Factor

Total Cronbach's Alpha= 0.719

Original Values	Renamed Values	Item	Factor Loading	Item Total Correlation	Cronbach's Alpha after Del.
7. Attitude	ATT1		.819	.746	.725
6. Attitude	ATT2		.818	.757	.723
1. Attitude	ATT3		.752	-.218	.837
1.Knowledge	ATT4		.723	.445	.759
2.Attitude	ATT5		.693	.553	.749
9.Attitude	ATT6		.612	.462	.758
6.Knowledge	ATT7		.606	.647	.733
4.Attitude	ATT8		.514	.297	.777

7.Environment	ATT10	.501	.426	.762
4.Knowledge	ATT11	.466	.477	.756
2.Knowledge	ATT12	.464	.385	.766
3.Knowledge	ATT13	.41	.746	.725

The original questionnaire used nine variables to test attitude (1. Attitude to 9. Attitude) but only six variables (7. Attitude, 6. Attitude, 1. Attitude, 2. Attitude, 9. Attitude and 4. Attitude) loaded from the original nine variables. These six factors represented factor reliably as they were all above the 0.300 cut-off. Additional variables (1. Knowledge, 6. Knowledge 7. Environment, 4. Knowledge, 2. Knowledge and 3. Knowledge) loaded on the attitude factor and were renamed ATT4, ATT7, ATT9, ATT10, ATT11 and ATT12 respectively. It is apparent from Table 18 that the attitude factor had a Cronbach's alpha coefficient of 0.719 and was therefore considered a reliable measuring instrument for the factor.

ii. The habit factor

Habit is defined as a routinised form of past behaviour (Vance et al., 2012), or alternatively as unconscious or automatic behaviour (Pahnila et al., 2007). Chen et al. (2013) argue that banking organisations should consider employees' habits when dealing with BYOD information security. Employees develop routines in dealing with information assets that collectively have an influence on habitual perceptions which inform the way the organisation's ISC can be improved and built. With BYOD this is even more important as employees will also develop habits or routines on their private devices at home, which will translate to workplace practice. How employees secure their private phones in regard to physical access or authorisation to access the phone at home is unlikely to change when they enter the workplace.

Table 19. Reliability and Validity of Habit as a Scale

Cronbach’s Alpha = 0.390

Original Values	Renamed Values	Item	Factor Loading	Item Total Correlation	Cronbach’s Alpha after Del.
5. Habit	HAB1		.679	.277	.202
6.Habit	HAB2		.551	.318	.267
3. Training	HAB3		-.536	.035	.474

Habitual behaviour explains the ISC of individuals in any banking organisation. Table 19 contains the statistical inference carried out on employee habit as a factor for building a BISB. Of the six habit variables that were identified from the literature review, only two (5. Habit and 6. Habit) loaded during the factor loading. The two variables were renamed as HAB1 and HAB2 respectively. Another variable, 3. Training, loaded showing a negative loading, suggesting that it does not have a positive association with the behavioural intent and attitude construct. From the statistics it can also be seen that habit has a Cronbach’s alpha coefficient of 0.390, showing that this scale provides insufficient evidence of validity. Following the assertion by Bayens and Roberson (2011) that reliability shadows validity, this study still deems habit to be a reliable trait based on the overwhelming findings of the literature review as discussed in section 7.3.2 of Chapter 7.

iii. The knowledge factor

Knowledge underpins the success of knowledge management initiatives within an organisation and has been recognised as a vital pursuit for organisational transformation and success in implementing new solutions and standards within the business (Ahmed et al., 2011). The discussion relating to the model description in Chapter 7 pointed out that the BISB requires employees to be knowledgeable about the devices that they operate. In order for the BISB to be developed, there is a need for organisations (banks in this context) to invest in employee training regarding the consequences of not properly managing information security on their devices. Notably, an investment in the knowledge and training on the BYOD information security will encourage the right attitude and behaviour from employees towards information security.

Table 20. Reliability and Validity of Knowledge as a Scale

Cronbach's Alpha = 0.320

Original Values	Renamed Values	Item	Factor Loading	Item Total Correlation	Cronbach's Alpha after Del.
1.Habit	KNOW1		.560	.219	.186
5.Governance	KNOW2		.509	.189	.260
2.Habit	KNOW3		.505	.180	.244
8.Attitude	KNOW4		.402	.108	.343

Knowledge of the information security risks makes it easy for banking organisations to implement attendant information security policies and encourage the sharing of best practices. Van Niekerk and Von Solms (2010) argue that employees' lack of information security knowledge is detrimental to the organisation, as such organisations have to invest in employee information security knowledge. From Table 20 it is evident that items KNO1 to KNO6 intended to measure employee knowledge on the ISC aspects around the BYOD did not load. The knowledge construct did not load as expected although the item loadings KNOW1 to KNOW4 shown in Table 20 were from other constructs. This had a Cronbach's alpha of 0.320 which was deemed insufficient for this study; nevertheless it was still deemed reliable for the model as, according to Bayens and Roberson (2011), reliability shadows validity. In this study, knowledge refers to employee knowledge on BYOD information security and this construct will remain valid based on the findings of the literature study. The justification for retaining this construct will be explored in Chapter 9. Additional tests were conducted on these factors to establish the level of participation by the three individual factors in improving an ISC for the BYOD unintended administrator.

8.10.1.2 Organisational Factor Analysis

Organisational traits also play a central role in formulating a BISB. Organisational factors include training, the environment and governance, which were identified as being the key organisational components of employee behavioural intention formulation (Gordon, 1991). The next section addresses the statistical analysis carried out and reports the findings, which will later be used for the evaluation included in Chapter 9.

iv. Training

Information security training differs from awareness (Lim et al., 2010). Training is associated with examination and continuous assessment, which is tends to be formal and is confined to classrooms, whereas awareness is more relaxed, very informational and less controlled. Training teaches employees to be conscious about the ISC in an organisation. Further, organisations may not achieve high levels of ISC if training is low and not an integral part of the employees' day-to-day operations (Lim et al., 2010). Table 21 contains the results from the statistical tests conducted on training as a construct for the model.

Table 21. Reliability and Validity of Training as a Scale

Cronbach's Alpha: 0.720

Original Values	Renamed Values	Factor Loading	Item Total Correlation	Cronbach's Alpha after Del.
1.Training	TRAN1	.851	.531	.662
2.Training	TRAN2	.801	.655	.633
4.Training	TRAN3	.644	.357	.719
5.Training	TRAN4	.520	.633	.641
1.Governance	TRAN5	.405	.333	.731
5.Knowledge	TRAN6	.400	.373	.705

The literature study initially identified five variables as the ones to identify the training attributes. However, all other variables from the factor loadings loaded reliably except 3. Training. Two additional factors were loaded as follows:

- **1.Governance** – *There is need for the regulator to examine the implementation of and to have oversight over BYOD in the banking industry.*
- **5. Knowledge** – *Technological innovation must be organised as part of the bank's objectives in order for BYOD to be successfully ingrained into company culture.*

A total of six variables were loaded and renamed TRAN1 to TRAN6, as shown in Table 21. After renaming, the factors were retested and the recalculated Cronbach's alpha coefficient of 0.720 was deemed sufficient to confirm the results as valid. The next section will discuss the environment as a factor for building the BISB.

v. Environment

ISC is defined as the way information security is managed in any given environment. The highly dynamic banking environment is characterised by complex competitive practices where an employee finds derivative values that correspond to institutionalising the means by which the organisation conducts its business. Table 22 contains the validity and reliability of the results of the environment as a factor.

Table 22. Reliability and Validity of Macro Environment as a Scale

Cronbach's Alpha: 0. 800

Original Values	Renamed Values	Factor Loading	Item Total Correlation	Cronbach's Alpha after Del.
3.Environment	ENV1	.869	.682	.739
5.Environment	ENV 2	.796	.609	.758
4.Environment	ENV3	.779	.605	.758
6.Environment	ENV 4	.613	.447	.792

2.Environment	ENV5	.603	.532	.775
1.Environment	ENV6	.460	.476	.791

Seven variables were used for the data collection, and were then subjected to factor analysis. Six of the seven variables identified loaded successfully and were renamed as ENV1 to ENV6, as shown on Table 21. The factor variables loaded with a Cronbach's alpha coefficient of 0.800, which was deemed exceptional for the tests.

vi. Governance

ISC in the banking sector is a prerequisite for good governance and the application of an effective regulatory framework. This is supported by Vignesh and Asha (2015) who further caution that there is an urgent need for organisations, including banks, to update their information security governance policies to deal with the challenges that come with BYOD. In the context of BYOD for banks, a good governance system will improve information security, thereby forming an ISC for the BYOD unintended administrator. The results from the statistical tests conducted on governance as a trait influencing the BYOD behavioural intention to observe and implement security will be presented.

Table 23: Reliability of Governance as a Scale

Cronbach's Alpha: 0.600

Original Values	Renamed Values	item	Factor Loading	Item Total Correlation	Cronbach's Alpha after Del.
4.Habit	GOV1		.626	.394	.433
5.Attitude	GOV2		.601	.309	.506
4.Governance	GOV3		.534	.331	.491
2.Governance	GOV4		.411	.327	.493

8.11 Linking Constructs with Questionnaire Item Variables

The findings to be analysed in this section emanated from the survey results. The survey questions were subdivided into eight categories with the first category collecting demographic data on the employees. The other categories sought to measure the BISB constructs, namely, knowledge, attitude, habit, training, environment, governance and behavioural intention. Table 24 contains the new factors and categories that were linked following the confirmatory factor analysis.

Table 24. New Factors and Categories Indicated after Factor Analysis

Old Number	**New Number**	Item	**1 = Attitude**	**2 = Environment**	**3 = Training**	**4 = Habit**	**5 = Governance**	**6 = Knowledge**
7. Attitude	ATT1	I believe allowing employees to bring their own devices will create a more conducive working environment.	0.819					
6. Attitude	ATT2	I believe that allowing bank employees to bring and use personal devices in the workplace is more beneficial than it is detrimental to their productivity.	0.818					
1.Attitude	ATT3	I am willing to use my personal devices such as smart phone and tablet to conduct the bank's business.	0.752					

1.Knowledge	ATT4	Using a personal device at work would allow me access to all the information I require in order to perform my job satisfactorily.	0.723					
2.Attitude	ATT5	I feel that using my own devices in the workplace compromises my privacy.	0.693					
9.Attitude	ATT6	I am more comfortable in an environment where I am allowed to access some information such as email from a personal device than where I am not.	0.612					
6.Knowledge	ATT7	I think that the nature of my industry is such that the information is too sensitive to allow employees to bring and use their own devices for company business.	0.606					
4.Attitude	ATT8	Being cognisant of the sensitive nature of a bank’s information and systems, I believe that if managed well, the advantages of BYOD outweigh the risks in today’s modern technological era.	0.514					

7.Environment	ATT9	Using my personal device for work will not create a risk of sensitive information leaking to outsiders.	0.501						
4.Knowledge	ATT10	Banks that allow employees to bring their own devices are more Information Security conscious than those that do not.	0.466						
2.Knowledge	ATT11	Using personal devices to perform my tasks at work will not affect the quality of my work or how I interact with customers or colleagues.	0.464						
3.Knowledge	ATT12	There is a growing demand from employees for the use of personal devices in the banking environment to allow unmonitored access to information and systems.	0.41						
3.Environment	ENV1	The organisational culture at my place of work is not prohibitive to new technological trends such as BYOD.		0.869					

5.Environment	ENV2	My company's information security policy is supportive of BYOD.		0.796					
4.Environment	ENV3	My superiors are comfortable enough with technology to appreciate the benefits of BYOD?		0.779					
6.Environment	ENV4	The information security culture in my organisation is robust enough to enable BYOD to be implemented successfully without infringing on information security policy.		0.613					
2.Environment	ENV5	The technologies and applications I use at work are compatible with my personal devices.		0.603					
1.Environment	ENV6	The environment at my workplace is conducive to bring and use my personal devices (considering such things as internet connectivity and accessing networked resources).		0.46					
2.Trainning	TRAN1	There is need for education in order for employees to understand information security for the			0.851				

		successful implementation of BYOD within my organisation.						
5.Trainning	TRAN2	I could benefit from additional training on information security if my organisation wants to adopt BYOD.			0.801			
1.Trainning	TRAN3	I believe that training is the best way to communicate information security tenets of BYOD to ensure that they are understood and accepted as opposed to using fines, threat of punishment or other coercive methods.			0.644			
4.Trainning	TRAN4	I need to be taught how to access organisational resources from BYOD devices such as email and Customer Relationship Management (CRM) systems even where I am already familiar with these systems/resources in the work environment.			0.52			
1.Governance	TRAN 5	There is need for the regulator to examine the			0.405			

		implementation of and to have oversight over BYOD in the banking industry.						
5.Knowledge	TRAN6	Technological innovation must be in organisational into the bank's objectives in order for BYOD to be successfully ingrained into company culture.			0.4			
5.Habit	HAB1	I have received some form of training around information security from my employer.				0.679		
6.Habit	HAB2	If you answered yes to question 23 above, did that training involve aspects of information security around BYOD?				0.551		
3.Attitude	HAB3	I will only use my personal devices for work related business where there is a reimbursement policy.				-0.536		
3.Trainning	HAB4	I do not fully understand data ownership policies as defined by my bank such as distinctions between organisational and personal email, social				0.535		

		network access and account ownership and business vs. personal contacts and need to be trained in these aspects.						
3.Governance	HAB5	Accountability for the information security around BYOD must lie with the Risk department and not the IT department for BYOD to be managed successfully.				-0.405		
4.Habit	GOV	If my personal devices are stolen, I have contingency plans in place to ensure that my data does not fall into the wrong hands such as encryption, remote erase or remote disable.					0.626	
5.Attitude	GOV	I believe that personal devices are being optimally managed within my bank in order to maximise their benefits while mitigating the information security risks? If not, please give reasons why below.					0.601	
4.Governance	GOV	Legislation around data					0.534	

		protection in the finance industry in Zimbabwe is robust enough to mitigate the new risks introduced by BYOD.						
2.Governance	GOV	Information security policy around BYOD is best governed by putting responsibility in the hands of the employees and only establishing controls for management.					0.411	
1.Habit	KNOW1	My personal devices are used by family, friends and colleagues when I am at home.						0.56
5.Governance	KNOW2	The Data Protection Bill that supports privacy on one’s mobile device can be a hindrance to the successful implementation of BYOD in Zimbabwe.						0.509
2.Habit	KNOW3	Personal and organisational data such as documents and contacts are stored together (are allowed to mix) on my personal devices that I use for work.						0.505

8.Attitude	KNOW 4	In light of the nature of my work and industry, the organisation should be able to monitor what I do on my personal device while in the work environment.						0.402

During the factor loading, variables loaded onto other factors besides the initial factors that they were placed under. Table 24 shows the renamed factors and the loading results that were used for this data analysis. The next section contains the correlations as well as the multiple regression analysis of the constructs, followed by an evaluation of the research propositions which were formulated from the model constructs.

8.12 Correlations

Multicollinearity of relationships and the strength of the direction of the relationships that exist between the variables in this research were measured by correlation. Correlation coefficients give an indication of whether the relationship is positive (changes to constructs increase or decrease in the same direction) or negative (constructs respond in opposite directions). Pearson's correlation coefficient was used to investigate the relationship between the constructs of the BISB model introduced in Chapter 7. The Pearson correlation coefficient (r) ranges from –1 to +1, with the sign in front indicating whether there is a positive (as one variable increases, so too does the other) or negative correlation. The size of the absolute value provides an indication of the strength of the positive or negative relationship (Pallant, 2011). Pearson correlation was used because the variables were suitably centred and normally distributed (Neuman, 1997). The relationships are evaluated using Cohen's criteria (Salkind, 2010).

- 0.1– small correlations
- 0.3 – moderate correlations
- 0.5 – large correlations
- 0.8 – extremely large correlations

Table 25. Correlation Matrix

Scale	BI	ATT	KNO	HAB	ENV	GOV	TRA
Behavioural Intention (BI)	-	0.317**	0.108	-0.59	0.262**	0.327**	0.270**
Attitude (ATT)		-	0.108	-0.59	0.262**	0.327**	0.270**
Knowledge(KNO)			-	-0.138	0.175*	0.041	0.189*
Habit (HAB)				-	0.045	0.185*	0.246**
Environment (ENV)					-	0.350**	0.376**
Governance (GOV)						-	0.244**
Training (TRA)							-

***. Correlation is significant at the 0.01 level (2-tailed).*

**. Correlation is significant at the 0.05 level (2-tailed).*

A perfect positive linear relationship or correlations between the variables is shown by a Pearson correlation of +1 point, while a Pearson value of 0 indicates an uncorrelated relationship between the variables. From the results contained in Table 25, the behavioural intention is positively related to five of the six model constructs, with the strongest positive relationship being with attitude. There is an inverse correlation between habit and behavioural intention. The correlation results contained in Table 25 will be used to evaluate the propositions. The next section discusses the regression analysis between the variables which will be used in the evaluation of the model propositions.

8.13 Multiple Regression Analysis

Multiple regression describes how much of the variance in dependent variables can be explained by the independent variables. It also indicates the relative contribution of each independent variable. Tests determine the statistical significance of the results in terms of both the model itself and the individual independent variables.

Table 26. Regression Analysis Summary

DEPENDENT VARIABLE	INDEPENDENT VARIABLE	COEFFICIENT	BETA	R^2	F	SIG
BEHAVIOURAL INTENTION	Attitude	0.47	0.123	0.321	9.395	0.142
	Knowledge	-0.46	0.630			0.630
	Habit	-0.77	-0.059			0.472
	Environment	0.086	0.127			0.143
	Governance	0.201	0.176			0.041
	Training	0.434	0.381			0.000

Table 26 presents a summary of the results of the multiple regression analysis and the variance analysis for the dependent variables. Regression analysis was used to test the relationships between the dependent variable and the independent variables. A significance level of $p < 0.05$ was chosen for this analysis and the criteria for multicollinearity were set at a tolerance value of more than 0.25 and a VIF value below 4 (Marczyk et al., 2010). Although an analysis was carried out to ascertain whether the data met the assumption of collinearity, it should be noted that multicollinearity was not a concern in this research project. Detailed results of the regression test are contained in Appendix 5.

From the output presented in Table 26 it can be concluded that behavioural intention depends on the individual and organisational traits that collectively explain 32.1% ($R^2 = 0.321$) of the total output control. The beta weight of habit (Habit =-0.059 at $p > 0.05$) showed a negative effect on the dependent variable. The other predictive variables of attitude (0.123), knowledge (0.630), environment (0.127), governance (0.176) and training (0.381) clearly impacted on the dependent variable. Attitude showed the weakest relationship while knowledge showed the strongest relationship (refer to Appendix 4). The analysis of variance statistically showed a fit for the model, since the significance value, $p < 0.01$, applied to the majority of variables, that is, attitude, environment, training and governance. Whilst the other two variables (habit and knowledge) showed positive results which were not necessarily significant at $p < 0.01$, the resultant statistics combined with the supporting evidence from the literature review confirm their relevancy in explaining behavioural intention. The next section contains the evaluation of the theoretical propositions discussed in Chapter 7. Results from the correlations and the multiple regression analysis will be used to analyse the findings on the statistical propositions.

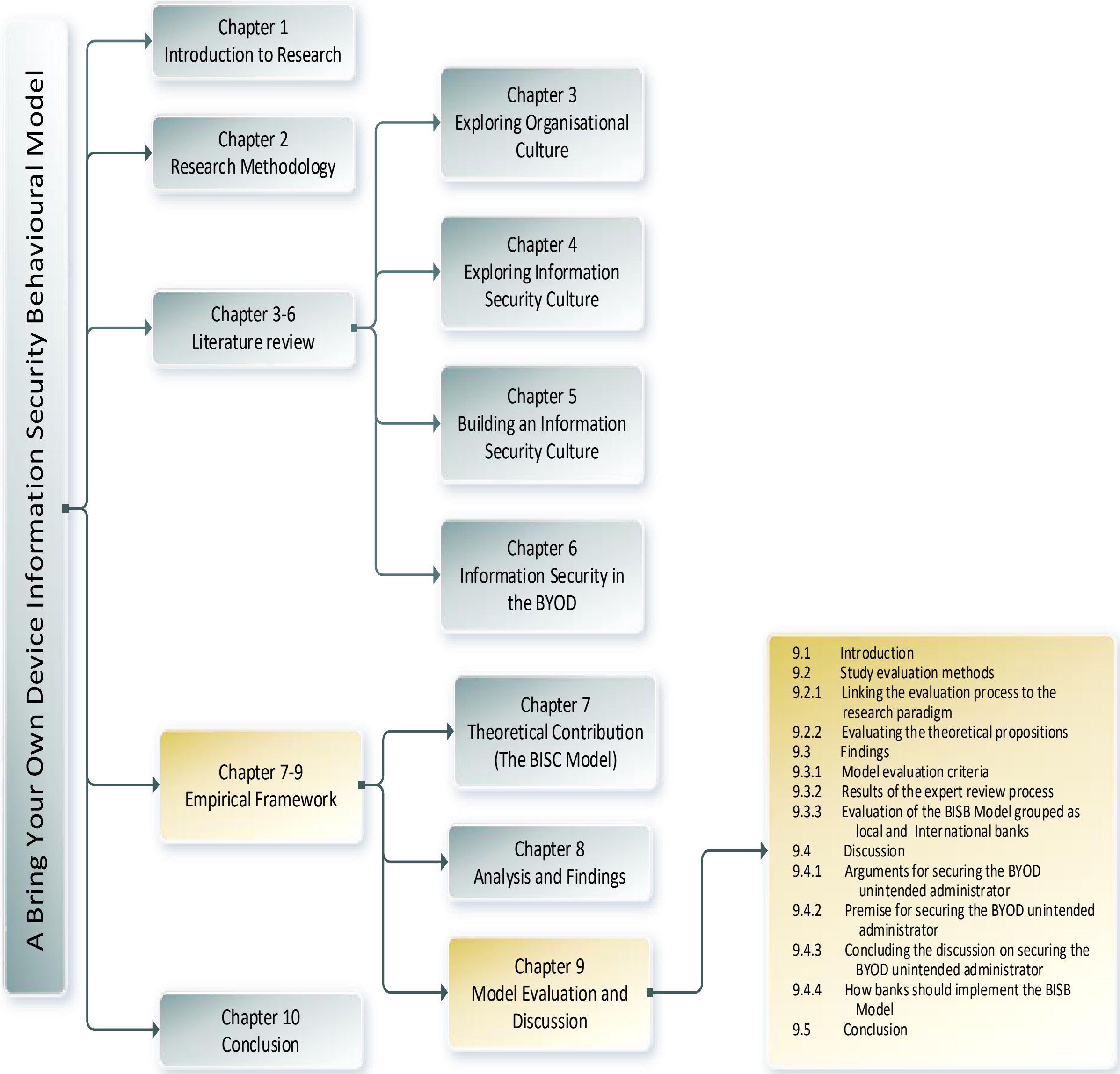
8.14 Conclusion

From the statistical analysis carried in this chapter, it can be observed that valid statistical derivations were made from the survey results. A pilot study was conducted to refine the questionnaire by clarifying ambiguities and testing any lack of clarity in the questions for the audience. The participants for the survey were employees from a commercial bank in Zimbabwe. A response rate of approximately 90% was achieved. The largest number of participants were found to be in the 30–40 age group and 60% of the respondents were males.

The research instrument was made up of questions directed at extracting responses for testing the six constructs for the BISB model identified from the literature review. The reliability of the research instrument was tested using the Cronbach’s alpha coefficient followed by a measurement of the internal and external validity. A factor analysis of the variables ensued and this was followed by a correlation analysis and a multiple regression analysis of the model constructs. Finally, a statistical correlation analysis was conducted followed by a multiple regression analysis of the variables.

Chapter 9 : Model Evaluation and Discussion

"Good critical writing is measured by the perception and evaluation of the subject; bad critical writing by the necessity of maintaining the professional standing of the critic." Raymond Chandler


A Bring Your Own Device Information Security Behavioural Model
Chapter 1
Introduction to Research
Chapter 2
Research Methodology
Chapter 3-6
Literature review
Chapter 3
Exploring Organisational Culture
Chapter 4
Exploring Information Security Culture
Chapter 5
Building an Information Security Culture
Chapter 6
Information Security in the BYOD
Chapter 7-9
Empirical Framework
Chapter 7
Theoretical Contribution (The BISC Model)
Chapter 8
Analysis and Findings
Chapter 9
Model Evaluation and Discussion
Chapter 10
Conclusion
9.1 Introduction
9.2 Study evaluation methods
9.2.1 Linking the evaluation process to the research paradigm
9.2.2 Evaluating the theoretical propositions
9.3 Findings
9.3.1 Model evaluation criteria
9.3.2 Results of the expert review process
9.3.3 Evaluation of the BISB Model grouped as local and International banks
9.4 Discussion
9.4.1 Arguments for securing the BYOD unintended administrator
9.4.2 Premise for securing the BYOD unintended administrator
9.4.3 Concluding the discussion on securing the BYOD unintended administrator
9.4.4 How banks should implement the BISB Model
9.5 Conclusion

9.1 Introduction

In this chapter, the BISB model discussed in Chapter 7 is explored using the expert review evaluation method. The chapter commences with a high-level discussion of the research evaluation methods followed by linking the evaluation process to the research paradigm. This is followed by an evaluation of the theoretical propositions, and the presentation and analysis of the results of the expert review process conducted. The chapter concludes with a discussion on the contribution that this research makes to the body of knowledge. Saunders et al. (2009) argue that the integrity of research may be considered to be a general evaluative judgement of the extent to which the study contains the truth. Peffers et al. (2012) suggest that research artefacts should be evaluated on the basis of criteria that are informed by the requirements of the context in which they are implemented. The evaluation criteria applied in this study utilise the design science research guidelines which cover pertinent aspects such as completeness, consistency, accuracy, performance, usability, reliability, best fit and many other parameters (Peffers et al., 2012).

Design science was presented in Chapter 2 as the research methodology and design for this study. Guideline number 4 of Hevner's design science guidelines presents research evaluation as one of the critical stages of the research process. It is from this angle that the evaluation of the model will be conducted. The next section will outline in detail the evaluation methods employed in this study by briefly looking at the reliability and validity of the model. This will be followed by the evaluation of the BISB refined model which will be the research artefact for this study. This will then be followed by an examination of the dependent variable of the model. The dependent variable, as indicated in Chapters 1 and 7, is the unintended administrators' behavioural intention to build an ISC. The statement of the problem that this research intends to address is centred on the unintended administrator's total control of their mobile device when connecting to the bank's network. Chapter 7 emphasises the need for a behavioural intention to build an ISC as being the solution to the problem that the unintended administrator poses to the bank's security. The study concludes with a discussion on how banks can implement the BISB model.

9.2 Study Evaluation Methods

Design evaluation is important in ensuring that an artefact has been rigorously evaluated to ensure its utility, eminence and efficacy (Hevner et al., 2004). Hevner and Chatterjee's (2004) seven-point research process satisfies guideline number 3 of the design science guidelines, as discussed in section 2.6 of Chapter 2. Weber (2012) explains that, for a proper assessment to take place, the artefacts can be evaluated as theories with four parts. These four parts are the constructs, the associations, states and the actions taken. These parts are accompanied by four elements, namely, the parsimony level, importance, falsifiability and novelty. Weber's approach was not adopted in this study as it was deemed not to be sufficiently exhaustive for the chosen approach.

Several other methods exist for research evaluation in the literature, including research symposiums, research consortiums, peer feedback, industry expert review, journals, conferences, and many others (Ahmed & Sundaram, 2011). Below is a high-level overview of other existing evaluation methods which were discussed in detail in sections 2.6.3 and 2.11 of Chapter 2. The list is not necessarily exhaustive but it does covers pertinent existing methods and concludes with the method chosen for the evaluation of this study.

- **Research symposiums**. These are conferences or meetings to discuss research with several speakers talking about various research subjects.
- **Research consortiums**. These refer to an association of more than one research organisation with the objective of participating in research targeted at a particular goal.
- **Journal publication.** To be accepted for publication in a journal, a paper on the artefact is evaluated rigorously by the editorial team as well as peers as part of the review process. This method is usually applied when evaluation is conducted in the form of a research paper.
- **Peer reviews**. These are generally conducted by getting feedback from peers. Usually the request is sent anonymously so that the feedback does not become subjective.
- **Expert reviews.** Various subject matter experts are carefully selected and then approached and presented with a detailed overview of the model or study, as discussed in section 2.12 of Chapter 2.

Considering that the BISB model is targeted at making it easier for CIOs and security experts in the bank to manage information security, an expert review of the model was selected as the most appropriate approach for evaluating the model. The review involved CIOs from other banks in Zimbabwe who participated in the evaluation process. The expert review approach was also considered to be an appropriate research evaluation method because industry experts were available to give input; in addition, they are the ones who will implement the BISB model in the event that their banks adopt it.

The next section details the expert review approach that was used in evaluating the BISB model for the unintended administrator.

9.2.1 Linking the Evaluation Process to the Research Paradigm

Hevner’s design science paradigm contains seven stages, which were adapted to explain the entire research process followed in this study (Hevner et al., 2004). In order to place this chapter in context, the seven research guidelines previously discussed in detail in section 2.6 of Chapter 2 will be briefly discussed below. Emphasis was placed on guideline number three, which describes design evaluation. From this paradigm, the evaluation criteria for the BISB model was formulated in line with seven points which were then used as the basis for the evaluation questions.

1. **Guideline 1: Design as an artefact**

This guideline leads to the creation of a research model for building an ISC for the BYOD unintended administrator. This model is evaluated by means of an expert review process in this chapter.

2. **Guideline 2: Problem relevance**

This guideline leads to the answer to the research problem, which is the unintended administrators’ full control of the mobile devices they use in the BYOD. The expert review process followed in this study is used to evaluate the relevance of the problem to be addressed by the BISB model.

3. **Guideline 3: Design evaluation**

The reasons for choosing expert reviews as the approach for this research study are cited in the introduction to this chapter. The BISB model was presented to the CIOs of banks in Zimbabwe through a guided review process, as detailed in section 9.5.1. In view of the fact that information security falls under the CIOs of the various banks, the CIOs were deemed to be the best experts for reviewing this artefact. The results of the evaluation process are presented in section 9.5.2.

4. **Guideline 4: Research contribution**

The creation of a BISB model for the unintended administrator is the contribution for this study. In the literature review, it was noted that little emphasis is placed on the employees’ contribution to securing the BYOD. Consequently, the grouping of the individual and organisational traits, as contributing to securing the BYOD unintended administrator, provides a unique security model which is evaluated in this chapter.

5. **Guideline 5: Research rigour**

Research rigour was assured by applying social science theories. This was backed by a detailed literature study leading to the identification of the gaps that this research contribution intends to fill.

Chapters 3, 4, and 7 cover the research rigour in detail as they address the research process followed, with design science being the paradigm of choice.

6. **Guideline 6: Design as a search problem**

This guideline was satisfied by means of a literature search that culminated in the construction which guided the formulation of the BISB model for the unintended administrator.

7. **Guideline 7: Communication**

This guideline was applied through the communication of results in conference papers as well as in journals. The model was shared with industry experts who are CIOs for banks in Zimbabwe as they participated in the evaluation process.

9.2.2 Evaluating the Theoretical Propositions

In much the same way as research on ISC tends to focus on its inductive mechanisms rather than its implications, the behavioural studies reviewed in this chapter pay little attention to the methodical complexities which prompt certain responses by bank employees. Berg (2004) state that information security research can be qualitative, quantitative or both. However, qualitative research may create a notable disconnect with the quantitative analysis of results. In this regard, Myers and Avison (2002) argue that the motivation for carrying out a qualitative research study stems from the realisation that humans are natural beings, such that qualitative research helps researchers to understand people in their social and cultural context, which is often lost when textual data are quantified. Regardless of this perspective, the findings made in the studies reviewed in Chapter 8 can be used in the review of the six theoretical propositions formulated to evaluate the influence of BISB. The next phase of the statistical analysis involved the evaluation of the propositions formulated in Chapter 7. The results of the statistical analysis conducted in Chapter 8 will be used in the evaluation of the propositions based on the results relating to reliability, correlation analysis and multiple regression analysis.

Table 27. Evaluation of Theoretical Propositions

Proposition One	*Employee attitude towards information security is positively associated with the building of an information security culture for the BYOD unintended administrator.*
P1	Based on the statistical computations carried on the model constructs, attitude loaded positively in all the computations. It loaded a Cronbach's alpha coefficient value of 0.719, thus confirming that it is a valid construct for the model. Attitude also showed a strong positive correlation with behavioural intention with a value of 0.317. On the multiple regression analysis which had a R2 value of 0.321 overall, attitude had a beta value of 0.127, which was sufficient to explain that it is a valid construct. In combining the results of these statistical computations, proposition P1 can be confirmed as being positive, indicating that employee attitude is indeed important in building an ISC for the BYOD unintended administrator.

Proposition Two	*The habits of the employee towards information security are positively associated with the building of an information security culture in the BYOD phenomenon.*
P2	Statistical results on the habit construct loaded negatively on all the tests conducted. The Cronbach's alpha coefficient result relating to habit indicated a value of 0.390 which is deemed invalid. The correlation results between habit and the dependent variable of behavioural intention showed a negative value of -0.59, implying that there is an inverse relationship between habit and behavioural intention. The multiple regression computations also loaded a -0.059 beta value, indicating that the relationship is inverse. Of the 32.1% that the constructs explain in the relationship between the dependent and independent variables, it can be concluded that habit did not contribute positively. Based on the arguments above, it can be concluded that habit has an inverse effect on behavioural intention and therefore proposition P2 was not confirmed statistically.

Proposition Three	*Employee knowledge is positively associated with the building of an information security culture in the BYOD phenomenon.*
P3	Knowledge loaded with a Cronbach's alpha coefficient value of 0.320, which is deemed statistically invalid. The results of the correlation computation between knowledge and behavioural intention yielded an insignificant 0.108 value. Statistically, this shows a positive relationship between knowledge and behavioural intention but not significant enough to make the requisite statistical impact. The multiple beta value for regression showed a negative value of -0.46, which indicates that there is an inverse relationship between knowledge and behavioural intention. Therefore, this neither confirms nor invalidates proposition P3 statistically.

Proposition Four	*The training offered to the employee by organisations is positively associated with the building of an information security culture in the BYOD phenomenon.*
P4	The Cronbach's alpha coefficient for training loaded significantly at a value of 0.720, indicating that training positively influences the behavioural intention construct. The Pearson's correlation coefficient (r) between training and behavioural intention loaded with a significant value of 0.270, indicating a strong correlation. The regression coefficient of 0.381 indicated the highest value, thus confirming that proposition P4 is indeed valid.

Proposition. Five	*The environment is positively associated with the building of an information security culture in the BYOD phenomenon.*
P5	The environment as a construct evaluated under proposition P5 loaded positively with a Cronbach's alpha coefficient of 0.800, thus indicating strong validity. The correlation coefficient between environment and behavioural intention loaded positively with 0.262, indicating a strong positive correlation. The regression beta

	value was found to be 0.127. These statistical calculations confirm that proposition P5 is indeed valid.

Proposition	*Governance is positively associated with the building of an information security culture in the BYOD phenomenon.*
P6	The Cronbach's alpha value for governance loaded at 0.600, thus confirming validity, followed by a correlation value of 0.327 and a regression value of 0.176. These all confirmed a positive relationship between behavioural intentions as a dependent variable and governance. These statistics individually confirm proposition P6 and collectively validate the model construct of governance.

The propositions above each contribute to the subjective probability that information security should be treated as a culture when addressing BYOD security. Table 27 below contains a summary of the theoretical proposition statistics that were discussed in detail in Table 26.

Table 28. Evaluation of Research Propositions

Proposition	Cronbach's Alpha	R^2	Beta	Result
P1 (Attitude)	0.719	0.321	0.127	Accepted
P2 (Habit)	0.390	-0.59	-0.059	Rejected
P3 (Knowledge)	0.320	0.108	-0.46	Rejected
P4 (Training)	0.720	0.270	0.381	Accepted
P5 (Environment)	0.800	0.262	0.127	Accepted
P6 (Governance)	0.600	0.327	0.176	Accepted

From the evaluation of the propositions conducted above, propositions P1, P4, P5 and P6 were found to be statistically positive and were accepted to explain the BISB model, as all their statistical measurement showed positive results in explaining the relationships. Propositions P2 and P3 were rejected as they were not statistically explained. Although propositions P2 and P3 were rejected, the results obtained from the literature discussed in section 7.3 of Chapter 7 deemed them sufficient to explain the BISB model and they were therefore retained as constructs of the model. The next section examines the refined BISB model constituting the findings for this study.

9.3 Findings

The constructs obtained from the literature review were subjected to the statistical analysis presented in Chapter 8. The evaluation of the research proposition introduced in Chapter 7 resulted in the final research artefact, which is presented in Figure 39 of this research document. The evaluation of the research proposition revealed that four of the six model constructs statistically explained the model at a level above the acceptable statistical thresholds.

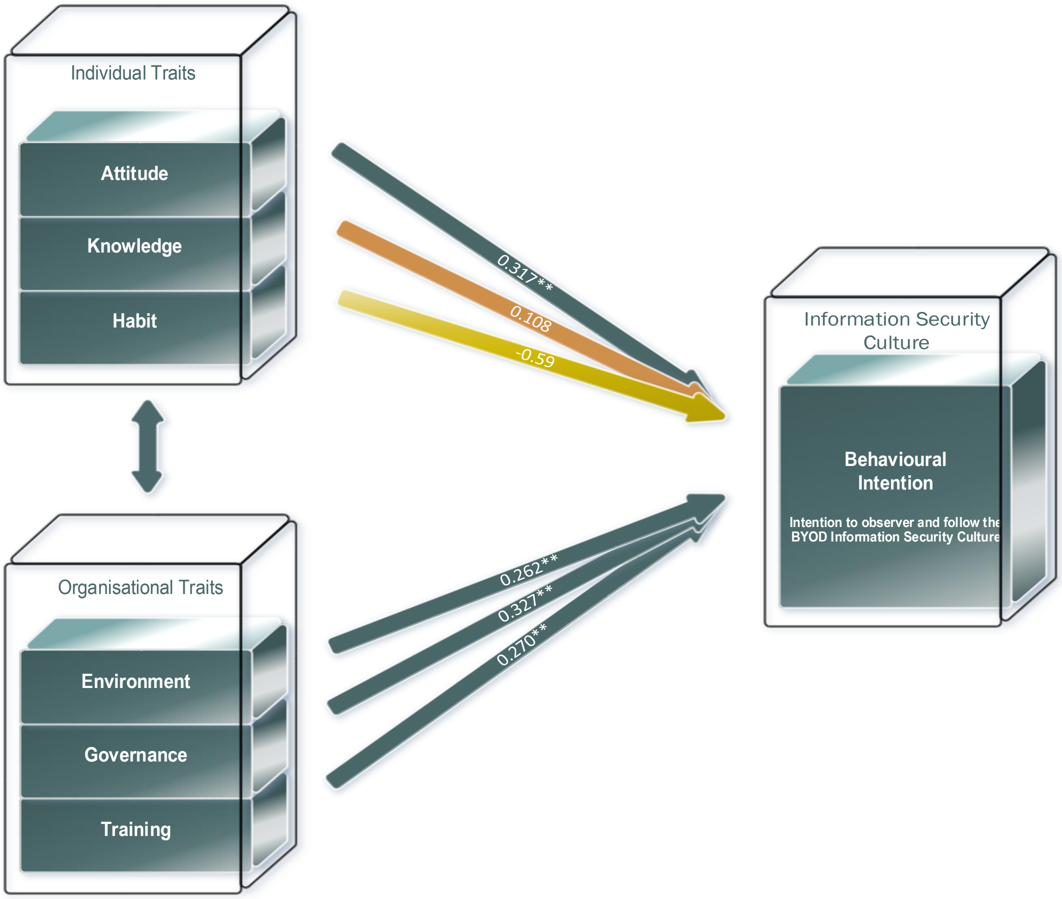


Figure 39. The Refined BISB Model

Attitude, environment, governance and training, as shown in Table 27, all displayed valid Cronbach's alpha, $R^2$and beta values, whereas values related to attitude and knowledge were invalid. Nevertheless, as indicated above, these two constructs were still retained as valid model constructs. The BISB model is designed to qualitatively present the components that are required for building an ISC for the BYOD unintended administrator. As previously discussed, qualitative research helps researchers in understanding people within the social and cultural contexts in which they exist. Quantitative research often fails to account for the social and institutional context that is generally retained when qualitative data are used (Myers & Avison, 2002). All six model constructs were therefore deemed valid in influencing the BISB for the unintended administrator. The next section contains the model evaluation process using the expert review approach. Section 9.5.1 discusses the review of the evaluation criteria followed by the expert review results in section 9.5.2.

9.3.1 Model Evaluation Criteria

A set of fifteen questions were created and presented to the 16 CIOs selected from banks in Zimbabwe. The CIOs all have more than five years' experience working in the Zimbabwe banking sector The questions were designed to evaluate the model against the criteria of completeness, consistency, accuracy, performance, usability, reliability, and best fit. Wahyuni (2012) proposes interpretivist evaluation criteria that evaluate research on line with the five points of trustworthiness, confirmability, dependability, credibility and transferability. Whilst this approach is applicable to this study, the evaluation approach proposed by Hevner and Chatterjee (2004) was deemed more rigorous, relevant and applicable to this study as it covered the following seven criteria:

- **Completeness**. This criterion evaluates to what extent the model covers the problem it is meant to address. The evaluation template used to conduct the expert reviews included two questions to measure the completeness of the artefact in addressing the problem.
- **Consistency**. This criterion evaluates to what extent the model consistently secures the BYOD unintended administrator, considering the fast changing technological landscape.
- **Accuracy.** This criterion addresses the level at which the model tackles the BYOD information security challenges. This also covers how comprehensive the BISB model is in articulating the unintended administrator's security challenges.
- **Performance.** This criterion is viewed as a measure of how the model improves BYOD information security for the unintended administrator. It also evaluates the impact of the BISB model on information security improvement for organisations, which is an ongoing process.

- **Usability.** Usability describes how easily banking organisations apply the BISB model in their environment and whether it fits seamlessly into the banking environment in Zimbabwe.
- **Reliability.** This criterion evaluates the extent to which the BISB model can be depended upon by banks in Zimbabwe to build an ISC for the unintended administrator.
- **Best fit.** This criterion measures how banks can easily fit within the existing banks. Best fit also evaluates the amount of adjustment required in order to make use of the model.

9.3.2 Results of the expert review process

Table 28 shows the evaluation questions and responses recorded during the expert review evaluation process. The responses were grouped into a five-point Likert scale, as presented in the table. As indicated in Chapter 1, it is important to reiterate that there are two kinds of banks in Zimbabwe: local banks, which are wholly owned by Zimbabwean shareholders and have headquarters in Zimbabwe, and foreign-owned banks, whose head office is in a country other than Zimbabwe. The analysis will also factor in the responses from both the locally owned and the international banks.

Table 29. BISB Model Evaluation Criteria

Completeness	***Not exhaustive***	***To a lesser extent***	***Moderately exhaustive***	***To a larger extent***	***Completely Exhaustive***
To what extent are the BISB individual traits exhaustive in covering the employee's contribution to information security in the BYOD?	0	0	4	9	3
To what extent are the BISB organisational traits exhaustive in covering the employee's contribution to information security in the BYOD?	0	0	2	12	2
Consistency	**Completely Disagree**	**Disagree**	**Neither Agree Nor Disagree**	**Agree**	**Completely Agree**
Do you feel that the BISB model will maintain its relevance with the ever-changing security landscape?	0	1	1	8	6

How well structured are the arguments for the BISB model?	0	0	0	14	2
Accuracy	**Very Inaccurately**	**Inaccurately**	**Moderately**	**Fairly accurately**	**Very Accurately**
How accurately do you think the BISB model addresses the challenges of information security around BYOD in Zimbabwe?	0	0	2	8	6
How comprehensive is the BISB model in addressing the factors affecting information security around BYOD?	0	0	0	10	6
Performance	**Extremely unlikely**	**Unlikely**	**Indifferent**	**Likely**	**Extremely likely**
How likely are you to recommend that your organisation adopt the BISB model?	0	0	1	10	4
How likely is your organisation to adopt the BISB model on your recommendation?	0	2	2	10	2
Usability	**Very Inapplicable**	**Inapplicable**	**Moderately applicable**	**Fairly applicable**	**Very applicable**
How applicable is this model to your organisation?	0	0	3	9	4
How adaptable is the BISB model to be applied to the various banks in Zimbabwe?	0	2	1	7	6
How applicable is this model in Zimbabwe's banking environment?	0	0	2	9	5
Reliability	**Completely disagree**	**Mostly disagree**	**Agree on some aspects**	**Mostly in agreement**	**Completely in agreement**
How much of the model are you in agreement with?	0	0	3	11	2

How much of the BISB model is already in practice in your organisation?	1	2	2	10	1
Best Fit	**Does not fit**	**To a lesser extent**	**Indifferent**	**To a larger extent**	**Seamlessly**
To what extent does the BISB model fit in with the existing security culture at your organisation?	1	0	0	13	2
How easily can the BISB model be applied to your organisation?	0	4	0	9	3

Table 28 shows the responses from the expert review process conducted on the BISB model. The seven evaluation points (criteria) presented to the CIOs during the expert review process all obtained positive feedback on the relevance of the BISB model in the various banks in Zimbabwe represented by the CIOs. From Table 28 it can be concluded that the majority of CIOs agreed to a greater extent with the BISB model, as the majority of the responses ranging from “agree” to “strongly agree” were skewed to confirming the relevance of the model. The responses and feedback from the CIOs are portrayed in Figure 40 below as percentages quantifying the degree of relevance to the various banks as a function of the total responses received from the Likert points.

The general trend analysis shows the bank CIOs’ acceptance of the BISB model. Whilst information security is viewed as a preserve of the banks’ IT department, the CIOs showed a general consensus on the need for the departments to take part in information security management in the bank. The results of the seven-point evaluation criteria used for the evaluation process, from consistency to best fit, all strongly suggest the important place that the unintended administrator now holds if organisations are to leverage on BYOD.

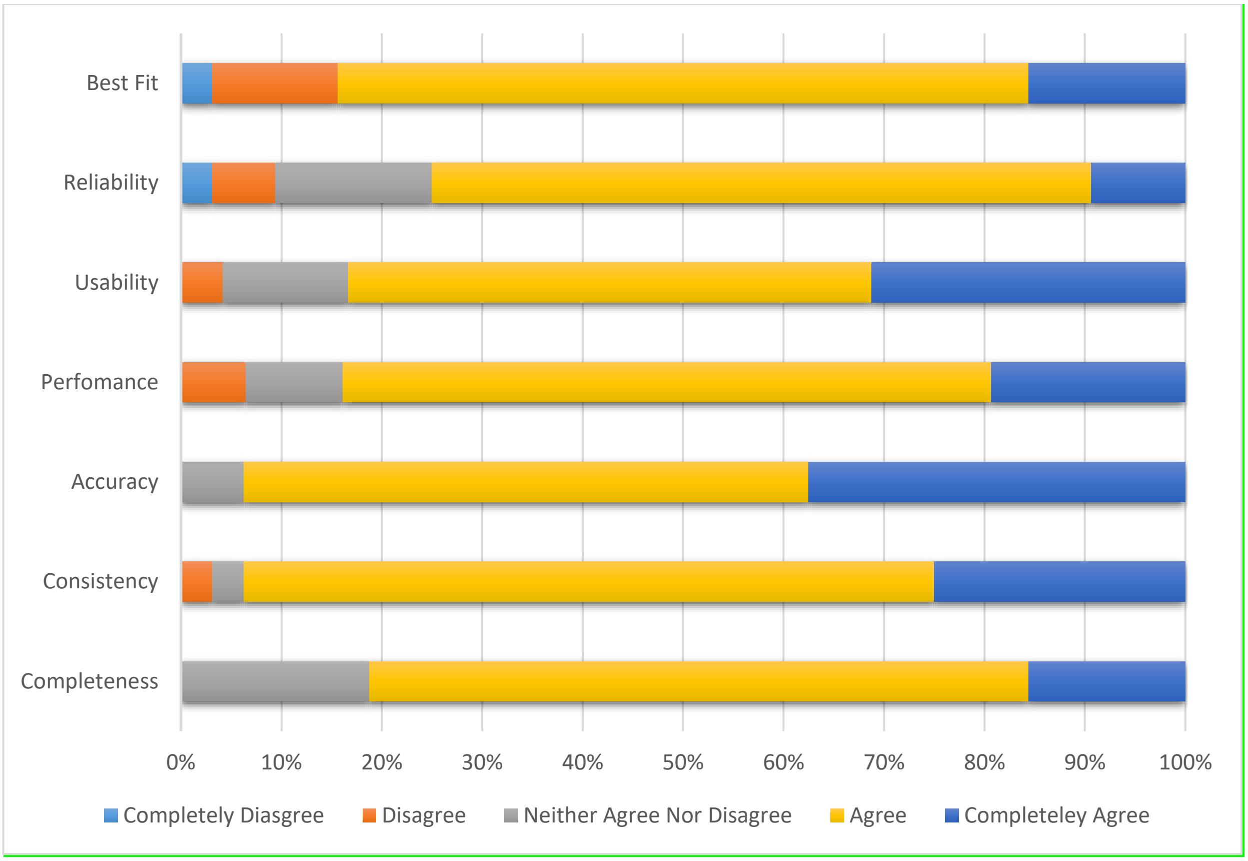


Figure 40. The BISB Evaluation Results

The CIOs generally agreed with the application of the model across all the seven measurement criteria. A considerable number agreed completely that the BISB model satisfies their requirements, with a small number neither agreeing nor disagreeing. Very few to none of the CIOs disagreed with the BISB model. On the measurement criterion, close to 70% of the CIOs agreed that the BISB model is a complete presentation of how the unintended administrator can be secured, while above 15% completely agreed with the model. On consistence, more than 70% agreed followed by above 20% who completely agreed. On the accuracy criterion, in excess of 50% agreed with the model and more than 35% completely agreed. Computations from the performance measurement criterion show above 65% agreed with the BISB model and about 18% completely agreed. On usability as criterion, about 50% were in agreement while about 35% were completely in agreement. Reliability as a criterion displayed agreement of above 65% while 15% completely agreed. On the best fit criterion about 70% were in agreement followed by 15% completely in agreement. Across all seven measurement criteria, a summation of the results from the scale measurement of agree and completely agree found all to be above 50%. This response confirms that there is a general positive evaluation of the BISB model.

The next section is a further analysis and compared the evaluation of the local and foreign-owned banks. It is important to establish the evaluation of the model by these two types of institution to build a strong case for the Zimbabwean context in contradistinction to other countries.

9.3.3 Evaluation of the BISB Model by Local and International Banks

Of the CIOs who participated, six were employed by international banks and ten by local banks. The responses generally portray positive feedback. Whilst the BISB model is premised on the Zimbabwean context, the expert reviews from the CIOs of banks with a foreign head office will act as a yardstick for measuring the applicability of the BISB model to other countries. This is because the model constructs of governance, environment, and training and even the individual model constructs of attitude, habit and knowledge, will most likely produce different results if a survey were conducted in a another country. This analysis will also provide an opportunity for future research work. Figure 41 gives a comparison of the results from the local and international banks.

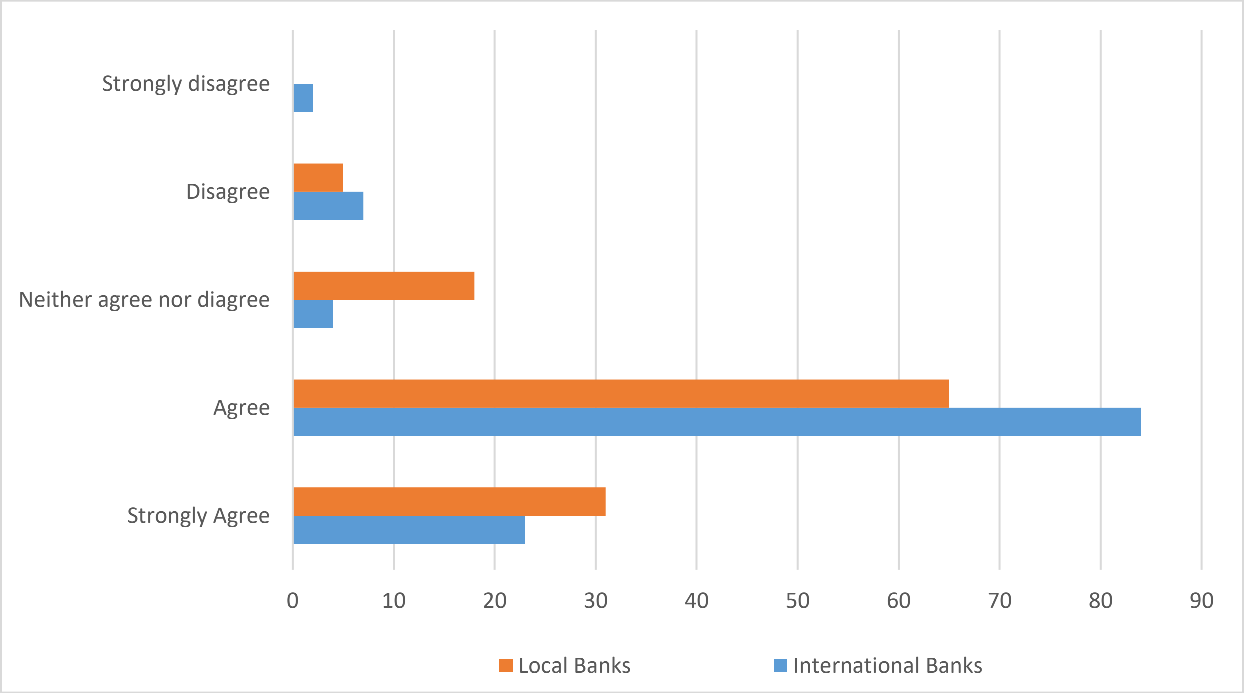


Figure 41. Comparison of International and Local Banks

From Figure 41, it is clear that, on average, international banks agree with the BISB model, as there is a normal distribution of the acceptance by both local and international banks. This confirms that the BISB model can be applied to banks in other countries similar to Zimbabwe with little adjustment. The results of the evaluation of the model propositions and the evaluation of the BISB model by the experts form the basis for the discussion on this study, which will be covered in the next chapter.

9.4 Discussion

This section combines the findings from the literature review with the statistical findings, the evaluation outcomes for the model propositions, as well as the expert review conducted on the model. The discussion section will be structured into three phases. Firstly, the discussion will present the argument for this study which in essence formed the basis for the researcher's attempt to provide reasons for thinking that the research problem is true. Secondly, a premise for the argument for this study will be presented which in effect gives the reasons and statements that support the discussion. Thirdly, the discussion section will contain the conclusion, that is, a summary of what the research argument supported as evidenced by the premise.

9.4.1 Arguments for Securing the BYOD Unintended Administrator

As identified by the literature study presented in Chapters 3 to 6, information security management in banks is an area that has been entirely the preserve of the IT department. Various scholars share the same belief that information security has subsequently moved from the IT department to all employees (Dillon et al., 2015; Eslahi, Naseri, Hashim, Tahir, & Saad, 2015; Kritzinger & Von Solms, 2012).

The advent of BYOD has confirmed this belief and underlines the urgency of absorbing it in the organisational culture (OC). Today, most organisations are grappling with the means by which to secure the unintended administrator who now carries information wherever he or she goes. In the banking sector, the literature review revealed that information security can under no circumstances be compromised (Eschelbeck & Schwartzber, 2012). Banks have also adopted BYOD and most banks have invested heavily in technical solutions to combat the challenges presented by BYOD, yet the challenges persist. The next section therefore presents the premises that qualified the BISB model as a relevant panacea for securing the BYOD unintended administrator.

9.4.2 Premise for Securing the BYOD Unintended Administrator

General systems theory (GST), which was discussed in Chapters 1 and 4, proposes that the elements of a system are interdependent and contribute to the operation of the whole system (Von Bertalanffy, 1972). The various part of the premise, which are in essence the research sub-questions, are combined to formulate the main research question which is answered by the entire research project. The fact that information security is no longer the preserve of the IT department provides the first premise for need to secure the BYOD unintended administrator. This premise is explained by answering the first research sub-question, which seeks to identify what organisations require to build an ISC for the BYOD unintended administrator. The research sub question, as discussed in section 1.5 of Chapter 1, reads "*What is required for organisations to build an information security culture?*". Hu et al. (2012) argue that the security of every organisation is as strong as its weakest link, which in this instance is the unintended administrator.

The second research sub-question, which reads "*How does the BYOD unintended administrator impact the organisational information security culture?*" forms the basis for the second premise. This sub-question attempts to find answers on how the BYOD unintended administrator has affected organisational ISC. The argument for securing the BYOD unintended administrator is the fact that information security has moved from endpoint security (i.e. security within the organisational network boundaries) to the mobile devices that the unintended administrator has total control over. The discussion in Chapters 5 and 6 showed that building an ISC and securing BYOD require concerted efforts by all members of the organisation. It is upon this basis that the third premise for the evaluation process is derived.

Research sub-questions 3 and 4 form the basis for the third premise. The third premise for securing the BYOD is that technical solutions alone do not address the BYOD security challenges. The third research sub-question seeks to explain how an ISC mitigates information security risks as opposed to the technical solutions alone. "The genie for security is now outside the bottle" (Singh & Phil, 2012) and as such the key imperative is that practical means be put in place to secure the unintended administrator. The arguments presented in section 9.4.1 supported by the premise in 9.4.2 culminate in the conclusion discussed in 9.4.3 concerning how the BISB model secures the unintended administrator. The fourth research sub-question on what roles employees play in building a BYOD ISC is addressed by this premise from the perspective that employees constitute the individual traits of the BISB model.

9.4.3 Concluding the Discussion on Securing the BYOD Unintended Administrator

Based on the arguments and premises presented above, it can be inferred that the solution for securing the BYOD unintended administrator lies with the unintended administrator and the organisation. BYOD information security can therefore be viewed as a combination of employees' individual traits and the traits of the organisation in which they work.

As illustrated by the study carried out in the commercial bank in Zimbabwe, the individual and organisational traits that culminated in the BISB model show that the solution does indeed lie within the employees; the attitude they have towards the ISC as well as the knowledge and habits they practise when using their mobile devices can be exploited in building a BISB. However, this would be incomplete if the organisational traits of governance, environment and training given to the employees were not included. It can therefore be concluded that a model that addresses the behavioural intention to observe ISC holds promise for securing banks with regard to BYOD. The results of the statistical analysis and the expert reviews of the model confirm this conclusion.

9.4.4 How Banks Should Implement the BISB Model

As presented in the document, the BISB model is employee centric which gives banks a way of ensuring total buy-in from employees regarding BYOD. Researchers (Brodin, 2016b ;Von Solms, 2001) in the area of information security share the belief that employees play a key role in building an ISC. In the banking environment, information security is a key component of organisational operation. Hence, banks have to incentivise the secure use of the BYOD in the organisations so that they can influence the way the employees use the devices (Anderson & Moore, 2006) . If security behaviours are practised over time, they can become an ISC, which is what the BISB is advocating. The BISB model recommends that for banks to build an ISC for the unintended administrator, they have to explore the three individual traits and three organisational traits, as presented in Chapter 7.

In harnessing the individual and organisational traits when implementing the BISB model, banks can follow various basic steps. The basic steps are explained for each model construct, which if combined will result in the banks enjoying the benefits of using the BISB model. Banks can encourage and build positive employee attitudes towards the BISB by implementing policies that support the use of mobile devices. If they ban such usage, employees will sneak the devices in through what is termed Shadow IT. Because employees will be fearful of being caught they will be likely to be careless with regard to security. Encouraging the use of mobile devices will allow the employee to support the bank’s information security efforts and this buy-in will be a step towards securing the unintended administrator by building the right attitude.

If employees know the consequences of information security breaches, banks can use a certain level of determined knowledge as a benchmark when hiring. Employees may also be exposed to the challenges faced if they do not observe the ISC. From this angle, banks can encourage employees or even organise training on BYOD information security. This should result in knowledgeable employees who will be cautious when using mobile devices in a BYOD environment.

Banks need to encourage good mobile device usage habits by opening their policy framework to encourage buy-in from employees. From the literature review, it was learnt that habits can be formed as a result of the existing controls in the environment. Banks should ensure policy frameworks that encourage the forming of good habits as a step in implementing the BISB model. The environment within the bank should be such that the employees participate in the banks' information security management. Hence, the BISB model requires an environment where employees are involved. By contrast, a policed environment will be misconstrued by the employees and may in effect worsen the information security management efforts.

Proper governance structures should be available at banks that support employee involvement in the overall BISB model rollout. Accordingly, banks could choose an approach in which divisional champions are appointed in the various departments to monitor and promote the BISB model rollout. This could take the form of coordinated awareness campaigns and workshops. An employee who is aware, trained and involved will automatically buy in and this will be an easier way of handling the introduction of the BISB model. Depending on the banks' structures, the training and development division under the human resources department in conjunction with the IT department can spearhead the rollout of the BISB model in a classroom-like approach, which will then be followed up by continuous assessment workshops. Several other approaches not necessarily included in this document may also be used to implement the BISB model in banks.

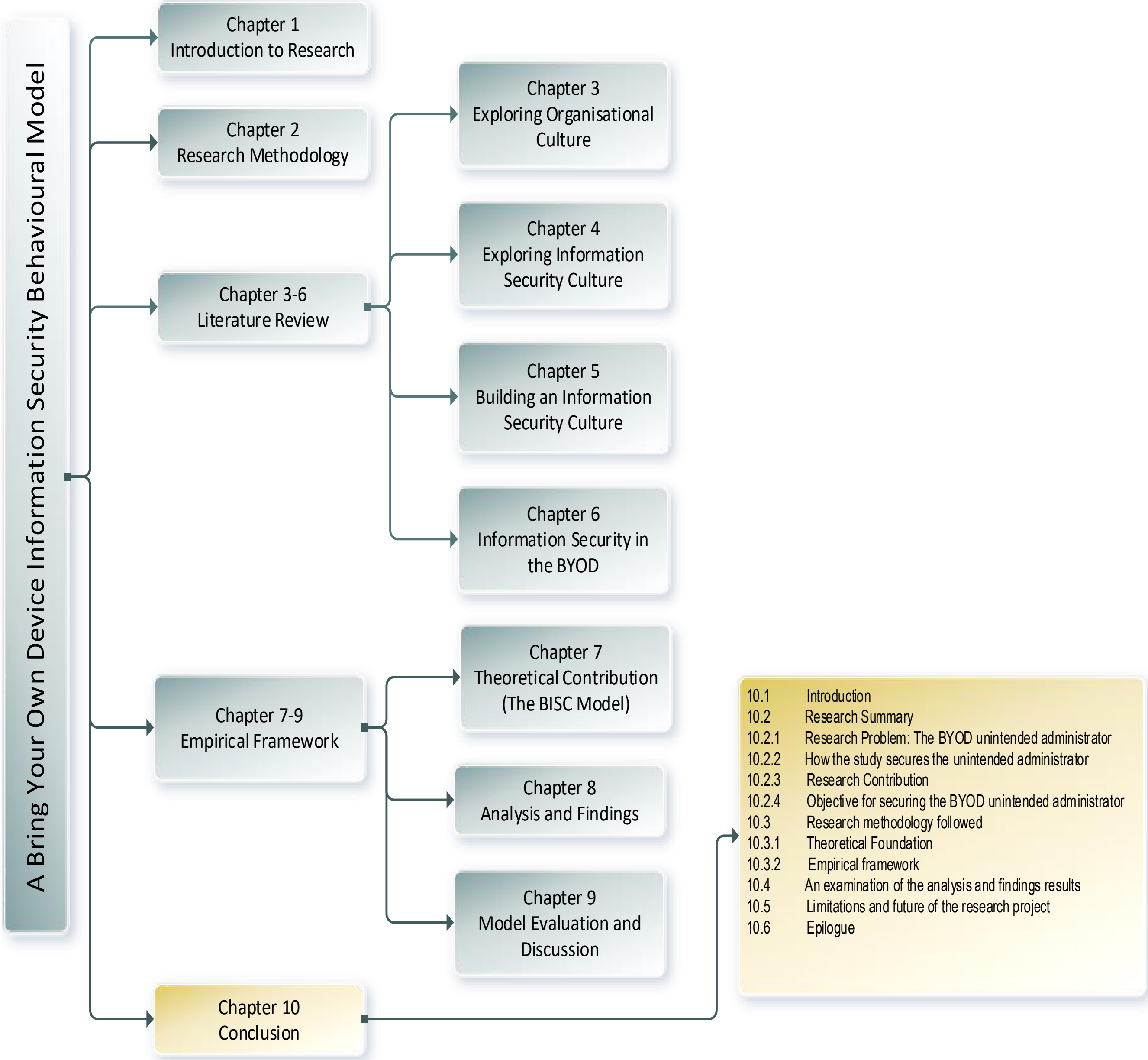
9.5 Conclusion

This chapter provided an overview of the research evaluation methods available in no particular order of significance. In this study, the expert review evaluation method was chosen as the appropriate approach to evaluate the BISB model, since the people intended to make use of this model (CIOs from banks) they could carry out the assessment. This was followed by an analysis of the expert review process which culminated in seven evaluation criteria derived from Hevner's guidelines. Guideline number three proposes research evaluation as a key function of the research process. This then led to the linking of the evaluation process to the research paradigm of design science, which was followed in this study.

The theoretical propositions introduced in Chapter 7 were evaluated in this chapter based on the statistical analysis conducted in Chapter 8. Conclusions reached on the theoretical propositions were then used as the basis for formulating the final BISB research model. The refined BISB model was then presented for the expert review process. The expert review process carried out was based on fifteen questions formulated based on the seven criteria informed by guideline number three of Hevner's design science paradigm. The results of the expert review process confirmed the importance of the BISB model across the criteria of completeness, consistency, accuracy, performance, usability reliability and best fit. More than 50% of the responses across all the criteria were confirmed as positive with regard to the BISB model. Further analysis of the responses from local and international bank CIOs showed the same results. The chapter concluded with a discussion on the findings of the BISB evaluation process. A number of premises cited in 9.4 supported the argument that information security for BYOD is no longer the preserve of the IT department and that technology alone can no longer secure the BYOD. This led to the conclusion that securing the BYOD unintended administrator requires building a culture that is made up of certain individual and organisational traits.

Chapter 10 : Conclusion

"A conclusion is the place where you get tired of thinking."-Arthur Bloch


A Bring Your Own Device Information Security Behavioural Model
Chapter 1
Introduction to Research
Chapter 2
Research Methodology
Chapter 3-6
Literature Review
Chapter 3
Exploring Organisational Culture
Chapter 4
Exploring Information Security Culture
Chapter 5
Building an Information Security Culture
Chapter 6
Information Security in the BYOD
Chapter 7-9
Empirical Framework
Chapter 7
Theoretical Contribution (The BISC Model)
Chapter 8
Analysis and Findings
Chapter 9
Model Evaluation and Discussion
Chapter 10
Conclusion
10.1 Introduction
10.2 Research Summary
10.2.1 Research Problem: The BYOD unintended administrator
10.2.2 How the study secures the unintended administrator
10.2.3 Research Contribution
10.2.4 Objective for securing the BYOD unintended administrator
10.3 Research methodology followed
10.3.1 Theoretical Foundation
10.3.2 Empirical framework
10.4 An examination of the analysis and findings results
10.5 Limitations and future of the research project
10.6 Epilogue

10.1 Introduction

This chapter provides a summative conclusion to the research project. The main study theme presented centred on how the security risks posed by the unintended administrator can be mitigated. The thesis was divided into two sections: the theoretical foundation of the study, which focused on the literature review, and the empirical framework, which dealt with the analysis, evaluation and conclusion of the study. The entire research venture sought to find an answer to the research question: How can an organisation build an information security culture (ISC) to mitigate the risks of the BYOD phenomenon? The model presented in this study was based on secondary data collected from a review of existing literature on information security policy development and implementation methods. The primary data used to validate the proposed model were collected by means of a survey. In addition, the respondents' feedback from the survey was used to refine the framework. The model was then further refined through an expert review process.

This chapter summaries how the research objectives were met in order to answer the research questions posed by the study. It further discusses the theoretical contribution, the research methodology used, research evaluation and the limitations of study. Finally, the chapter offers recommendations for future research. The next section presents a summary of the research project followed by the research problem.

10.2 Research Summary

Historically, the computing environment was characterised by a computing policy framework through which organisations provided the employee with everything they needed in terms of what was referred to as the Use What You are Told (UWYT) (discussed in detail in the introduction to the study). The BYOD gained precedence as a result of the massive penetration of smart phones and the improvement in Internet speed. BYOD is an employee-driven phenomenon that benefits both the employee and the organisation by offering flexibility and reducing the IT investments required by organisations (organisations in this instance refers to banks). Through the BYOD phenomenon, employee hours are unlimited as long as there is connectivity; the employee can work anywhere at any time of their choice. Several additional benefits include reduced IT budgets, employee flexibility and many others.

Whilst BYOD brought a number of benefits, there are also a number of risks and challenges that organisations have to address at the same time, prompting some researchers (Ghosh et al., 2013;

Larryfurst, 2013) to call the phenomenon “Bring Your Own Disaster”. Several banks have thus devised technical solutions to address BYOD challenges, creating security policy to implement these solutions. The fact that employees drive BYOD also implies that their choices regarding the devices they use vary. This also means that if a bank is to invest in technical solutions to secure BYOD, it has to cover all device types such as Apple, Android, Windows and others on offer. The rate of change in complexity for the BYOD devices is also faster than the policy changes in banks. This is the reason why Sobers (2014) and Brien et al. (2013) state that policy and culture will always play catch-up to technology. If banks are to continue to remain abreast of modern computing trends, the adoption of BYOD will be the rule rather than the exception (Eschelbeck & Schwartzberg, 2012; Song & Kong, 2017). Accordingly, it is imperative that banks take a proactive approach in addressing these security concerns if they are to remain in business.

This forms the basis for the problem statement which motivated this research study. Whilst all administrative rights on devices historically resided within the IT department, the BYOD has made employees the unintended administrators by default as they have complete administrative rights over their device in terms of BYOD. The unintended administrator has changed the rules of information security management in the organisation, which needs to be addressed immediately for the continuous survival of the banks. The next section summarises the problem this research study attempted to address.

10.2.1 Research Problem: The BYOD Unintended Administrator

This study sought to solve the problem of the unintended administrator’s total control of the devices, which poses information security risks and challenges to banks. CIOs and IT security experts no longer have total control of the IT environment. Because the monitoring of traditional end point security systems like antivirus software and network perimeter devices is no longer centrally controlled, this exposes organisations to many forms of attacks. In essence, under BYOD the organisation no longer has control over the devices they use. For banks, risk is something that should always be guarded against. Banking is about trust, the moment customers lose trust in the bank, the banks will suffer numerous losses. Banking is a heavily regulated industry where the regulators encourage and enforce strict adherence to information security. In order to secure the unintended administrator, this study followed the approach of answering the questions in the subsequent section.

10.2.2 How the Study Secures the Unintended Administrator

This study attempted to answer the main research question: *How can organisations build an ISC to mitigate the risks posed by the BYOD unintended administrator?* This research question is based on the realisation that the best way to secure unintended administrators is to build their information security culture (ISC). Proponents of organisational culture (OC) state that in building an OC, organisations should consider the employees' contribution (Nguyen, 2014; Olson, 1982). In Chapter 4, ISC is situated as a subculture of OC. The chapters covering the theoretical contribution (Chapters 3 to 6) emphasise the relevance and application of the ISC in securing the BYOD unintended administrator. In order to answer this research question, four sub-questions were formulated. The answers to these research sub-questions resulted in the answer to the main research question. These sub-questions were subsequently answered as follows:

i. **Sub-question 1: What is required for organisations to build an information security culture?**

Considering that ISC is situated as a subculture of OC, in Chapter 3 it was identified that organisations need to tap into their employees' traits such as attitude, knowledge and habit. These individual employee traits will also require organisation-wide traits such as a conducive environment, good governance and a training programme that complements the individual traits.

The three employee traits of attitude, knowledge and habit were identified from the literature study as being central to the creation of an ISC. ISC is defined as the collective attitude and knowledge traits combined with additional ones such as values and assumptions. The theory of reasoned action (TRA) described in section 4.4.1 also points out that the individual's attitude contributes immensely to the behavioural intention towards ISC. Knowledge, as explained in Chapter 5, was also identified as being important in building an ISC. Nonaka's (1994) model of model creation fits very well into the culture creation. Regarding habit, Lee et al. (2016) state that continuous habits formulate behavioural intention to observe information security. Organisation traits aware consolidated into three as governance, environment and training.

ii. Sub-question 2: How does the BYOD unintended administrator impact the organisational information security culture?

The BYOD unintended administrator has shifted information security management in banks from the traditional organisational network perimeter controlled by the IT department to the network perimeter where the BYOD device connects at any given time. Consequently, this demands that the way banks manage their information security on the BYOD devices changes to meet the level of complexity that comes with the phenomenon. The unintended administrator both requires and demands that there be a culture in place that mitigates information security risks. As was uncovered by this study, technical solutions alone are no longer sufficient to mitigate the risks that the unintended administrator brings to the bank.

iii. **Sub-question 3: How can BYOD information security behaviour mitigate the risks associated with the unintended administrator?**

Most manufacturers of mobile devices used in the BYOD environment have developed technical solutions for managing security on their devices. However, BYOD is not necessarily vendor specific in terms of the type of device used in banks as employees buy the mobile devices they prefer. This makes is difficult for CIOs to implement a platform agnostic solution that covers the various devices that the employees acquire for BYOD. This study recommends that an ISC for the BYOD phenomenon holds promise for the management of information security in banks. The BISB model presented in Chapter 7 is made up of employee and organisational traits which if collectively implemented will encourage the appropriate behavioural intention towards the management of information security.

iv. **Sub-question 4: What roles do the employees and the organisation play in securing the BYOD unintended administrator?**

In order to secure the unintended administrator, the research pointed out that there is need for a combination of efforts on the part of the employee and the organisation. The six constructs that culminated in the BISB model consist of employee and organisational traits. Through their individual traits of attitude, habit and knowledge combined with the organisational traits of environment, governance and training, employees were found to contribute significantly to the creation of a BISB. These traits were thus combined to form the constructs of the BISB model. The answers to these four sub-questions were therefore deemed sufficient for answering the research question for this study.

10.2.3 Research Contribution

The main contribution made by this study is the development of a model for building an ISC for the BYOD unintended administrator. This model intends to serve as a guide for information security practitioners, managers and CIOs in the Zimbabwe banking industry in the process of developing and implementing information security policies around the BYOD phenomenon. The proposed model indicates that employees are central to the development and enforcement of an effective ISC. In addition, the study emphasises the importance of the organisation's contribution to building a BISB. Furthermore, the model breaks down the individual and organisational traits involved in building an ISC. The next section summarises the findings of the study culminating in the proposed BISB model.

The theoretical contribution section formed the first part of the empirical framework. This section, in Chapter 7 of the study, introduced the BISB model and aligned it to the tacit assumptions of the model creation process. The sections in chapter 7 explore the process followed in identifying the constructs and re-emphasise that the constructs were obtained from the literature review process. This was then followed by the establishment of the relationships between the traits which marked the beginning of the model formulation process.

Behavioural intention is singled out as representing ISC. The definition of behavioural intention is based on the theories of Ajzen and Fishbein discussed in Chapter 4. At this point the six BISB model constructs were enlisted and grouped as individual and organisation traits. The individual traits are made up of attitude, knowledge and habit whereas the organisational traits consist of environment, governance and awareness. The theoretical contributions resulted in the formulation of research propositions which were then evaluated in Chapter 9 in the model evaluation and the ensuing discussion. This section concluded by presenting the first version of the proposed BISB model. The findings of the literature study were subjected to a survey in one commercial bank in Zimbabwe and the results of will be discussed in the next section, marking the second phase of the empirical framework.

10.2.4 Objective for Securing the BYOD Unintended Administrator

Having identified the problem that the BYOD unintended administrator brings to the bank and also that the best way to secure the unintended administrator is to create an ISC, the objective pursued in this study is to build a model to address the research problem as outlined in Chapter 1. If banks can build a culture of information security for the BYOD phenomenon, they can easily leverage on the benefits that BYOD brings (Ginovsky, 2012) Thus, this study makes a significant research contribution.

The summary of the findings was divided into three sections: Firstly, an overview of the research methodology followed was given and, secondly, the findings were analysed in line with the theoretical foundation of the study. This theoretical foundation mainly covered the literature review and culminated in the traits that were then used as constructs for the BISB model. The third and last phase covers the analysis of the findings from the empirical framework of the study. The empirical framework contained aspects of the study such as the statistical analysis and the evaluation of the results.

10.3 Research Methodology Followed

The research methodology sections provided a structured way for conducting the research process. Methodology forms part of the research worldview that the research paradigm in essence followed (Trochim et al., 2016). Further, research methodology gives direction and sequence to ontology, which is the nature of the reality being studied, and the epistemology, which is the knowledge construction process. Therefore, that methodology is the way in which knowledge is attained. The research methodology followed in this study can be summarised under five headings:

- **Research paradigm.** The overall philosophical framework or research paradigm applied in this study is design science. Following the literature review conducted, design science was chosen as the appropriate paradigm for this study. The seven design science guidelines, as introduced by Hevner et al. (2004), formed the design of this research. Subsequently, a detailed discussion of the research method followed in the study was covered in Chapter 2.
- **Study population.** A survey was conducted on a total of 270 bank employees via an online questionnaire loaded in Survey Monkey. Of the population of 270, 205 employees participated. Of the 205 questionnaires returned, 179 were deemed usable, giving a response rate of 87% (see questionnaire in Appendix 2). As a response rate of 30% or higher is deemed acceptable in a research project (Oates, 2006) this response rate was deemed acceptable.
- **Data collection.** The questionnaire was the main method of data collection. Chapter 8 discussed how the data collection was conducted in detail, culminating in an analysis of the results.
- **Data analysis.** Chapter 8 comprised a detailed analysis of the data. Statistical tests of factor analysis were used to analyse the data, with regressions and multiple correlation computations being conducted to highlight the statistical relevance of the research.

The next stage of the summary of research findings covers the theoretical foundation for this study and summarised the findings in this regard from the literature review conducted. The discussions in Chapter 7 identified that the theoretical contribution, namely, the BISB model, was based on the theoretical foundation.

10.3.1 Theoretical Foundation

This section of the research was covered in four chapters, ranging from Chapters 3 to 6. It is important to note that the research model, which is the contribution of this study, is premised on the traits that were obtained from the literature review through an inductive approach. The first part of the theoretical foundation related to the way organisations can build an ISC for the BYOD unintended administrator by influencing the OC. The second part explored ISC in organisations. This was followed by an examination of ways in which organisations can build an organisational ISC. The discussion on the theoretical foundation concluded by examining information security in the BYOD environment. In order to summarise the theoretical foundation, the four chapters will be summarised.

OC is viewed as the way things are done in a given organisation (Lundy & Cowling, 1996). In this research study, OC is also viewed from Schein's perspective, which holds that OC is a collective pattern of basic assumptions learnt by an organisation over time. OC was deemed important in this study considering that the final research artefact (the BISB model) is a culmination of the organisational traits combined with individual traits. Scholars such as Sun (2008), Singh and Phil (2012) and Martins and Terblanche (2003) agree on the central role played by the OC in influencing employees' behaviour, attitude and knowledge. They maintain that the governance within the organisation and the training and awareness programmes offered to employees influence the overall OC.

Theories by OC experts were also explored to bring about rigour in the research. Schein's OC theory was one of the theories explored in Chapter 3 (Schein, 1990). The theory postulates that OC can be viewed on three levels: the artefact level, the espoused level, and shared tacit assumptions. These three levels helped to confirm the validity and relevance of the constructs for the BISB model. Details on how the theories support the BISB model were discussed on Chapter 3. A perspective from Hofstede (2010) manifests culture on four levels: symbols, heroes, rituals and values. This model contributed significantly to the governance of organisations as a construct of the BISB model. The third theory examined under OC is Denison's (1990) perspective. Denison's model centres on four perspectives: involvement, consistency, adaptability and motivation. Chapter 3 contains a detailed analysis of the model.

OC has emerged from the literature as pivotal to the three organisational constructs for the BISB model. Chapter 3 detailed the way in which the conclusion that governance, environment and awareness training were the three major organisational constructs was arrived at. When building an OC, employee attributions also play a pivotal role. Employees come from different cultural backgrounds that all combine in the BISB model. The narrative on OC in the banking context would be incomplete if the employees' contributions were not recognised.

Chen et al. (2015) situate ISC as a subculture of OC as it is essentially part of the entire OC framework. From this perspective, ISC can be viewed as the way information security is managed in any given organisation, borrowing from the definition of OC given by Lundy and Cowling (1996). From another perspective, Udeh and Dhillon (2008) maintain that ISC is a collection of individual attributes such as behaviour and attitude towards the protection of information. Behaviour was cited as a central aspect of the creation of an ISC. As discussed in Chapter 4, Alfawaz et al. (2010) devised three behaviour modes that support the building of an ISC.

Human behaviour theories were also discussed in detail in Chapter 4, qualifying the way the employees' individual traits result in building an ISC. The TRA points out that behavioural intentions, which are a function of an individual's attitude, drive and influence the behaviour of an employee in any organisation (Ajzen, 1991). This behavioural intention construct thus became the dependent variable in the formulation of the BISB model. Additionally, Ajzen's (1991) TPB, which is an extension of TRA, posits that predicting a particular behaviour can be used in guiding the creation of an ISC, provided the behaviour is intentional. These theories are articulated in Chapter 4 in detail, linking them to the BISB model. ISC forms the core of this research study. The theoretical foundation formed the basis for the inductive formulation of the BISB model constructs, which are all aimed at addressing the BISB for the unintended administrator.

The organisational characteristic that influences employee performance in the organisation forms one of the cornerstones for building an organisational ISC. The literature review identified that in building an organisational ISC, change management is required so as to avoid a culture shock. Bibb (2010) believes that organisational ISCs are made up of different individual cultures, some of which conflict. This view, discussed in Chapter 5, is shared by Cameron and Quinn (2006) who point out that building an organisational ISC is an intra-organisational process driven by all departments and employees.

Gordon (1991) proposed a model in which he pointed out that an organisational ISC is developed by organisational beliefs. In his model, a key component is management's influence in building an organisational ISC (Gordon, 1991), as well as the organisation's customers. Other models like the CVF and the MISSTEV were also discussed in Chapter 5 as supporting pillars for building an organisational ISC. The CVF is based on four values – collaborate, control, compete and create – which organisations can explore in building a BISB. Chapter 5 discussed these values in detail and contained other models, like the CCLM and the model for knowledge creation, on how an ISC can be created. The theoretical foundation on building culture, both OC and ISC, is covered in Chapters 3 and 5.

Chapter 6 discussed BYOD trends in detail. The theme for this chapter was information security for the BYOD phenomenon. The chapter discussed how information security is implemented and managed in BYOD. It gave an overview of the way CoIT has impacted on organisations' information security management and discussed various forms of the BYOD such as Shadow IT, CoIT, enterprise mobility among others. This section also revealed the security challenges introduced by BYOD. Information security in BYOD and information security for mobile devices in the banking context were also discussed in detail. The chapter covered the technical aspects of BYOD security which were not necessarily the focus of this study and summarised the empirical framework. The following sections provided a high-level overview of the empirical framework for this study.

10.3.2 Empirical Framework

The empirical framework basically covers the scientific computations and deductions that were carried out in this study leading to the conclusions that were reached. Frechtling (2002) argues that there is a trade-off between the depth and breadth that is achieved by including both empirical and theoretical study frameworks. The empirical framework section for this study comprised three chapters (Chapters 7 to 9). The focus of the section is on the scientific application of the research methods for this study.

10.4 An Examination of the Analysis and the Findings

The findings of the statistical analysis are discussed in Chapter 8 and a detailed account of the way the survey was conducted was given. A pilot study was conducted to empirically test the practicality and applicability of the research questions. The formulated research instrument was then emailed to the bank employees and a response rate of 87% was received. In this bank, 89% of respondents indicated that they owned smart devices and 92% understood the implications of breaching information security controls.

The reliability of the research instrument was measured using Cronbach's alpha and factor analysis was used to test its validity. Internal and external validity were also measured. In addition, the factors were tested for correlation and multiple regression and the results were presented in Chapter 8.

10.5 Limitations and Future of the Research

Inasmuch as this study was evaluated and found to satisfy the expectations of experts who reviewed it, some model limitations are also acknowledged. These limitations will be addressed in future research efforts. They do not, however, impact in any way on the application of the BISB model. However, addressing them will improve the model applicability and usability.

Firstly, the research study was confined to a single bank, which implies that the components measured were only reflective of the organisational ISC for the particular bank not the whole market. The traits measurements derived from this study were a representation of the selected bank and not necessarily the entire Zimbabwean banking industry. There is a likelihood that the results obtained are not a true representation of what is happening in the industry although the BISB model is designed to represent the banking industry in Zimbabwe. Confirmations by CIOs during the model evaluation process, however, brought a considerable level of comfort in confirming that the BISB model is relevant.

Secondly, the study was confined to Zimbabwe which means the context within which the constructs were tested only represent Zimbabwe. Although the context for the BISB model is Zimbabwe, the researcher deems the model to be applicable to countries other than Zimbabwe. However, the findings were made in Zimbabwe and confirmed by CIOs from Zimbabwe which may imply that the evaluation criteria only satisfy the Zimbabwean context and may need a complete overhaul which could change the results found in regard to the BISB model. Inasmuch as there are international banks in Zimbabwe, it cannot be ignored that the CIOs from the international banks in Zimbabwe evaluated the BISB model with a bias to the Zimbabwean context. Future work will include a wider scope of banks and more than one country, thus using Zimbabwe as the research baseline.

Thirdly, the BISB model traits were not necessarily exhaustive in measuring the behavioural intention of the unintended administrator to implement an ISC. Additional constructs could potentially be added to the model to address other characteristics, especially when being applied to other countries. The constructs that were chosen, however, were confirmed as sufficient for the Zimbabwean context by the results of the evaluation process conducted in Chapter 9 of this research document. Future research will build on this study by exploring these additional constructs to satisfy the additional scope elements. Future works will include a wide population of banks in Zimbabwe and abroad. Additional statistical tests on the model will be conducted to obtain empirical evidence to support the model and its application to the banking sector. Confirmatory tests will also be conducted to scientifically and rigorously prove the contribution made by the model's six traits. The next section explores the means by which banks can make use of the BISB model.

10.6 Epilogue

This thesis present a study of the way banks can build an ISC for the BYOD unintended administrator. The relevance and applicability of the model is determined by the impact it will have on enabling banks to secure the unintended administrator in the BYOD environment. It was noted that banks are always playing catch-up to technological trends, therefore the BISB model will quicken their pace when attempting to catch up with BYOD security. Overall, the model has been deemed applicable in building an ISC for banks in Zimbabwe. If the model proposed in Chapter 7 is implemented by banks in Zimbabwe, their information security challenges will be addressed with ease. In addition, its implementation will enable them to leverage on the benefits that come with BYOD. The BISB model will sanitise the banks in Zimbabwe against the security risks that come with the consumerisation of banking and this will enable them to participate on the world stage in terms of banking technology.

References

Absalom, R. (2012). *International data privacy legislation review: A guide for BYOD policies*. Ovum.

Ackerman, A., & Krupp, M. (2012). Five components to consider for BYOT/BYOD. In *IADIS International Conference on Cognition and Exploratory Learning in Digital Age (CELDA 2012)* (pp. 35–41). New Jersey: IADIS

Adam, K. A., & Lawrence, E. K. (2015). *Research methods, statistics, and application*. Thousand Oaks, CA: Sage Publications.

Afreen, R. (2014). Bring Your Own Device (BYOD) in higher education: Opportunities and challenges. *International Journal of Emerging Trends & Technology in Computer Science*, *3*(1), 233–236.

Ahmed, G., Ragsdell, G., & Olphert, W. (2011). Knowledge sharing and information security: A paradox? *European Conference on Knowledge Management*, *3*, 1083–1091.

Ahmed, M. D., & Sundaram, D. (2011). Design science research methodology: An Artefact-centric creation and evaluation approach. In *Proceedings of the 22nd Australian Conference on Information Systems* (Vol. 1, p. Paper 79). ACIS 2011 Proceedings: Sydney

Ajzen, I. (2002, April). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. *Journal of Applied Social Psychology*, *6*, 665–683.

Ajzen, I., & Driver, B. E. (1992). Application of the theory of planned behaviour to leisure choice. *Journal of Leisure Research*, *24*(3), 207–224.

Ajzen, I., Netemeyer, R., & Van Ryn, M. (1991, January). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*, 179–211.

Alagbe, A. (2016). *The security implication of BYOD : Mobile devices in the workplace*. Glasgow: University of Strathclyde.

Albarq, A. N., & Alsughayir, A. (2013). Examining theory of reasoned action in internet banking using SEM among Saudi consumers. *International Journal of Marketing Practices*, *1*(1), 16–30.

Aldrich, H. E., & Auster, E. (1986, June). Even dwarfs started small: Liabilities of age and size and their strategic implications. *Research in Organizational Behavior*, *8*, 165–198. http://doi.org/10.2139/ssrn.1497769

Alfawaz, S., Nelson, K., & Mohannak, K. (2010). Information security culture: A behaviour compliance conceptual framework. *Conferences in Research and Practice in Information*

Technology Series, *105*(Aisc), 47–55.

Alhogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, *49*, 567–575.

AlHogail, A. (2015). Cultivating and assessing an organizational information security culture: An empirical study. *International Journal of Security and Its Applications*, *9*(7), 163–178. http://doi.org/10.14257/ijsia.2015.9.7.15

Alhogail, A., & Mirza, A. (2014a). A framework of information security culture change. *Journal of Theoretical and Applied Information Technology*, *64*(2), 540–549.

Alhogail, A., & Mirza, A. (2014b, February). Information security culture: A definition and a literature review. *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*, *3*, 1–7.

Alhogail, A., Mirza, A., & Bakry, S. H. (2015). A comprehensive human factor framework for information security in organizations. *Journal of Theoretical and Applied Information Technology*, *78*(2), 201–211.

Ali, M., & Brooks, L. (2009). Cultural aspects of multi-channel customer management : A UK case study. In *Fifteenth Americas Conference on Information Systems* (pp. 1–11). San Francisco, California.

Allam, S., Flowerday, S. V., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers and Security*, *42*, 55–65.

Alnatheer, M. A. (2014). A Conceptual Model to Understand Information Security Culture. *International Journal of Social Science and Humanity*, *4*(2), 104–107.

AMCTO. (2012). The consumerization of IT. *CIO Insight*.

Anderson, R., & Moore, T. (2006). The Economics of Information Security. *Science*, *314*(5799), 610–613.

Armando, A., Costa, G., Verderame, L., & Merlo, A. (2014). Securing the "bring your own device" paradigm. *IEEE Computer Society*, *47*(6), 48–56. http://doi.org/164

Arwa, J. R. (2014). *Adoption of Bring Your Own Device to enhance customer service delivery in Kenya commercial bank.* University of Nairobi.

Ashwani, M. (2016). 1 in 5 enterprises admit of mobile data breach resulting from BYOD – ET CIO. Retrieved May 6, 2017, from http://cio.economictimes.indiatimes.com/news/digital-security/1-in-5-enterprises-admit-of-mobile-data-breach-resulting-from-byod/51707794

Atikomtrirat, W., Pongpayaklert, T., & Lundgren, M. (2011). *Managing diversity in* *multinational organizations: Swedish and Thai culture*. Linnaeus University, Sweden.

Babatunde, D. A., Selamat, M. H., & Salman, R. T. (2014). The Role of information security development (ISD) in effective information security management (ISM) implementation in the banks: A Nigerian case. *Journal of Modern Accounting and Auditing*, *10*(5), 614–619.

Bada, M., Sasse, A., & Nurse, J. R. C. (2015). *Cyber security awareness campaigns: Why do they fail to change behaviour?* Proceedings of the International Conference on Cyber Security for Sustainable Society. London.

Banerjee, U. (2012). *What is consumerization of IT?* Retrieved from http://udayanbanerjee.sys-con.com/node/2227616

BankingTech. (2016). *BYOD – Harnessing the opportunity securely.* Banking Technology. Retrieved July 30, 2016, from http://www.bankingtech.com/49879/byod-—-harnessing-the-opportunity-securely/

Barnes, S. J. (2003). Enterprise mobility: Concept and examples. *International Journal of Mobile Communications*, *1*(4), 341. http://doi.org/10.1504/IJMC.2003.003990

Barrett, R. (2006). *The Importance of Values in Building a High Performance Culture*. *Building a Values-Driven Organization: A Whole-System Approach to Cultural Transformation*. Boston, MA: Barrett Values Center.

Barrett, R. (2013). *Unleashing Human Potential for Performance and Profit*. London Routledge.

Basole, R. C. (2008). Enterprise mobility: Researching a new paradigm. *Information Knowledge Systems Management*, *7*(1), 1–7.

Bayens, G. J., & Roberson, C. (2010). *Criminal justice research methods: Theory and practice*. New York: CRC Press.

Beidokhti, A. A. A., & Ghaderi, M. M. (2011). Studying the relationship between organizational culture and customer satisfaction in Bank Mellat. *International Journal of Business and Commerce*, *1*(4), 74–89.

Belani, R. (2014). The evolution of cyber security. *Siliconindia*, pp. 40–42. Mumbai. Retrieved from http://www.cfr.org/publication/15577

Bennett, S. (2015). *Why information governance needs top-down leadership*. Governance Directions.

Berg, B. L. (2004). *Qualitative Research Methods for the Social Sciences*. *Journal of Research and Advanced Studies* (7th ed.). Boston, MA: Allyn and Bacon.

Bhatt, R. (2011). Theory of planned behavior: A perspective in India’s internet banking. *International Journals of Marketing and Technology (IJMT)*, *19*(2), 12–26.

Bibb, S. (2010). *Beyond the code of conduct: eight steps to building an ethical organisational culture*. *An Everyday Guide to Ethics in Business*. London.

Biggar, D., & Heimler, A. (2005). An increasing role for competition in the regulation of banks. *Antitrust Enforcement in Regulated Sectors -Subgoup 1*, *1*(June), 1–30.

Blatt, K., & Gallagher, J. (2014). Mobile workforce : The rise of the mobilocracy mobile and the work–life balance. In P. A. Bruck & M. Rao (Eds.), *Global mobile: Applications and innovations for the worldwide mobile ecosystem*. San Francisco, CA.

Blount, S. (2011). *the consumerization of IT : security challenges of the new world order*. *Agility made possible technology brief*. New York: CA Technologies.

Bodine, K., & Dorsey, M. (2013). The Business Impact Of Customer Experience. *Forrester Research*, 1–8. Retrieved from http://solutions.forrester.com/Global/FileLib/Forr_Perspective_/Forrester-Perspective-CX-2.pdf

Boisnier, A., & Chatman, J. A. (2003). Leading and Managing People in the Dynamic Organization. *Leading and Managing People in the Dynamic Organization*, 87–112. http://doi.org/10.4324/9781410607508

Bradbury, D. (2007). Decoding digital rights management. *Computers & Security*, *26*, 31–33.

Bransford, J. D. (2000). *How People Learn*. *Brain,Mind,Experience, and School* (Expanded). Washington DC: National Academies Press.

Bridges, W. (1987). *Getting them through the wilderness : A leader's guide to transition*. *New Management*. California.

Brien, J. O., Islam, S., Bao, S., Weng, F., Xiong, W., & Ma, A. (2013). *Information security culture: Literature review*. Melbourne: Minerva.

Brodin, M. (2016a). BYOD vs. CYOD: What is the difference? In M. B. Nunes, P. Isaías, & P. Powell (Eds.), *IADIS International Conference Information Systems* (Vol. 3, pp. 55–62). Vilamoura, Portugal.

Brodin, M. (2016b). Management of mobile devices: How to implement a new strategy. In *The 27th International Business Information Management Association Conference: Innovation Management and Education Excellence Vision 2020: From Regional Development Sustainability to Global Economic Growth* (pp. 1261–1268). Milan Italy.

Burgess, R., & Pande, R. (2005). Do rural banks matter? Evidence from the Indian social banking experiment. *American Economic Review*, *95*(3), 780–795.

Burns, R. B., & Burns, R. B. (2000). *Introduction to research methods*. London: Routledge/Sage.

Businessballs. (2013). *Conscious competence learning model matrix: Unconscious* *incompetence to unconscious competence.* Retrieved January 3, 2017, from http://www.businessballs.com/consciouscompetencelearningmodel.htm

Cameron, K. S. (2009). *An Introduction to the Competing Values Framework*. *Haworth Press*. Michigan,USA.

Cameron, K. S., & Quinn, R. E. (2006). Diagnosing and changing organizational culture: Based on the competing values framework. *Personnel Psychology* (Revised, Vol. 59). San Francisco, CA: Jossey Bass. http://doi.org/10.1111/j.1744-6570.2006.00052_5.x

Cameron, R. (2011). Mixed methods research: The five Ps framework: One stop search. *The Electronic Journal of Business Research Methods*, *9*(2), 96–108. http://doi.org/ISSN 1477-7029

Campbell, D., Stonehouse, G., & Houston, B. (2002). *Business strategy* (2nd ed.). Oxford, UK: Butterworth Heinemann.

Carden, P. (2007). Enterprise mobility. *Enriching Communications*, *1*(2), 1–21.

Cavoukian, A. (2013). *BYOD: (Bring Your Own Device) Is Your Organization Ready?* Ontario.

Chang, J. M., Ho, P. C., & Chang, T. C. (2014). Securing BYOD. *IT Professional, 16*.

Chatterjee, S., Sarker, S., & Valacich, J. S. (2015). The behavioral roots of information systems security: Exploring key factors related to unethical IT use. *Journal of Management Information Systems*, *31*(4), 49–87.

Chen, H., Li, J., Hoang, T., & Lou, X. (2013). *Security challenges of BYOD : A security education , training and awareness perspective*. Unpublished, 1–8.

Chen, J. (2014). Enterprise mobility: The next major risk management challenge (cover story). *Directors & Boards*, *39*(1), 18–21. Retrieved from http://search.ebscohost.com.ezproxy.liv.ac.uk/login.aspx?direct=true&db=bth&AN=100105809&site=bsi-live

Chen, W., & Hirschheim, R. (2004). A paradigmatic and methodological examination of information systems research from 1991 to 2001. *Information Systems Journal*, *14*(3), 197–235.

Chen, Y., Ramamurthy, K. (Ram), & Wen, K.-W. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems*, *55*(3), 11–19.

Cheng, H. (2014). *Banking supervision*. *Banking Supervision Report*. Hong Kong: Hong Kong Monetary Authority.

Chia, P. a., Maynard, S. B., & Ruighaver, a. B. (2002). Understanding Organizational Security Culture. *Pacis*, (September 2002), 1–23. Retrieved from http://people.eng.unimelb.edu.au/seanbm/research/2003SecCultChap.pdf

Childress, J. R. (2011). *Why Banks Should Focus On Culture , Now More Than Ever*. New York: The Principa Group.

Chiu, T. K. F., & Churchill, D. (2017). Adoption of mobile devices in teaching: Changes in teacher beliefs, attitudes and anxiety. *Interactive Learning Environments*, *24*(2), 317–327.

Cisco Systems. (2016). *Creating the Culture of Security*. *10 Tips for Building a Business of Pervasive Security*. Boston, MA: Cisco Press.

CITO Research. (2015). *Enterprise mobility management: The big bang theory -CIO*. *CITO Research Advancing the Craft of Technology Leadership*. California: Maas360.

Citrix. (2015). *Mobile analytics report*. New York Citrix Press.

Clark, W. C., & Lee, K. N. (2009). Nurturing sustainability. *Issues in Science and Technology, 26*. Hong Kong.

Collis, J., & Hussey, R. (2003a). *A Practical Guide For Undergraduate And Postgraduate Students. 2009* (3rd Editio). Palgrave. Retrieved from http://www.amazon.co.uk/Business-Research-Practical-Undergraduate-Postgraduate/dp/1403992479

Collis, J., & Roger Hussey. (2003b). *Business Research Business Research A Practical Guide for Undergraduate and Postgraduate Students*. *Nature* (3rd Editio, Vol. 142).

Connolly, L., & Lang, M. (2012). Data protection and employee behaviour: The role of information systems security culture. In *IADIS WWW/Internet 2012* (pp. 1–5). Dublin.

Cooper, D. R., & Schindler, P. S. (2003). *Business research methods* (11th ed.). Oxford, England: McGraw-Hill. Retrieved from http://130.209.236.149/headocs/31businessresearch.pdf

Copeland-Linder, N. (2009). Research and statistics: Reliability and validity in pediatric practice. *Pediatrics in Review*, *30*(7), 278–279. http://doi.org/10.1542/pir.30-7-278

Creswell, J. W., & Clark, P. V. L. (2011). *Designing and conducting mixed methods research* (2nd ed.) London: Sage. http://doi.org/10.1111/j.1753-6405.2007.00097.x/full

Crowley-Henry, M. (2005). Cultural diversity in multinational organisations. In *Dublin Institute of Technology* (p. 29). Galway Ireland: Irish Academy of Management Conference.

D'Arcy, P. (2011). *CIO strategies for consumerization: The future of enterprise mobile computing*. Dell CIO Insight Series. Boston, MA.

Da Veiga, A., & Eloff, J. H. P. (2007). An information security governance framework. *Information Systems Management*. http://doi.org/10.1080/10580530701586136

Da Veiga, A., & Eloff, J. H. P. (2008). *Cultivating and assessing information security culture*. University of Pretoria.

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers and Security*, *29*(2), 196–207. http://doi.org/10.1016/j.cose.2009.09.002

Davidson, G., Coetzee, M., & Visser, D. (2007). Organisational culture and financial performance in a South African investment bank. *SA Journal of Industrial …*, *33*(1), 38–48.

De Vos, A., Strydom, H., Fouche, C., & Delport, C. S. (2005). Research at grass roots: For the social sciences and human services professions (3rd ed.). Pretoria: Van Schaik.

Deloitte. (2015a). *Creating the future in an age of disruption Transformation of the financial services CIO*. Seth Montgomery.

Deloitte. (2015b). The Deloitte Consumer Review Consumer data under attack: The growing threat of cyber crime contents. *Deloitte Consumer Review*.

Denison, D., Janovics, J., & Young, J. (2006). Diagnosing organizational cultures: Validating a model and method. *Researchgate, 304*. Lusanne, Switzerland.

Denison, D., Janovics, J., Young, J., & Cho, H. J. (2004). Diagnosing organizational cultures: Validating a model and method. *International Institute for Management Development* (Vol. 304).

Denison, D. R. (1990). *Corporate culture and organizational effectiveness* (3rd ed.). Oxford, UK: John Wiley & Sons.

Dillon, S., Stahl, F., & Vossen, G. (2015). BYOD and governance of the personal cloud. *International Journal of Cloud Applications and Computing (IJCAC)*, *5*(2), 23–35.

Diogenes, Y., & Gilbert, J. (2015). *Enterprise mobility suite managing BYOD and Company-owned devices*. Redmond, WA: Microsoft Press.

Disterer, G., & Kleiner, C. (2013). BYOD Bring Your Own Device. *Procedia Technology*, *9*(October), 43–53.

Dojkovski, S., Lichtenstein, S., & Warren, M. J. (2010). Enabling information security culture: Influences and challenges for Australian SMEs. In *21st Australasian Conference on Information Systems* (pp. 61–73). Brisbane, Australia: ACIS, Brisbane.

Dole, B. (2010). Generational differences chart: Traditionalists baby boomers generation X, millennials birth years. *Administrative Science Quarterly*, *63*, 44–62.

Downer, K., & Bhattacharya, M. (2016). BYOD security: A new business challenge. In *2015 IEEE International Conference on Smart City, Smart City 2015, Held Jointly with 8th IEEE International Conference on Social Computing and Networking, SocialCom 2015, 5th IEEE International Conference on Sustainable Computing and Communic* (pp. 1128–1133). New York, USA: IEEE.

Downs, D. S., & Hausenblas, H. A. (2005). The theories of reasoned action and planned behavior applied to exercise: A meta-analytic update. *Journal of Physical Activity and Health*, *2*(1), 76–97.

Duncan, R. B. (1972). Characteristics of organizational environments and perceived environmental uncertainty. *Administrative Science Quarterly*, *17*(3), 313.

Easterby-Smith, M., Thorpe, R., & Lowe, A. (2002). *Management research: An introduction* (2nd ed.). Indiana, USA: SAGE series in Management Research.

Eddy, N. (2013). Businesses must adapt to permanent BYOD presence: Ovum. Retrieved May 14, 2015, from http://www.eweek.com/small-business/businesses-must-adapt-to-permanent-byod-presence-ovum.

Ernest Chang, S., & Lin, C. (2007). *Exploring organizational culture for information security management*. *Industrial Management & Data Systems* (Vol. 107). http://doi.org/10.1108/02635570710734316

Ernst & Young. (2013). *Security and risk considerations for your mobile device program*: *Insights on governance, risk and compliance*. Geneva: Ernst & Young.

Eschelbeck, G., & Schwartzberg, D. (2012). *BYOD risks and rewards: How to keep employee smartphones, laptops and tablets secure* (A Sophos Whitepaper 06.12v1.dNA). Boston, MA/ Oxford, UK.

Eslahi, M., , E. H. M. (2015). BYOD: Current state and security challenges. In IEEE (Ed.), *ISCAIE 2014 -2014 IEEE Symposium on Computer Applications and Industrial Electronics* (pp. 189–192). Penang, Malaysia: IEEE.

Farooq, O., & Amin, A. (2017). National culture, information environment, and sensitivity of investment to stock prices: Evidence from emerging markets. *Research in International Business and Finance*, *39*, 41–46.

Fey, C. F., & Denison, D. R. (2000). Organisational culture and effectiveness: The case of foreign firms In Russia. *Journal of Animal and Plant Sciences, 27*. Stockholm.

Finch, N. (2009). Towards an understanding of cultural influence on the international practice of accounting. *Journal of International Business and Cultural Studies*, *2*(1), 1–6.

Fishbein, M., & Ajzen, I. (1981). On construct validity: A critique of Miniard and Cohen's paper. *Journal of Experimental Social Psychology*, *17*(3), 340–350. http://doi.org/10.1016/0022-1031(81)90032-9

Fliplet. (2016). *8 Incredible enterprise mobility trends and facts* (Infographic). Retrieved July 27, 2017, from http://fliplet.com/blog/enterprise-mobility-trends-and-facts/

Frechtling, J. (2002). An Overview of Quantitative of Qualitative Data Collection Methods. In *The 2002 User-Friendly Handbook for Project Evaluation* (2nd ed., pp. 43–62). New York: National Science Foundation, Directorate for Education & Human Resources, Division of Research, Evaluation and Communication.

French, A. M., Guo, C., & Shim, J. P. (2014). Current status, issues, and future of bring your own device (BYOD). *Communications of the Association for Information Systems*, *35*(10), 191–197.

Gantz, J., & Reinsel, D. (2012). *The digital universe in 2020: Big data, bigger digital shadows, and biggest growth in the far east*. (Vol. 2007). Washington, DC: International Data Corporation (IDC).

Garba, A. B., Armarego, J., Murray, D., & Kenworthy, W. (2015). Review of the information security and privacy challenges in bring your own device (BYOD) environments. *Journal of Information Privacy and Security*, *11*(1), 38–54.

Gartner. (2012). *Enterprise mobility: Trends, challenges and solutions Gartner at a glance*. Las Vegas: Gartner.

Gartner. (2016). *Consumerization*. Retrieved February 12, 2017, from http://www.gartner.com/it-glossary/consumerization/

Gast, L. (2003). Well begun is half done: Telling the IICD story of evaluation*. Information Development, 19*. Karachi, Pakistan.

Gessner, D., Girao, J., Karame, G., & Li, W. (2013). Towards a user-friendly security-enhancing BYOD solution. *NEC Technical Journal*, *7*(3), 113–116.

Ghemawat, P., & Reiche, S. (2011). *National cultural differences and multinational business*. Madrid, Spain: The Association to Advance Collegiate Schools of Business.

Ghosh, A., Gajar, P. K., & Rai, S. (2013). Bring your own device (BYOD): Security risks and mitigating strategies. *Journal of Global Research in Computer Science*, *4*(4), 62–70.

Ginovsky, J. (2012). “BYOD” quandary: When the bring your own device trend comes to the bank, measures the risks carefully. *ABA Banking Journal*, *3*(Tech Topics| Office Tools).

Göktürk, E. (2005). *What is “paradigm ”?* Oslo, Norway :Department of Informatics

Goldkuhl, G. (2012). Pragmatism vs interpretivism in qualitative information systems research. *European Journal of Information Systems*, *21*(2), 135–146.

Gordon, G. G. (1985). The relationship of corporate culture to industry sector and corporate performance. In R. H. Kilmann, M. J. Saxton, R. Serpa, & Associates (Eds.), *Gaining control of the corporate culture* (pp. 103–125). San Francisco, CA: Jossey-Bass.

Gordon, G. G. (1991). Industry determinants of organizational culture. *Academy of Management Review, 16*. Melbourne.

GSMA. (2010). *Mobile Money for the unbanked: Definitions*. London: GSM Association.

Hackshaw, A. (2009). *A concise guide to clinical trials*. Wiley-Blackwell/BMJ Books. Retrieved from https://books.google.co.zw/books?id=nDsiHnLu4nIC&dq=Allan+Hackshaw+©+2009+Allan+Hackshaw.+ISBN:+978-1-405-16774-1+205&source=gbs_navlinks_s

Haworth. (2015). *How to create a successful organizational culture: Build It — literally*. Michigan: Haworth Press.

Hazelton, C., Kingstone, S., Mckee, J., & Analyst, S. (2016). *2016 trends in enterprise mobility*. San Francisco, CA: 451 Research.

Healy, M., & Perry, C. (2000). Comprehensive criteria to judge validity and reliability of qualitative research within the realism paradigm. *Qualitative Market Research: An International Journal*, *3*(3), 118–126.

Hevner, A., & Chatterjee, S. (2010). Design research in information systems. In *Design research in information systems* (Vol. 22, pp. 75–105). London: Springer Science Business Media.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research 1. *Design Science in IS Research MIS Quarterly*, *28*(1), 75–105. http://doi.org/10.2307/25148625

Hill, R. (2014). *Best practices for BYOD: Citibank*. Retrieved July 30, 2016, from https://online.citi.com/US/JRS/pands/detail.do?ID=CitiBizArticleBYOD

Hillard, R. (2014, January). MDM paves the way for the mobilization of apps, content and entire businesses. *Biztech Magazine*, (2), 2.

Hofstede, G. (1981). Culture and organizations. *International Studies of Management & Organization*, *10*(4), 15–41. http://doi.org/Article

Hofstede, G. (2010, September). Geert Hofstede: An interview with a pioneer. *Sietar Europa*, pp. 2–6. Michigan, USA.

Hofstede, G., Neuijen, B., Ohayv, D. D., & Sanders, G. (1990). Measuring organizational cultures: A qualitative and quantitative study across twenty cases. *Administrative Science Quarterly*, *35*(2), 286.

Hofstee, E. (2006). *Constructing a good dissertation: A practical guide to finishing a master's, MBA or PhD on schedule*. Johannesburg: Exactica.

Hogg, B. (2013). *How to build your organizational culture based on trust and collaboration* (Vol. 5). Ontario, Canada: Bill Hogg & Associates.

Hopf, T. (2010). The logic of habit in international relations. *European Journal of International Relations*, *16*(4), 539–561.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Journal of the Decision Science Institute*, *43*(4), 615–660.

IBM. (2015). *Enterprise mobility trends 2015 and beyond*. London: IBM.

Ionides, N. (2002). Future imperfect. *Airline Business*, *2002*(2), 32. http://doi.org/10.1109/MIC.2010.12

ISACA.org. (2009). *An introduction to the business model for information security*. Rolling Meadows, IL: ICASA.

Jabangwe, J., & Kadenge, P. (2013). An Investigation of the relationship between capital levels and the performance of banks in Zimbabwe from 2009 to 2013. *Botswana Journal of Economics*, *3*(2), 68–86.

Jack, W., & Suri, T. (2011). *Mobile money: The economics of M-Pesa* (NBER Working Paper Series). Massachusetts **:** M-Pesa.

Jay Gordon. (2015). *Top 3 mobility trends for 2016*. Retrieved July 26, 2016, from https://enterprisemobile.com/top-3-mobility-trends-for-2016/

Johnson, M. E., & Goetz, E. (2007). Embedding information security into the organization. *IEEE Security and Privacy*, *5*(3), 16–24.

Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed methods research: A research paradigm whose time has come. *Educational Researcher*, *33*(7), 14–26.

Johnson, R. B., Onwuegbuzie, A. J., & Turner, L. A. (2007). Toward a Definition of mixed methods research. *Journal of Mixed Methods Research*, *1*(2), 112–133.

Johnson, S. (2013). Bringing IT out of the shadows. *Network Security*. London: Elsevier.

Kaufman, S. (2014). *2014 Trends to Watch : Telecoms Market*.

Kershenbaum, R. (2012). *Introduction to PayPal*. New York**:** PayPal.

Keyes, J. (2013). *Bring your own devices (BYOD) survival guide* (Vol. 6). http://doi.org/10.1201/b14050

Khatib, T. M. (1997). *Organizational culture, subcultures, and organizational commitment* (Dissertation Abstracts International Section A: Humanities and Social Sciences). Iowa State University.

King, B. (2012). *Bank 3.0: Why banking is no longer somewhere you go, but something you do* (3rd ed.). New York: Marshall Cavendish Business.

Klein, H. K., & Myers, M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly*, *23*(1), 67.

Köffer, S., & Fielt, E. (2015). IT consumerization and its effects on it business value, IT capabilities, and the IT function. *PACIS 2015 Proceedings*, *3*(2), 17.

Koh, K., Ruighaver, a., Maynard, S., & Ahmad, a. (2005). Security Governance : Its Impact on Security Culture. *Proceedings of The Third Australian Information Security Management Conference*, 1–12. Retrieved from http://igneous.scis.ecu.edu.au/proceedings/2005/aism/koh.pdf

Kołakowski, L. (1972). *Positivist philosophy from Hume to the Vienna Circle*. Retrieved August 24, 2017, from https://philpapers.org/rec/KOAPPF

Krauss, S. E., & Putra, U. (2005). Research paradigms and meaning making: A primer. *The Qualitative Report*, *10*(4), 758–770.

Kritzinger, E., & Von Solms, B. (2012). A framework for cyber security in Africa. *Journal of Information Assurance & Cybersecurity*, 1–10.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers and Security*, *25*(4), 289–296. http://doi.org/10.1016/j.cose.2006.02.008

Kufandirimbwa, O., Zanamwe, N., Hapanyengwi, G., & Kabanda, G. (2013). Mobile money in Zimbabwe: Integrating mobile infrastructure and processes to organisation infrastructure and processes. *Online Journal of Social Sciences Research*, *2*(4), 92–110.

Kuhn, T. S. (1970). *The structure of scientific revolutions*. *Philosophical review* (2nd Editio, Vol. II). Berkeley, CA: International Encyclopedia of Unified Science.

Kuusisto, T., & Ilvonen, I. (2003). Information security culture in small and medium size enterprises. *Frontiers of E-Business Research*, 431–439.

Lanaj, K., Johnson, R. E., & Barnes, C. M. (2014). Beginning the workday yet already depleted? Consequences of late-night smartphone use and sleep. *Organizational Behavior and Human Decision Processes*, *124*(1), 11–23.

Lange, P., & Lancaster, H. (2014). *2014 Africa: Mobile broadband market.* Retrieved April 24, 2015, from http://www.budde.com.au/Research/Africa-Mobile-Broadband-Market.html?r=51

Larryfurst. (2013). BYOD = “Bring Your Own Device?” or “Bring Your Own Disaster?” Retrieved July 30, 2016, from http://www.nstsystems.com/byod-bring-your-own-device-or-bring-your-own-disaster/

Laszlo, A., & Krippner, S. (1998). Systems theories: Their origins, foundations, and development. In J. S. Jordan (Ed.), *Systems theories and a priori aspects of perception* (Vol. 126, pp. 47–74). Amsterdam: Elsevier.

Leavitt, N. (2011). Mobile security: Finally a serious problem? *Computer*, *44*(6), 11–14. http://doi.org/10.1109/MC.2011.184

Leclercg-Vandelannoitte, A. (2015). Information technology & people article information. *Information Technology & People*, *28*(1), 2–33.

Lee, C., Lee, C. C., & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. *Computers and Security*, *59*, 60–70. http://doi.org/10.1016/j.cose.2016.02.004

Leedy, P. D., & Ormrod, J. E. (2010). *Practical research: Planning and design* (9th ed.). Boston, MA: Pearson Education.

Leetham, D. (2016). Rapid research methods for nurses, midwives and health professionals. *Nursing Standard, 30*. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=c8h&AN=116905483&lang=es&site=ehost-live

Lennon, R. G. (2012). Bring your own device (BYOD) with Cloud 4 education. In *Proceedings of the 3rd annual conference on Systems, programming, and applications: Software for humanity* (Vol. 3, p. 171).

Lichtman, M. (2014). *Qualitative research for the social sciences*. Boston: Sage Publications.

Lim, J. J. S., Ahmad, A., Chang, S., & Maynard, S. B. (2010). Embedding information security culture emerging concerns and challenges. *Pacis 2010*, *6*(2), 463–474.

Lim, J. S., Chang, S., Maynard, S. B., & Ahmad, A. (2009). Exploring the relationship between organizational culture and information security culture. In *7th Australian Information Security Management Conference* (pp. 88–97). Melbourne: Australian Information Security Management Conference.

Liu, Y., Kiley, J., & Ballard, H. (2006). *The relationship between organisational culture and effectiveness in the Western Cape banking industry*. Cape Peninsula University.

Lucca, D., Seru, A., & Trebbi, F. (2014a). *The revolving door and worker flows in banking regulation*. *Journal of Monetary Economics* (Vol. 65). New York, NY: .

Lucca, D., Seru, A., & Trebbi, F. (2014b). *The revolving door and worker flows in banking regulation*. *Journal of Monetary Economics* (Vol. 65).Econstor: New York, NY.

Lund, D., & Silva, J. (2015). *Financial services optimizing BYOD Strategies for success*. Retrieved from http://www.business.att.com/content/whitepaper/optimizing-byod-strategies-for-success-whitepaper.pdf

Lundy, O., & Cowling, A. (1996). *Strategic human resource management*. *London Routeledge* (6th Editio). London: London:Routledge.

Lunenburg, F. C. (2011). The generation and verification of theory: A bridge to the continuing quest for a knowledge base. *National Forum of Educational Administration and Supervision Journal*, *29*(4), 1–9.

Mack, L. (2010). The philosophical underpinnings of educational research. *Polyglossia*, *19*(3), 5–11.

Magdalena, D., Fotache, D., Munteanu, A., & Dospinescu, O. (2009). Transforming organisational culture through the impact of information integration. *Communication of the IBIMA*, *8*(1), 137–141.

Mambondiani, B. L., Zhang, Y., & Arun, T. (2014). *Corporate governance and bank performance: Evidence from Zimbabwe*. Manchester: .

Marczyk, G. R., DeMatteo, D., & Festinger, D. (2010). *Essentials of research design and methodology* (2nd ed.). New Jersey: John Wiley & Sons.

Marjani, A. B., & Forouzanfar, L. (2012). A comparative study of organizational culture in Saderat bank and Eghtesad Novin bank of Iran based on Denison â€™ s model. *International Journal of Business and Social Science*, *3*(11), 299–307.

Markus, M. L., & Robey, D. (1988). Information technology and organizational change: Causal structure in theory and research. *Management Science, 34*. INFORMS.

Martins, A., & Eloff, J. (2002). *Security in the information society*. In M. A. Ghonaimy, M. T. El-Hadidi, & H. K. Aslan, (Eds.)(Vol. 86). Boston, MA: Springer. http://doi.org/10.1007/978-0-387-35586-3

Martins, E. C., & Terblanche, F. (2003). Building organisational culture that stimulates creativity and innovation. *European Journal of Innovation Management*, *6*(1), 64–74.

Matsumoto, D. (2007). Culture, context, and behavior. *Journal of Personality*, *75*(6), 1285–1320.

Maximini, D. (2015). *The scrum culture*. Geneva, Switzerland: Springer International.

McDermid, D. (2006). Pragmatism *Internet Encyclopedia of Philosophy*. Retrieved from http://www.iep.utm.edu/pragmati/

McDermott, T. (2004). *Culture in banking.* Speech to the BBA July. London: Financial Conduct Authority.

McGrath, K. M. (2003). *Organizational culture and information systems implementation: A critical perspective*. Information Systems Department, London School of Economics and

Political Science.

Mehri, B., & Yeganeh, E. (2015). *The impact of national and organizational culture on information technology (IT) Abstract.* Karaj.

Michalow, M. J. (2016). *Analysis of the impact of technological advances on financial institutions*. Utica College.

Microsoft. (2016). *Consumerisation of IT.* Retrieved February 6, 2017, from http://www.slideserve.com/jasia/consumerization-of-it

Mir, S. Z. (2014). Towards Understanding The Impact Of Organizational Culture And Risk Management In Banking Sector In Developing Countries, 1–65.

Mobile Iron. (2014). *The ultimate guide to BYOD*.. California: MobileIron.

Mohanty, A. (2015). Effective team building, organisational culture and organisational climate in service sector: A study with special reference to hotels in Odisha Ashish Mohanty. *International Journal of English Language, Literature and Humanities*, *3*(7), 499–516.

Montesdioca, G. P. Z., & Maçada, A. C. G. (2015). Measuring user satisfaction with information security practices. *Computers & Security*, *48*(2), 267–280.

Morris, J., Marzano, M., Dandy, N., & O'Brien, L. (2012). *Theories and models of behaviour and behaviour change*. London: Forest Research.

Moschella, D., Neal, D., Opperman, P., & Taylor, J. (2004). *The "consumerization" of information technology* (Position paper). London: CSC's Research & Advisory Services.

Mphahlele, P. (2016). *The impact of Bring-your-own-device on work practices in the financial sector Information*. University of Cape Town.

Munteanu, A.-B., & Fotache, D. (2015). Enablers of information security culture. *Procedia Economics and Finance*, *20*(15), 414–422.

Murthy, N. R. N. (2009). *Enhancing Trust*. *Infosys Annual Report*. London: Inforsys.

Musarurwa, A., & Jazri, H. (2015). A proposed framework to measure growth of critical information infrastructure protection in Africa. In *Proceedings of 2015 International Conference on Emerging Trends in Networks and Computer Communications, ETNCC 2015* (pp. 85–90). Windhoek Namibia: IEEE.

Myers, M., & Avison, D. (2002). Qualitative research in information systems. *Management Information Systems*, *21*(2), 241–242.

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and Organization*, *17*(1), 2–26.

Nayak, N., Nath, V., & Goel, N. (2014). A study of adoption behaviour of mobile banking services by Indian consumers. *IMPACT: International Journal of Research in Engineering & Technology*, *2*(3), 209–222.

Ndlovu, M. W., Bhiri, T., Mutambanadzo, T., & Hlahla, B. P. (2013). A comparative analysis of the corporate governance practices in multinational and domestic banks in Zimbabwe. *Journal of Emerging Trends in Economics and Management Sciences Zimbabwe Journal of Emerging Trends in Economics and Management Sciences (JETEMS)*, *4*(45), 473–480.

Neuman. (1997). *Social research methods*. Oxford University Press. Retrieved from https://global.oup.com/academic/product/social-research-methods-9780199689453?cc=us&lang=en&

Ngo, L., Zhou, W., & Warren, M. (2005). Understanding transition towards information security culture change. In *Proceeding of the 3rd Australian Computer, Network & Information Forensics Conference, Edith Cowan University, School of Computer and Information Science* (pp. 67–73). Perth, Australia.

Nguyen, D. K. (2014). *Organizational culture: A case study of Standard Chartered Bank (Vietnam) Ltd*. Turku University of Applied Sciences.

Niehaves, B., Köffer, S., & Ortbach, K. (2012). IT Consumerization: A theory and practice review. In AMCIS (Ed.), *Americas Conference on Information Systems (AMCIS)* (Vol. Paper 18, pp. 1–9). Seatle, Washington.

Niehaves, B., Köffer, S., & Ortbach, K. (2013). The effect of private IT use on work performance: Towards an IT consumerization theory. In *11th International Conference on Wirtschaftsinformatik,* (Vol. 1, p. S.39-54). Leipzig, Germany.

Nilsen, P. (2015). Making sense of implementation theories, models and frameworks. *Implementation Science*, *10*(1), 53.

Nonaka, I. (1994). A dynamic theory knowledge of organizational creation. *Organization Science*, *5*(1), 14–37.

O'Donovan, G. (2004). *The corporate culture handbook*. New York, NY: Business Summaries.

Oates, B. J. (2006). *Researching Information systems and computing: Inorganic chemistry* (Vol. 37). London: Sage Publications.

Ojiako, U., Manungo, T., Chipulu, M., & Johnson, J. E. (2010). *The impact of regulation on risk perception: evidence from the banking industry* (Vol. 25). Johannesburg.

Olalere, M., Abdullah, M. T., Mahmod, R., & Abdullah, A. (2015). A review of bring your own device on security issues. *SAGE Open*, *5*(2), 11.

Olson, M. H. (1982). New Information Technology and Organizational Culture New information Technology and Organizational Culture. *MIS Quarterly*, *6*(4), 71–92.

Ovum. (2014). *Beyond BYOD: How businesses might COPE with mobility – Identifying the right mobility strategy for your organization*. London: Ovum.

Oxford University. (2015). *Oxford Business English Dictionary for learners of English*. *Oxford University*. London: Oxford University Press.

Ozigbo, N. C. (2013). Impact of organizational culture and technology on firm performance in the service sector, University of Abuja , Nigeria. *Communication of the IIMA*, *13*(1), 69–82.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. In *Proceedings of the Annual Hawaii International Conference on System Sciences* (pp. 1–10). Honolulu, Hawaii.

Pallant, J. (2011). *SPSS Survival Manual*. *A Step by Step Guide to Data Analysis using SPSS* (4th ed.). Crowns Nest,Australia: Allen and Unwin.

Peffers, K. E. N., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, *24*(3), 45–77. http://doi.org/10.2753/MIS0742-1222240302

Peffers, K., Rothenberger, M., Tuunanen, T., & Vaezi, R. (2012). Design science research evaluation. *Design Science Research in Information Systems. Advances in Theory and Practice*, *1*(3), 398–410.

Pelino, M., Kane, C., Koetzle, L., Christopher, & Voce, Caputo, M. (2014). *Research: Building The business case for a bring-your-own-device (BYOD) program*.

Perry, C., Riege, A., & Brown, L. (1999). *Irish Marketing Review*. *Enhancing Marketing Throught and Practice* (2nd ed., Vol. 12). Dublin: Mercury Publications.

Pfeffer, J., & Salancik, G. R. (2003). *The external control of organizations: A resource dependence perspective* (3rd ed.). Stanford, CA: Stanford Business Classics. http://doi.org/10.2307/2392573

Puhakainen, P. P., & Siponen, M. (2010). Improving employee' compliance through information systems security training: An action research study. *MIS Quarterly*, *34*(4), 757–778.

Punch, K. F. (2006). *Developing effective research proposals essential resources for social research* (3rd ed.). London: Sage Publications.

PwC. (2013). *Transform your bank's operations model: A best practices discussion*. Booz and Company Strategy. Chicago: PwC.

PwC. (2011). *The consumerization of IT -The next-generation CIO*.

PwC. (2015). *Bring your own device (BYOD) and customer data protection: Are you ready? C*ontracting Business. London: PwC.

Rahmani, T., & Ghorbani, M. (2015). The relationship among organizational culture in Denison's Model *(Adaptability) with Creative Thinking,3*(3), 793–802.

Rajasekar, S., Philominathan, P., & Chinnathambi, V. (2013). Research methodology. *Methods*, *68*(1), 25–39. http://doi.org/http://196.29.172.66:8080/jspui/bitstream/123456789/2574/1/Research%20Methodology.pdf

Rajendran, A., Furnell, S. M., & Gabriel, T. (2009). Factors Affecting Information Security Behaviour, 42–49.

Rasid, S. Z. A., Manaf, M. A. A., & Quoquab, F. (2013). Leadership and organizational commitment in the Islamic banking context: The role of organizational culture as a mediator. *American Journal of Economics*, *3*(5), 171–176.

RBZ. (2014). *Reserve Bank of Zimbabwe Banking Sector Report for Quarter Ended 31 March 2014*. Harare, Zimbabwe: RBZ.

Rees, C. (2011). *An introduction to research for midwives* (3rd ed.). Cardif, Wales: Elsevier Health Sciences. http://doi.org/9780750653510

Renaud, K., Flowerday, S., Othmane, L., & Volkamer, M. (2015). " I Am Because We Are ": Developing and Nurturing an African Digital Security Culture. In *Proceedings of the African Cyber Citizenship Conference 2015 Port Elizabeth, 2-3 November 2015 (http://accconference.nmmu.ac.za) ISBN: 978-1-920508-67-8* (pp. 94–104). Port Elizabeth.

Richey, R. C., & Klein, J. D. (2014). Design and development research. In M. Spector, M. D. Merrill, J. Elen, & M. J. Bishop (Eds.), *Handbook of research on educational communications and technology* (pp. 141–150). New York/Heidelberg: Springer. http://doi.org/10.1007/978-1-4614-3185-5_12

Riege, A. M. (2003). Validity and reliability tests in case study research: A literature review with "hands-on" applications for each research phase. *Qualitative Market Research: An International Journal*, *6*(2), 75–86.

Robbie Westacott. (2014). *Mobile technology in banking and finance.* Retrieved July 6, 2017, from http://www.enterprisemobilityexchange.com/eme-cloud/articles/Mobile-Technology-Banking-and-Finance

Robbins, S. T., Judge, T. A., & Hasham, E. S. (2009). *Organizational behavior*.. Essex, England: Pearson Education.

Robson, C. (2015). *Real world research: A resource for users of social research methods in applied settings* (4th ed.). Wiley-Blackwell.

Roer, K. (2015). *Build a security culture*. England: IT Governance Publishing.

Ross, S. J., & Masters, R. (2005). Creating a culture of security. *ISACA Journal* (Vol. 18). Rolling

Meadows, USA.

Rossman, G. B., & Rallis, S. F. (2011). An Introduction to Qualitative Research. Learning in the Field. SAGE Publications. SAGE.

Rossman, G. B., & Rallis, S. F. (2011). *An Introduction to Qualitative Research. Learning in the Field. SAGE Publications*. SAGE.

Rumelt, R. P., Schendel, D., & Teece, D. J. (1991). Strategic management and economics. *Strategic Management Journal*, *12*(S2), 5–29.

Russo, S. M. (2011). *Consumerization of IT*. London: Gartner.

Sadeghi, T., & Farokhian, S. (2011). Services quality model for online banking services by behavioral adoption theories and comparative study. *African Journal of Business Management*, *5*(11), 4490–4499.

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, *57*(3), 442–451.

Salkind, N. (2010). *Encyclopedia of research design*. California: Sage Publications.

Salvi, V., & Kadam, A. W. (2014). Information security management at HDFC Bank: Contribution of seven enabler*s. COBIT Focus, 1*.

Santomero, A. (1997). Risk in banking and capital regulation. In *Wharton Financial Institutions Center Conference on Risk Management in Banking* (Vol. 43, pp. 1219–1233). London: Wharton School.

Sathyan, J., Anoop, Narayan, N., & Vallathai, S. K. (2016). *A comprehensive guide to enterprise mobility*.. Boca Raton, FL: CRC Press.

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research methodology* (5th ed.). Harlow, UK: Pearson Education.

Scarfo, A. (2012). New security perspectives around BYOD. In *Proceedings – 2012 7th International Conference on Broadband, Wireless Computing, Communication and Applications, BWCCA 2012* (pp. 446–451). Victoria, Canada: IEEE Computer Society Press.

Schadler, T., Yates, S., & Wang, N. (2013). *2013 mobile workforce adoption trends*. Retrieved March 4, 2017, from https://www.forrester.com/report/2013+Mobile+Workforce+Adoption+Trends/-/E-RES89442

Schein, E. (1999). *Sense and nonsense about culture and climate*. Michigan: MIT Sloan School of Management..

Schein, E. H. (1988). *Organizational culture*. Boston, MA: American Psychological Association.

Schein, E. H. (1990). Organizational culture. *American Psychologist*, *45*(2), 109–119. http://doi.org/10.1037/0003-066X.45.2.109

Schein, E. H. (2009). *The corporate culture survival guide*. San Francisco, CA: Jossey Bass.

Schlienger, T., & Teufel, S. (2003). Information security culture: From analysis to change. *South African Computer Journal*, *31*, 46–52.

Schuman, S. (2006). *Organizational culture: The effect of behavior on performance*. New York: GE Capital.

Selamat, M. H., & Babatunde, D. A. (2014). Mediating effect of information security culture on the relationship between information security activities and organizational performance in the Nigerian banking setting. *International Journal of Business and Management*, *9*(7), 33–38.

Sharfman, M. P., & Dean, J. W. (1991). Conceptualizing and measuring the organizational environment: A multidimensional approach. *Journal of Management*, *17*(4), 681–700.

Shrier, D., Canale, G., & Pentland, A. (2016). *Mobile money & payments: Technology trends*. Boston, MA: Massachusetts Institute of Technology.

Shumate, T., & Ketel, M. (2014). Bring your own device: Benefits, risks and control techniques. In *Ieee Southeastcon 2014* (pp. 1–6). Baltimore: IEEE.

Silic, M., & Back, A. (2014). Shadow IT: A view from behind the curtain. *Computers and Security*, *45*, 274–283.

Singh, M. N., & Phil, M. (2012). BYOD: Genie Is out of the bottle – “devil or angel.” *Journal of Business Management & Social Sciences Research*, *1*(3), 1–12.

Smith, J. M., & Levins, R. (1970). Evolution in changing environments. *Population Studies, 24*. http://doi.org/10.2307/2173276

Sobers, A. (2014). *BYOD and the Mobile Enterprise: Organisational challenges and solutions to adopt BYOD*. *Computers and Society*. Ithaca, New Yourk.

Sobh, R., & Perry, C. (2006). Research design and data analysis in realism research. *European Journal of Marketing*, *40*(11/12), 1194–1209.

Sohal, P. (2014). *Top 10 Mobility and IT trends in the banking indus...* -Hewlett Packard Enterprise Community. Retrieved July 29, 2016, from http://community.hpe.com/t5/Enterprise-Services/Top-10-Mobility-and-IT-Trends-in-the-Banking-Industry/ba-p/6795009#.V5rpjnkkoid

Song, Y., & Kong, S. C. (2017). Affordances and constraints of BYOD (bring your own device) for learning and teaching in higher education: Teachers’ perspectives. *The Internet and Higher Education*, *32*(August), 39–46.

Stephanou, A., & Dagada, R. (2014). The impact of information security awareness training on information security behaviour: The case for. *Information Security*, *1*(2), 309–330.

Strang, D., & Aldrich, H. (2002). Organizations evolving. *Contemporary Sociology, 31*. http://doi.org/10.2307/3089484

Sun, S. (2008). Organizational culture and its themes. *International Journal of Business and Management*, *3*(12), 137–141.

Symantec. (2012). *2012 Norton cybercrime report*. Massachusetts.

Taljaard, L. (2016). How to succeed in your master's and doctoral studies: A South African guide and resource book, Johann Mouton : book review, (September), 280.

Terre Blanche, M., Durrheim, K., & Painter, D. (2006). *Research in practice: Applied methods for the social sciences*. (2nd ed.). Cape Town: Cape Town: UCT Press. Retrieved from http://pins.org.za/pins35/pins35_bookreview03_Wilbraham.pdf

Thakor, A. (2015). *Corporate culture in banking*. Washington University.

Tharenou, P., Donohue, R., & Cooper, B. (2007). *Management research methods*. London: Cambridge University Press.\

Tharp, B. M. (2009). Defining " Culture " and " Organizational Culture ": From Anthropology to the Office. *Interpretation a Journal of Bible and Theology*, 1–5.

Thomson, G. (2012). BYOD: Enabling the chaos. *Network Security*, *2012*(2), 5–8. http://doi.org/10.1016/S1353-4858(12)70013-2

Thomson, K. L. (2007). *MISSTEV: Model for information security shared tacit espoused values*. Nelson Mandela Metropolitan University.

Thomson, K. L., & Von Solms, R. (2005). Information security obedience: A definition. *Computers & Security*, *24*(1), 69–75.

Thomson, K. L., Von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud and Security*, (10), 7–11.

Trend Micro. (2012). *The consumerization of iT*. *Digital Spotlight*. Dallas.

Trompenaars, F., & Hampden Turner, C. (2008). *Riding the waves of change together: Are we all paying attention?*. London, UK: Nicholas Brearley.

Trompenaars and Turner. (1997). *Riding the waves of culture* (2nd ed.). London: Nicholas Brearley.

Tsoukas, H. (1989). The validity of idiographic research explanations. *The Academy of Management Review*, *14*(4), 551.

Twinomurinzi, H., & Mawela, T. (2014). Employee perceptions of BYOD in South Africa: Employers are turning a blind eye? *South African Institute of Computer Scientists and Information*, 1–6.

Udeh, I., & Dhillon, G. (2008). An analysis of information security governance structures: The case of Société Générale Bank. *Information Assurance ASIA'08*, *1*(2), 41.

Ula, M., Ismail, Z., & Sidek, Z. (2011). A framework for the governance of information security in banking system. *Journal of Information Assurance & Cybersecurity*, *23*(8), 1–12.

Ullman, E. (2011). BYOD and security. *Tech & Learning, 31*.

Vallerand, R. J., Deshaies, P., Cuerrier, J.-P., Pelletier, L. G., & et al. (1992). Ajzen and Fishbein's theory of reasoned action as applied to moral behavior: A confirmatory analysis. *Journal of Personality and Social Psychology*, *62*(1), 98–109.

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers and Security*, *29*(4), 476–486. http://doi.org/10.1016/j.cose.2009.10.005

Van Niekerk, J., & Von Solms, R. (2005). A holistic framework for the fostering of an information security sub-culture in organizations. In *International Information Security South Africa Conference (ISSA)* (pp. 1–13). Johannesburg, South Africa.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information and Management*, *49*(3–4), 190–198. http://doi.org/10.1016/j.im.2012.04.002

Vignesh, U., & Asha, S. (2015). Modifying security policies towards BYOD. *Procedia Computer Science*, *50*, 511–516.

VMware. (2016). Bank IT Leaders reveal 4 reasons why they are driving change: VMware End-User Computing Blog -VMware Blogs. Retrieved July 30, 2016, from http://blogs.vmware.com/euc/2016/04/bank-it-leaders-reveal-4-reasons-why-they-are-driving-change.html

Von Bertalanffy, L. (1950). An outline of general system theory. *The British Journal for Philosophy of Science*, *1*(2), 134–165.

Von Roessing, R. M. (2010). *The Business model for information security*. *Information Security*. Rolling Meadows, USA.

Von Solms, B. (2006). Information security: The 4th wave. *Journal of Theoretical and Applied Information Technology*, *43*(1), 1–7.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*, 97–102. http://doi.org/10.1016/j.cose.2013.04.004

Von Solms, R., & Von Solms, B. (2004). From policies to culture. *Computers and Security*, *23*(4), 275–279.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers and Security*, *23*(3), 191–198.

Wahyuni, D. (2012a). Deakin Research Online. *Asian Academy of Management Journal*, *18*(1), 3–19. http://doi.org/10.1675/1524-4695(2008)31

Wahyuni, D. (2012b). The research design maze: Understanding Paradigms, cases, methods and methodologies. *Journal of Applied Management Accounting Research*, *10*(1), 69–80.

Waisfisz, B. (2010). *An organisational cultural perspective*. Amsterdam: *ITIM International*.

Wang, Y., Wei, J., & Vangury, K. (2014). Bring your own device security issues and challenges. In *IEEE 11th Consumer Communications and Networking Conference (CCNC)* (Vol. 3, pp. 80–85). Las Vegas, NV, USA: IEE Digital Library.

Watson, J. C., & Flamez, B. (2015). *Counseling assessment and evaluation: Fundamentals of applied practice* (2nd ed.). Texas: Sage Publications.

Weaver, K., & Olson, J. K. (2006). Understanding paradigms used for nursing research. *Journal of Advanced Nursing*, *53*(4), 459–469. http://doi.org/10.1111/j.1365-2648.2006.03740.x

Weber, R. (2012). Evaluating and developing theories in the information systems discipline. *Journal of the Association for Information Systems*, *13*(1), 1–30.

Whitbeck, C., & Bhaskar, R. (1977). *A realist theory of science: The philosophical review* (3rd ed.). London: Routledge. http://doi.org/10.2307/2184170

Williams, B., Onsman, A., & Brown, T. (2010). Australian paramedic graduate attributes: A pilot study using exploratory factor analysis. *Emergency Medicine Journal: EMJ*, *27*(10), 794–799.

Williams, B., Onsman, A., & Brown, T. (2012). A Rasch and factor analysis of a paramedic graduate attribute scale. *Evaluation & the Health Professions*, *35*(2), 148–168.

Woodill, G. (2012). Managing mobile in the corporate environment | Float Mobile Learning. Retrieved May 14, 2015, from http://floatlearning.com/2012/11/managing-mobile-in-the-corporate-environment/

Woretaw, A., & Lessa, L. (2012). *Information security culture in the banking sector in Ethiopia*. Addis Ababa.

Yin, R. K. (2004). Case study methods. *Teaching and Teacher Education*, *5*(4), 355–357. http://doi.org/10.1016/0742-051X(89)90032-2

Yin, R. K. (2010). *Case study: Research design and methods* (2nd ed.). London: Sage

Publications.

Zakari, M., Poku, K., & Owusu-Ansah, W. (2013). Organizational Culture and organisational performance: Empirical evidence from the banking industry in Ghana. *International Journal of Business, Humanities and Technology*, *3*(1), 95–107.

Zakaria, O. (2004). Understanding challenges of information security culture: A methodological issue. *2nd Australian Information Security Management Conference*, *2*(3), 83–93.

Zakaria, O., Gani, A., Nor, M. M., & Anuar, N. B. (2007). Reengineering Information security culture formulation through management perspective. *Electrical Engineering*, *2*(June 2016), 638–641.

Zikmund, W. G., Babin, B. J., Carr, J., & Griffin, M. (2013). *Basic and applied research*: *Business research methods* (9th ed.). Sydney: Cengage Learning Australia. Retrieved from http://amzn.com/0030350840

Appendices

Appendix 1: Research Instrument

Appendix 2: Ethical Clearance Certificate

Appendix 3: Clearance from the Bank to Conduct Research

Appendix 4: Correlation Computations

Appendix 5: Multiple Regression Coefficients

Appendix 6: Expert Review Questionnaire

Appendix 1: Research Instrument

University of Fort Hare
Together in Excellence

Department of Information Systems, University of Fort Hare

Questionnaire: A Model for Building an Information Security Culture for the Bring Your Own Device: the case of the unintended administrator

Dear Colleague,

I am a student in the Department of Information Systems at the University of Fort Hare (East London Campus), currently conducting research for my Doctor of Philosophy Degree under the supervision of Prof. Stephen Flowerday and Dr Liezel Cilliers. The focus of the research project is to understand the security culture concerning BYOD (Bring Your Own Device) within the banking industry. BYOD is the practice of allowing the employees of an organisation to use their own computers, smartphones, or other devices for work purposes. The objective of the research project is to build an information security culture around BYOD within the Banking Industry in Zimbabwe.

Your participation in this research study is voluntary. You may choose not to participate. If you decide to participate in this research survey, you may withdraw at any time. If you decide not to participate in this study or if you withdraw from participating at any time, you will not be penalized. We will do our best to keep your information confidential. All data is stored in a password protected electronic format. To help protect your confidentiality, the surveys will not contain information that will personally identify you such as your name, email address or IP address. The results of this study will be used for scholarly purposes only and may be shared with Fort Hare University representatives. If you have any questions about the research study, please contact any of the individuals above. This research has been reviewed according to University of Fort Hare procedures for research involving human subjects.

ELECTRONIC CONSENT: Please select your choice below.

Clicking on the "agree" button below indicates that:

- you have ready the above information
- you voluntarily agree to participate
- you are at least 18 years of age

If you do not wish to participate in the research study, please decline participation by clicking on the "disagree" button.

● Agree

○ Disagree

Looking forward to your responses.

Yours sincerely

Mr. Alfred Musarurwa

Contact Information

Mr. A. Musarurwa

PhD Student

Department of Information Systems

University of Fort Hare

Email: 201515333@ufh.ac.za

Phone: +263 772 644 756

Supervisor/s
Professor. S. Flowerday

Dr L. Cilliers
Department of Information Systems
University of Fort Hare

Emails: sflowerday@ufh.ac.za

Section 1: Demographics

1. What is your gender?
    - Male

- Female

2. Indicate your age.
    - < 30 years
    - 30-40 years
    - 41-50 years
    - > 50 years
3. How long have you been employed?
    - <5 years
    - 5-10 years
    - 11-15 years
    - > 15 years
4. The information that I deal with:
    - Is extremely confidential (where confidentiality is enforced by the RBZ)
    - Have sensitive details about internal operations of the bank.
    - Is sensitive but mostly functional.
    - General and not damaging to the bank.
5. Which of the following devices do you own?
    - Smartphone
    - Tablet
    - Laptop
    - Desktop
    - USB/Flash drive
    - Hard Disk Drive/External Hard Drive
6. Are you accessing any of the following services from your personal device? (Select one or more options).
    - Access email
    - Make work related phone calls
    - Access the company's non-banking systems

- Access the company’s banking systems
- Work Calendar

Knowledge-I am knowledgeable of the following regarding the use of BYOD in my work place

7.	Using a personal device at work would allow me access to all the information I require in order to perform my job satisfactorily.	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
		1	2	3	4	5
8.	Using personal devices to perform my tasks at work will not affect the quality of my work or how I interact with customers or colleagues.	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
		1	2	3	4	5
9.	There is a growing demand from employees for the use of personal devices in the banking environment to allow unmonitored access to information and systems.	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
		1	2	3	4	5
10.	Banks that allow employees to bring their own devices are more Information Security conscious than those that do not.	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
		1	2	3	4	5
11.	Technological innovation must be in the bank’s objectives in order for BYOD to be successfully ingrained into company culture.	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
		1	2	3	4	5
12.	I understand the distinction between personal and organisational data and am able to keep them wholly separate while using a personal device for work				YES	NO
13.	I think that the nature of my industry is such that the information is too sensitive to allow	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

	employees to bring and use their own devices for company business.	1	2	3	4	5

Attitude

14.	I am willing to use my personal devices such as smart phone and tablet to conduct the bank's business.	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
		1	2	3	4	5
15.	I feel that using my own devices in the workplace compromises my privacy.	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
		1	2	3	4	5
16.	I will only use my personal devices for work related business where there is a reimbursement policy.	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
		1	2	3	4	5
17.	Being cognisant of the sensitive nature of a bank's information and systems, I believe that if managed well, the advantages of BYOD outweigh the risks in today's modern technological era.	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
		1	2	3	4	5
18.	Do you believe that personal devices are being optimally managed within your bank in order to maximise their benefits while mitigating the information security risks? If not, please give reasons why below.	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
		1	2	3	4	5
19.	I believe that allowing bank employees to bring and use personal devices in the workplace is more beneficial than it is detrimental to their productivity.	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
		1	2	3	4	5

20. I believe allowing employees to bring their own devices will create a more conducive working environment.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	2	3	4	5

21. In light of the nature of my work and industry, the organisation should be able to monitor what I do on my personal device while in the work environment.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	2	3	4	5

22. I am more comfortable in an environment where I am allowed to access some information such as email from a personal device than where I am not.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	2	3	4	5

Habit

23. Are you currently allowed to use personal devices in the work environment for company business?

Yes	No	I don’t know

24. My personal devices are used by family, friends and colleagues when I am at home.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	2	3	4	5

25. Personal and organisational data such as documents and contacts are stored together (are allowed to mix) on my personal devices that I use for work.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	2	3	4	5

26. My personal devices that I use at work are secured by a password or pin to ensure that both the company and my data are protected.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	2	3	4	5

27. If my personal devices are stolen, I have contingency plans in place to ensure that my data does not fall into the wrong hands such as encryption, remote erase or remote disable.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	2	3	4	5

Training

28. Have you ever received training around information security from your employer?

Yes No

29. If you answered yes to question 23 above, did that training involve aspects of information security around BYOD?

Yes No

30. I believe that training is the best way to communicate information security tenets of BYOD to ensure that they are understood and accepted as opposed to using fines, threat of punishment or other coercive methods.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	2	3	4	5

31. There is need for education in order for employees to understand information Security for the successful implementation of BYOD within my organisation.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	2	3	4	5

32. I do not fully understand data ownership policies as defined by my bank such as distinctions between organisational and personal email, social network access and account ownership and business vs. personal contacts and need to be trained in these aspects.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	2	3	4	5

33. I need to be taught how to access organisational resources from BYOD devices

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

	such as email and Customer Relationship Management (CRM) systems even where I am already familiar with these systems/resources in the work environment.	1	2	3	4	5
34.	I could benefit from additional training on information security if my organisation wants to adopt BYOD.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
	Micro Environment					
35.	The environment at my workplace is conducive to bring and use my personal devices (Considering such things as internet connectivity and accessing networked resources).	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
36.	The technologies and applications I use at work are compatible with my personal devices.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
37.	The organisational culture at my place of work is not prohibitive to new technological trends such as BYOD.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
38.	My superiors are comfortable enough with technology to appreciate the benefits of BYOD?	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
39.	My company’s information security policy is supportive of BYOD.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
40.	The information security culture in my organisation is robust enough to enable BYOD	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

	to be implemented successfully without infringing on information security policy.	1	2	3	4	5
41.	Using my personal device for work will not create a risk of sensitive information leaking to outsiders.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5

Governance

42.	There is need for the regulator to examine the implementation of and to have oversight over BYOD in the banking industry.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
43.	Information security policy around BYOD is best governed by putting responsibility in the hands of the employees and only establishing controls for management.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
44.	Accountability for the information security around BYOD must lie with the Risk department and not the IT department for BYOD to be managed successfully.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
45.	Legislation around Data Protection in the finance industry in Zimbabwe is robust enough to mitigate the new risks introduced by BYOD.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
46.	The Data Protection Bill supports privacy on one’s mobile device, can be a hindrance to the successful implementation of BYOD in Zimbabwe.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5

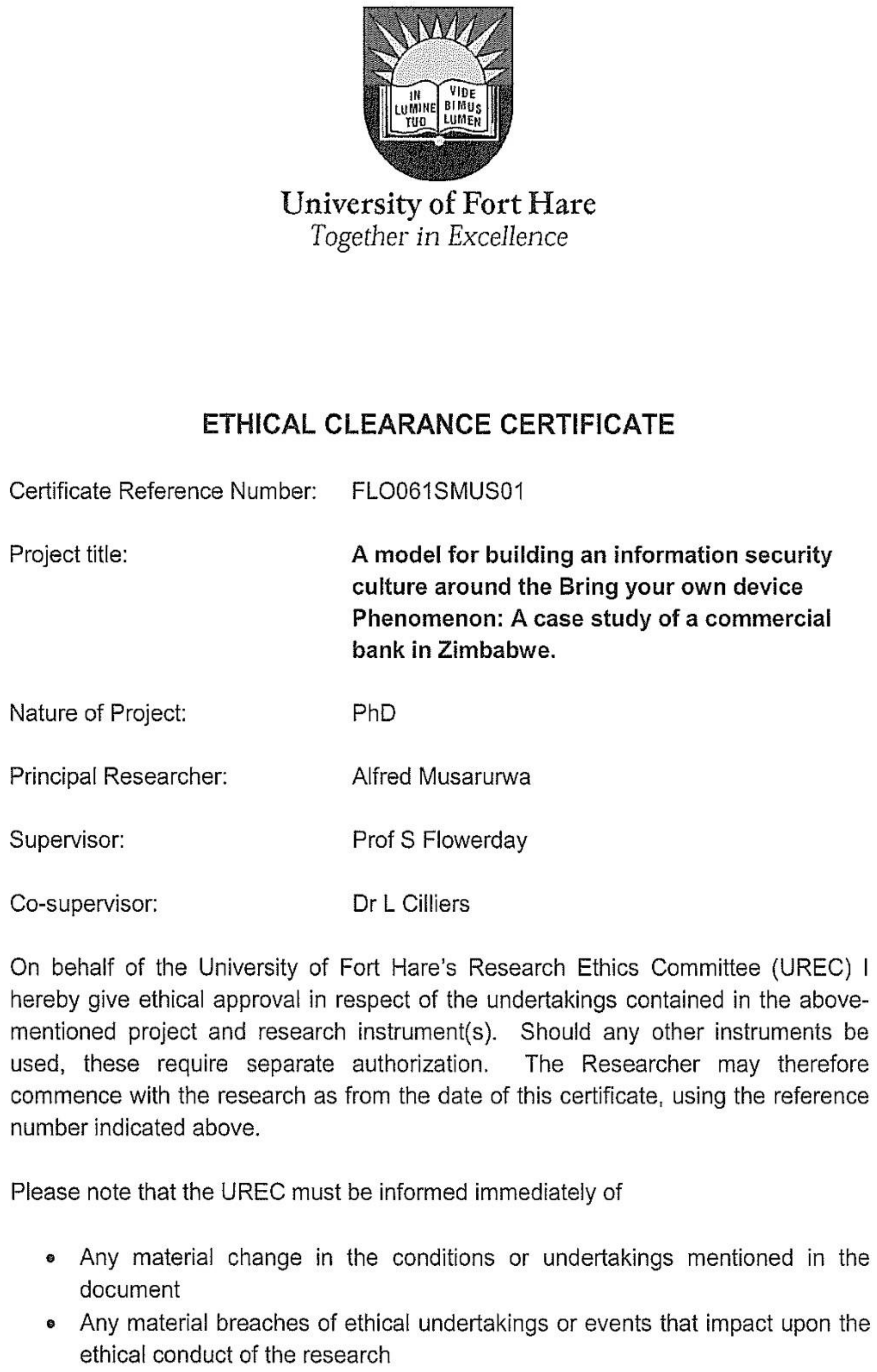
Behavioural intention

47.	I am willing to participate in any activities organised by the bank in order to improve information security around BYOD such as workshops and focus groups.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5

48.	I intend to comply with the bank’s Information Security policies when using my own device for work purposes.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
49.	I am willing to use additional security measures at the bank’s recommendation such as desisting from connecting my personal devices to unsecured public Wi-Fi access points or installing certain applications on devices that I use at work.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
50.	I am willing to invest money in more security measures for my personal devices that I will use at work.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5
51.	I am willing to report any potential breaches of organisational data in my personal devices even when I do not think they pose a risk.	Strongly Agree 1	Agree 2	Neutral 3	Disagree 4	Strongly Disagree 5

52. Please state any other comments regarding BYOD policies in your bank below.

Appendix 2: Ethical Clearance Certificate



University of Fort Hare
Together in Excellence

ETHICAL CLEARANCE CERTIFICATE

Certificate Reference Number:	FLO061SMUS01
Project title:	**A model for building an information security culture around the Bring your own device Phenomenon: A case study of a commercial bank in Zimbabwe.**
Nature of Project:	PhD
Principal Researcher:	Alfred Musarurwa
Supervisor:	Prof S Flowerday
Co-supervisor:	Dr L Cilliers

On behalf of the University of Fort Hare's Research Ethics Committee (UREC) I hereby give ethical approval in respect of the undertakings contained in the above-mentioned project and research instrument(s). Should any other instruments be used, these require separate authorization. The Researcher may therefore commence with the research as from the date of this certificate, using the reference number indicated above.

Please note that the UREC must be informed immediately of

- Any material change in the conditions or undertakings mentioned in the document
- Any material breaches of ethical undertakings or events that impact upon the ethical conduct of the research

The Principal Researcher must report to the UREC in the prescribed format, where applicable, annually, and at the end of the project, in respect of ethical compliance.

Special conditions: Research that includes children as per the official regulations of the act must take the following into account:

Note: The UREC is aware of the provisions of s71 of the National Health Act 61 of 2003 and that matters pertaining to obtaining the Minister's consent are under discussion and remain unresolved. Nonetheless, as was decided at a meeting between the National Health Research Ethics Committee and stakeholders on 6 June 2013, university ethics committees may continue to grant ethical clearance for research involving children without the Minister's consent, provided that the prescripts of the previous rules have been met. This certificate is granted in terms of this agreement.

The UREC retains the right to

- Withdraw or amend this Ethical Clearance Certificate if
  - Any unethical principal or practices are revealed or suspected
  - Relevant information has been withheld or misrepresented
  - Regulatory changes of whatsoever nature so require
  - The conditions contained in the Certificate have not been adhered to

- Request access to any information or data at any time during the course or after completion of the project.

- In addition to the need to comply with the highest level of ethical conduct principle investigators must report back annually as an evaluation and monitoring mechanism on the progress being made by the research. Such a report must be sent to the Dean of Research's office

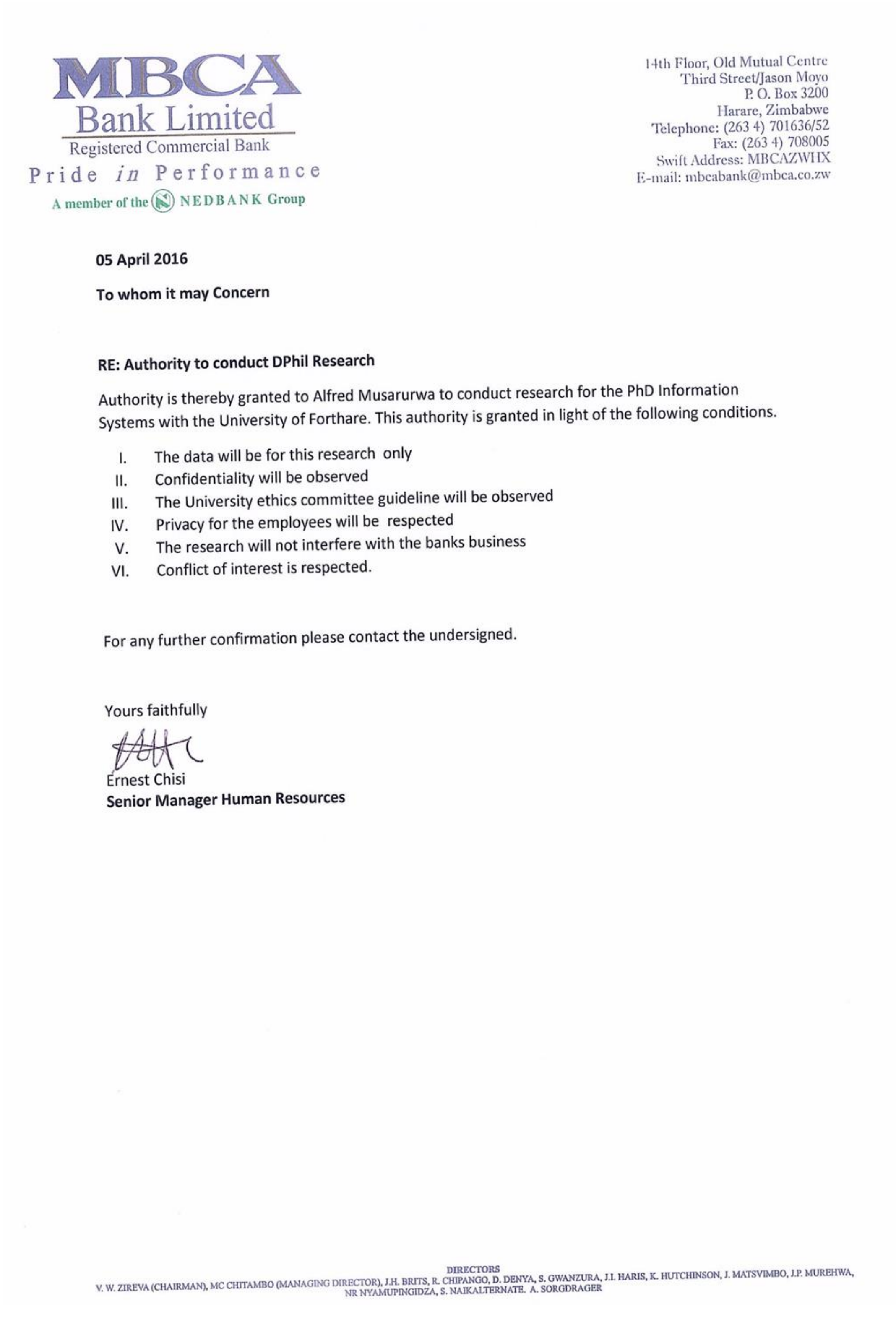
The Ethics Committee wished you well in your research.

Yours sincerely

Professor Gideon de Wet
Dean of Research

08 June 2016

Appendix 3: Clearance from the Bank to Conduct Research



MBCA
Bank Limited
Registered Commercial Bank
Pride *in* Performance
A member of the NEDBANK Group

14th Floor, Old Mutual Centre
Third Street/Jason Moyo
P. O. Box 3200
Harare, Zimbabwe
Telephone: (263 4) 701636/52
Fax: (263 4) 708005
Swift Address: MBCAZWHX
E-mail: mbcabank@mbca.co.zw

05 April 2016

To whom it may Concern

RE: Authority to conduct DPhil Research

Authority is thereby granted to Alfred Musarurwa to conduct research for the PhD Information Systems with the University of Forthare. This authority is granted in light of the following conditions.

I. The data will be for this research only
II. Confidentiality will be observed
III. The University ethics committee guideline will be observed
IV. Privacy for the employees will be respected
V. The research will not interfere with the banks business
VI. Conflict of interest is respected.

For any further confirmation please contact the undersigned.

Yours faithfully

Ernest Chisi
Senior Manager Human Resources

Appendix 4: Correlation Calculations

		ATTITUDE	ENVIRONMENT	TRAINING	HABIT	GOVERNANCE	KNOWLEDGE	Behavioural Intention
ATTITUDE	Pearson Correlation	1	.262**	.270**	-.059	.327**	.108	.317**
	Sig. (2-tailed)		.002	.001	.513	.000	.205	.000
	N	145	138	137	126	132	140	141
ENVIRONMENT	Pearson Correlation	.262**	1	.376**	.045	.350**	.175*	.356**
	Sig. (2-tailed)	.002		.000	.608	.000	.031	.000
	N	138	160	151	135	144	152	154
TRAINING	Pearson Correlation	.270**	.376**	1	.246**	.244**	.189*	.484**
	Sig. (2-tailed)	.001	.000		.004	.003	.019	.000
	N	137	151	161	139	146	153	154
HABIT	Pearson Correlation	-.059	.045	.246**	1	.185*	-.138	.071
	Sig. (2-tailed)	.513	.608	.004		.034	.107	.406

	N	126	135	139	145	132	138	139
GOVERNANCE	Pearson Correlation	.327**	.350**	.244**	.185*	1	.041	.342**
	Sig. (2-tailed)	.000	.000	.003	.034		.618	.000
	N	132	144	146	132	154	147	147
KNOWLEDGE	Pearson Correlation	.108	.175*	.189*	-.138	.041	1	.085
	Sig. (2-tailed)	.205	.031	.019	.107	.618		.292
	N	140	152	153	138	147	163	156
Behavioural Intention	Pearson Correlation	.317**	.356**	.484**	.071	.342**	.085	1
	Sig. (2-tailed)	.000	.000	.000	.406	.000	.292	
	N	141	154	154	139	147	156	165

***. Correlation is significant at the 0.01 level (2-tailed).*

**. Correlation is significant at the 0.05 level (2-tailed).*

Appendix 5: Multiple Regression coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B		Correlations			Collinearity Statistics	
		B	Std. Error	Beta			Lower Bound	Upper Bound	Zero-order	Partial	Part	Tolerance	VIF
1	(Constant)	7.761	2.844		2.729	.007	2.129	13.393					
	ATTITUDE	.047	.032	.123	1.479	.142	-.016	.110	.317	.134	.112	.819	1.221
	ENVIRONMENT	.086	.059	.127	1.476	.143	-.030	.202	.356	.134	.111	.765	1.307
	TRAINING	.434	.100	.381	4.353	.000	.237	.631	.484	.371	.329	.744	1.343
	HABIT	-.077	.107	-.059	-.721	.472	-.290	.135	.071	-.066	-.054	.859	1.164
	GOVERNANCE	.201	.097	.176	2.062	.041	.008	.393	.342	.186	.156	.781	1.280
	KNOWLEDGE	-.046	.095	-.038	-.483	.630	-.234	.142	.085	-.044	-.037	.917	1.090

Dependent Variable: Behavioural Intention

Appendix 6: Expert Review Questionnaire

University of Fort Hare
Together in Excellence

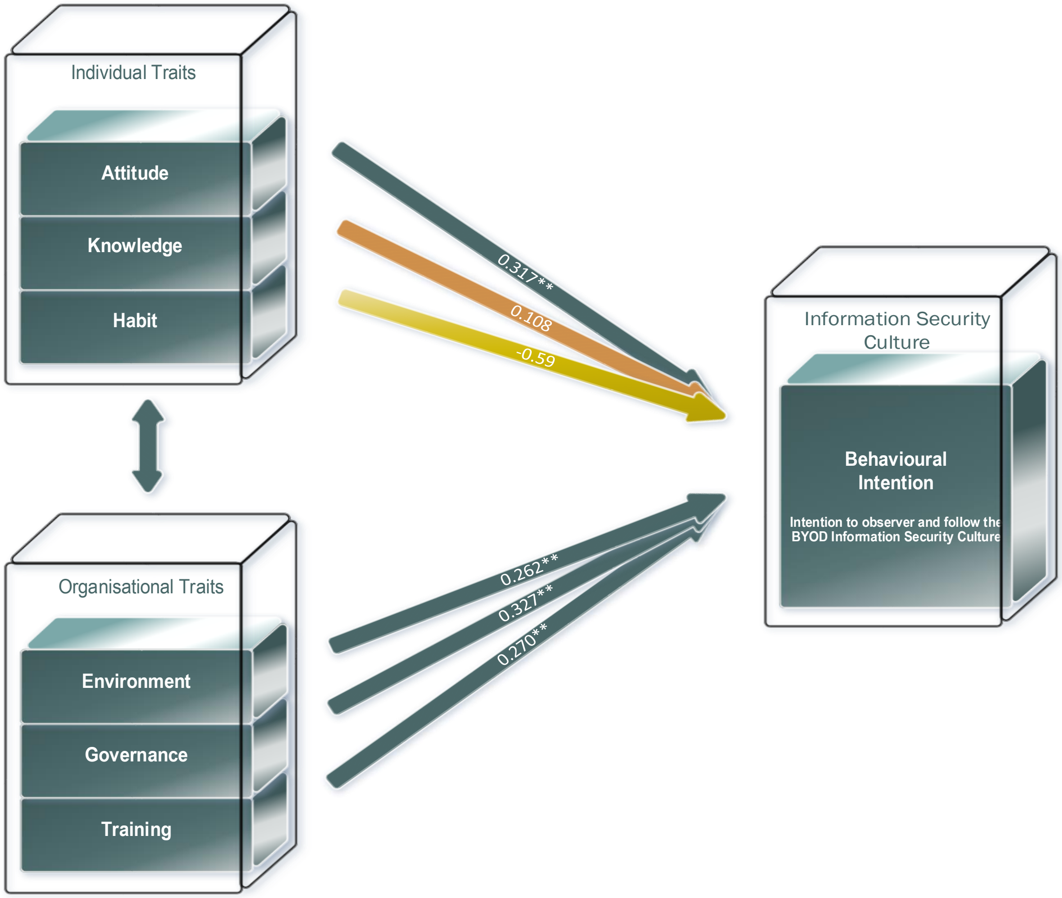
Department of Information Systems, University of Fort Hare

Questionnaire: A Model for Building an Information Security Culture for the Bring Your Own Device: the case of the unintended administrator

Dear Colleague,

I am a student in the Department of Information Systems at the University of Fort Hare (East London Campus), currently conducting research for my Doctor of Philosophy Degree under the supervision of Prof. Stephen Flowerday and Dr Liezel Cilliers. The focus of the research project is to understand the security culture concerning BYOD (Bring Your Own Device) within the banking industry. BYOD is the practice of allowing the employees of an organisation to use their own computers, smartphones, or other devices for work purposes. The objective of the research project is to build an information security culture around BYOD within the Banking Industry in Zimbabwe. A BISB model was developed based on six constructs of attitude, knowledge and habit as show on the figure 1. By answering the 15 questions in this questionnaire you will have participated in the evaluation of the BYOD Information Security Behavioural mode. As a CIO in a commercial bank in Zimbabwe, you are nominated as an expert in the Information Security on the BYOD.

Your participation in this research study is voluntary. You may choose not to participate. If you decide to participate in this research survey, you may withdraw at any time. If you decide not to participate in this study or if you withdraw from participating at any time, you will not be penalised.



BYOD Information Security Behavioural (BISB) model

We will do our best to keep your information confidential. All data is stored in a password protected electronic format. To help protect your confidentiality, the surveys will not contain information that will personally identify you such as your name, email address or IP address. The results of this study will be used for scholarly purposes only and may be shared with Fort Hare University representatives.

If you have any questions about the research study, please contact any of the individuals above. This research has been reviewed according to University of Fort Hare procedures for research involving human subjects.

ELECTRONIC CONSENT: Please select your choice below.

Clicking on the "agree" button below indicates that:
- you have ready the above information
- you voluntarily agree to participate
- you are at least 18 years of age

If you do not wish to participate in the research study, please decline participation by clicking on the "disagree" button.

● Agree

○ Disagree

Looking forward to your responses.

Yours sincerely

Mr. Alfred Musarurwa

<u>Contact Information</u>
Mr. A. Musarurwa
PhD Student
Department of Information Systems
University of Fort Hare
Email: 201515333@ufh.ac.za
Phone: +263 772 644 756

<u>Supervisor/s</u>
Prof. S. Flowerday
Dr. L. Cilliers
Department of Information Systems
University of Fort Hare
Emails: sflowerday@ufh.ac.za
lcilliers@ufh.ac.za

•

Completeness	Not exhaustive	To a lesser extent	Moderately exhaustive	To a larger extent	Completely Exhaustive
(To what extent the model covers the problem it is meant to address)	1	2	3	4	5
1. To what extent are the BISB individual traits exhaustive in covering the employee's contribution to information security in the BYOD?					
	1	2	3	4	5
2. To what extent are the BISB organisational traits exhaustive in covering the employee's contribution to information security in the BYOD?					
Consistency	Completely Disagree	Disagree	Neither Agree Nor Disagree	Agree	Completely Agree
(To what extent the model consistently securers the BYOD unintended administrator)	1	2	3	4	5
3. Do you feel that the BISB model will maintain its relevance with the ever changing security landscape?					
	1	2	3	4	5

4. How well structured are the arguments for the BISB M?

Accuracy	Very Inaccurately	Inaccurately	Moderately	Fairly accurately	Very Accurately
(The level of detail at which the model tackles the BYOD information security challenges.)	1	2	3	4	5

5. How accurately do you think the BISB model addresses the challenges of information security around BYOD in Zimbabwe?

	1	2	3	4	5

6. How comprehensive is the BISB model in addressing the factors affecting Information Security around BYOD?

Performance	Extremely unlikely	Unlikely	Indifferent	Likely	Extremely likely
(How the model improves the BYOD information security for the unintended administrator)	1	2	3	4	5

7. How likely are you to recommend your organisation to adopt the BISB model?

	1	2	3	4	5

8. How likely is your organisation to adopt the BISB model on your recommendation?					
Usability	Very Inapplicable	Inapplicable	Moderately applicable	Fairly applicable	Very applicable
(How banking organisations easily apply the BISB model)	1	2	3	4	5
9. How applicable is this model to your organisation?					
	1	2	3	4	5
10. How adaptable is the BISB model to be applied to the various banks in Zimbabwe?	0	2	1	7	6
	1	2	3	4	5
11. How applicable is this model in Zimbabwe's banking environment?					
Reliability	Completely disagree	Mostly disagree	Agree on some aspects	Mostly in agreement	Completely in agreement
(Evaluates how the BISB model can be depended upon by banks in Zimbabwe)	1	2	3	4	5
12. How much of the model are you in agreement with?					
	1	2	3	4	5

13. How much of the BISB model is already in practice in your organisation?

Best Fit	Does not fit	To a lesser extent	Indifferent	To a larger extent	Seamlessly
(How the BISB model can be depended upon by banks in Zimbabwe)	1	2	3	4	5

14. To what extent does the BISB Model fit in with the existing security culture at your organisation?

	1	2	3	4	5

15. How easily can the BISB model be applied to your organisation?