DESIGNING A BRING YOUR OWN DEVICE SECURITY AWARENESS MODEL FOR MOBILE DEVICE USERS IN NAMIBIAN ENTERPRISES

A THESIS SUBMITTED IN FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF COMPUTER SCIENCE

AT THE

NAMIBIA UNIVERSITY OF SCIENCE AND TECHNOLOGY

BY

ESTER SHIHEPO

201072653

SUPERVISOR: PROF FUNGAI BHUNU SHAVA

CO-SUPERVISOR: DR MERCY CHITAURO

METADATA

TITLE:	Ms
STUDENT NAME:	Ester Shihepo
SUPERVISOR:	Prof Fungai Bhunu-Shava
CO-SUPERVISOR:	Dr Mercy Chitauro
DEPARTMENT:	Computing and Informatics
QUALIFICATION:	Master of Computer Science
SPECIALISATION:	Information security
STUDY TITLE:	Designing a Bring Your Own Device security awareness model for mobile device users in Namibian enterprises
KNOWLEDGE AREA:	HCI
KEYWORDS:	Bring Your Own Device, threats, awareness, model, security, users, enterprise
TYPE OF RESEARCH:	Applied Research
METHODOLOGY:	Qualitative
STATUS:	Thesis
SITE:	Motor Vehicle Accident Fund (MVA FUND)
DOCUMENT DATE:	30 May 2023
SPONSOR:	N/A

DECLARATION

I, Ester Shihepo, hereby declare that the work contained in this report presented for the degree of Master of Computer Science at the Namibia University of Science and Technology titled **"Designing a Bring Your Own Device security awareness model for mobile device users in Namibian enterprises"** is my original work and I have not previously submitted it to any other higher education institution for the award of a degree.

_____Ester Shihepo_____ ____30 May 2023_____
Student Name & Surname Date

RETENTION AND USE OF THESIS

I, Ester Shihepo being a candidate for the degree of Master of Computer Science accept the requirements for the Namibia University of Science and Technology relating to the retention and use of thesis deposited in the Library and Information Services.

In terms of these conditions, I agree that the original of my thesis deposited in the Library and Information Services will be accessible for purposes of study and research, in accordance with the normal conditions established by the Librarian for the care, loan or reproduction of the thesis.

Signature:  Date: _____30 May 2023_____

DEDICATION

This thesis is dedicated to my husband for his unconditional support and for constantly reminding me that there is always an end to every situation. It is also dedicated to my colleagues at work who have been constantly encouraging me not to give up despite the hurdles I have been going through.

ACKNOWLEDGMENTS

Firstly, I would like to thank and praise the Almighty God for his loving kindness, great mercy, and guidance throughout the academic years.

Secondly, I would like to thank my supervisors, Prof Fungai Bhunu-Shava and Dr Mercy Chitauro for their perseverance, guidance, and continuous support during this study. It is because of your efforts and guidance that I managed to accomplish this milestone.

Lastly, I would like to thank the officials and experts who participated in this study. Their participation helped me achieve the study objectives.

ABSTRACT

The phrase Bring Your Own Device (BYOD) also known as Dual-Use Devices is a mutual practice which has increased employees' access to new mobile technologies and a rising trend within many organisations. The concept refers to employers allowing their employees to bring their personal mobile devices to workplaces and use them as their workstations. Enterprises are enjoying the benefits of BYOD, which allows them to cut operational costs as they do not need to purchase computers for their employees. Employees are enjoying the comfort and convenience offered by BYOD; however, this exposes organisations to security breaches. There is currently a lack of security awareness among mobile device users within enterprises against BYOD cyber threats. The situation has made it difficult for organisations to monitor the usage of resources among the mobile users towards protecting the confidentiality, integrity, and availability of corporate data. Moreover, cyber attackers see more potential with mobile devices as company and personal data get mixed up on such devices. Although the BYOD concept has not been formally implemented within the enterprise, it does not mean that the enterprise data is not prone to attackers. This study presents a BYOD Security Awareness Model designed following Design Science Research methods based on findings of a single case study conducted in one of the enterprises in Windhoek, Namibia. Qualitative research following the interpretivism philosophy was used. To select participants, purposeful random sampling method was used for this study. Data was collected using interviews, a questionnaire and through literature review. Furthermore, the study implemented the qualitative content analysis as the data analysis technique. The study identified malware and network spoofing as some of the BYOD related threats affecting the case enterprise. The researcher observed lack of end user awareness on BYOD security as a cause of BYOD related security threats. The study identified four main components of the model namely: BYOD threats, security awareness, policy and access control. The BYOD security awareness model will be a guideline to Namibian enterprises in creating BYOD security awareness among their mobile devices with the aim to safeguard the organisational data. Furthermore, the findings will also contribute to the new technology horizon of Namibia's future BYOD security awareness by motivating enterprises to implement mechanisms that will protect the enterprise confidential information. Since Namibia is reported as one of the least ranked countries in Africa in terms of cyber security, the model is a guideline on how enterprises can create BYOD security awareness among users within their enterprises and improve their security posture as well as that of the nation. Additionally, the model will also contribute to the BYOD security awareness knowledge to researchers and practitioners through conference papers and thesis publication.

Key words: Bring Your Own Device, Threats, Awareness, Model, Security, Users, Enterprise

PUBLICATIONS

Shihepo, E., Bhunu Shava, F., & Chitauro, M. (2022). Assessment of BYOD security awareness within Namibian enterprises. *1st Zimbabwe Conference of Information and Communication Technologies (ZCICT)*, Harare, Zimbabwe, pp. 1-5, doi: 10.1109/ZCICT55726.2022.10046002.

Shihepo, E., Bhunu-Shava, F., & Chitauro, M. (2023). Designing A Real-Time Bring your Own Device Security Awareness Model for Mobile Device Users within Namibian Enterprises, 6th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 2 pp. 1-4, doi: 10.1109/ISCON57294.2023.10112191.

Table of Contents

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS/ACRONYMS

BYOD	Bring Your Own Device
BYOD-SAM	Bring Your Own Device Security Awareness Model
DDoS	Distributed Denial of Service
DSR	Design Science Research
IT	Information Technology
OS	Operating System

CHAPTER 1: INTRODUCTION AND BACKGROUND OF THE STUDY

1.1 Introduction

This chapter gives an overview of the research background by presenting current developments in BYOD security. It outlines the problem statement and the purpose of the study. The chapter further highlights the overall objectives and research questions which the study is trying to diagnose. A brief research methodology used to meet the research objectives is also introduced in this chapter. Lastly, the chapter concludes with the research overview.

1.2 Research Background

Nowadays, enterprises and employees conduct business via internet-based technologies and have implemented the BYOD concept (Gökçe & Dogerlioglu, 2019). The concept offers flexibility, increased productivity, efficiency and reduced Information Technology (IT) hardware expenses, (Amoud & Roudies, 2017). BYOD is vulnerable to cyber threats including (but not limited to) identity theft, hacking, piracy, eavesdropping, and phishing. In the UK, the cost of cybersecurity breaches due to BYOD vulnerabilities is valued at $ 3.14 million as stated by (Alotaibi, Furnell, Stengel & Papadaki, 2016).

It can be challenging to monitor information security when BYOD is implemented in an enterprise (Lucas, 2020). This is because of mobile device users who are mostly the weak link due to their limited understanding of BYOD security awareness, as highlighted by (Brook, 2020). The COVID-19 pandemic has also contributed to the increased implementation of BYOD within enterprises and how businesses operate (Al-Katib, 2020). Without any doubt, BYOD poses security threats to enterprises that have implemented it and there is no threat that is too small to overlook as this will put the organisation data at risk (Al-Katib, 2020). Solutions to address this include adopting better cybersecurity practices by users as alluded by Brook (2020) and policies (Flores, Qazi & Juhmka, 2016). Currently the most effective solution is policies: however, this alone cannot mitigate BYOD security issues. Namibia is not excluded from the BYOD security dilemma, thus there is a need to investigate the extent of the dilemma and create BYOD security awareness among the mobile users as a mitigation strategy.

1.3 Statement of Problem

Enterprises are enjoying the benefits of BYOD, which allow them to cut operational costs as they do not need to purchase computers for their employees. Employees are enjoying the comfort and convenience offered by BYOD; however, this exposes organisation to security breaches because there is currently a lack of security awareness among mobile device users within enterprises against BYOD cyber threats

(Gökçe & Dogerlioglu, 2019). Francis (2017) highlighted several BYOD security threats that can impact enterprises and their mobile users which include mobile malware, the not-so smart users, mixing business with pleasure, social media, loss and theft as highlighted in figure 1.1.

The situation has made it difficult for organisations to monitor the usage of resources among the mobile users towards protecting the confidentiality, integrity and availability of corporate data. Moreover, cyber attackers see more potential with mobile devices as company and personal data get mixed up on such devices (Gökçe & Dogerlioglu, 2019). Thus, it is important to grow BYOD security awareness among mobile device users by designing a model for BYOD security awareness and for enterprises to implement mechanisms that will safeguard enterprises' confidential information.

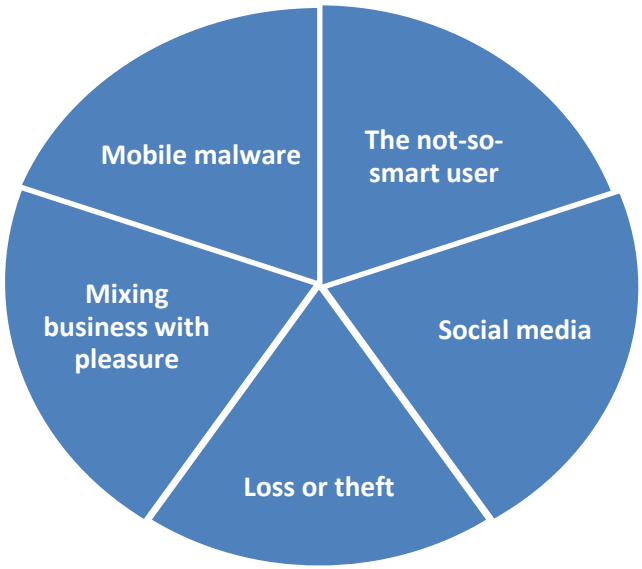


Figure 1.1 Overview of research problem

1.4 Research Questions

To address the research problem, the following research question and sub-questions were identified: The main research question of the thesis is defined as follows:

How can components of a BYOD security awareness among mobile device users be constituted into a model for Namibian enterprises?

The main research question is achieved by addressing the following sub-questions:

- How do Namibian enterprises address BYOD relate cyber threats?
- How effective are the existing BYOD security awareness models?
- How effective is the proposed BYOD security awareness model?

1.5 Research Objectives

The study intends to address the research questions highlighted above by designing a BYOD security awareness model for mobile device users within Namibian enterprises. Moreover, the study aims to:

Main objective: ***To design a BYOD security awareness model for mobile device users in Namibian enterprises.***

Sub-objectives:

- To evaluate how Namibian enterprises address BYOD related cyber threats prevalent in their space.
- To review the effectiveness of existing BYOD security awareness models.
- To assess the effectiveness of the proposed BYOD security awareness model.

1.6 Research Methodology and Philosophical Paradigm

The research followed a mono method and adopted a qualitative research design. According to Aspers and Corte (2019), qualitative research is useful when the research wants to understand motivations and perspectives of research participants, thus the researcher found this design suitable for this research. It is interpretive in nature and applies the inductive approach to collect context rich data. A semi-structured interview and a self-administered questionnaire, both with open-ended questions were used to collect data on BYOD security from research participants because they are a means to collect rich data.

Existing awareness models were reviewed and based on the research findings, the appropriate model was developed using the system design method. To evaluate the effectiveness of the proposed awareness model, the researcher went back to the enterprises in which the research was conducted and conducted

a test run. To enhance quality, data triangulation was used, meaning data was collected from different methods; interviews and questionnaires which are a form of data source triangulation. The following quality issues were addressed: data validity, consistency, credibility and transferability. Data was analysed using coding, a qualitative data analysis technique, (Linneberg & Korsgaard, 2019).

1.7 Significance of the Research

The study is relevant as it will provide baseline data with regards to BYOD security awareness. The study will provide insights to Namibian enterprises on how to create BYOD security awareness among mobile device users in general as they are considered to be the weakest link, with the intent to reduce threats to enterprises data.

1.8 Motivation of the Research

The motivation is that the implementation of BYOD has developed to be a crucial concern within Namibian enterprises. This research studies the best practises, challenges associated with BYOD implementation and design a model to help raise security awareness among mobile device users in Namibian enterprises. The model is intended to be used as a reference tool by Namibian enterprises.

1.9 Research Limitations

Data collection was limited to one organization to establish the state of BYOD on the ground which might vary in different size enterprises. Future work will focus on small-scale enterprises. Additionally, the demonstration and evaluation of the proposed BYOD model was not conducted in a real enterprise environment thus there is need for implementation and evaluation in real time.

1.10 Research Strategy and Outcomes

This section illustrates the linkage between research sub-questions. It outlines where in the thesis the research sub-questions and objectives were addressed and the references the appropriate sections of the thesis. Table 1.1 displays a summary of the sub-questions, their respective sub-objectives and the respective sections of this study that addressed them.

Table 1.1: Summary of research sub-questions and sub-objectives

Research sub-question	Research sub-objective	Chapters or sections that addressed sub-questions and sub-objectives
How do Namibian enterprises address BYOD relate cyber threats?	To evaluate how Namibian enterprises address BYOD related cyber threats prevalent in their space.	Chapter 4 section 4.2.3 and 4.4.5
How effective are the existing BYOD security awareness models?	To review the effectiveness of existing BYOD security awareness models	Chapter 2 section 2.2.4 Chapter 5 section 5.3.5.2.1
How effective is the proposed BYOD security awareness model?	To assess the effectiveness of the proposed BYOD security awareness model.	Chapter 5 section 2

1.11 Thesis Organisation

The rest of the thesis is organized as follows:

Chapter 2: This chapter gives an overview of BYOD security. It further examines existing BYOD security awareness models vital in creating security awareness among mobile device users.
Chapter 3: The chapter outlines the research methodology followed to address the research questions and attain the research objectives.
Chapter 4: This chapter analyses the data gathered during data collection.
Chapter 5: Focusses on designing the BYOD security awareness model based on the findings from chapter 4. The components of the BYOD security awareness model were identified and thereafter the model itself was designed.
Chapter 6: Concludes the research by revisiting the research questions and assessing what was done to address them and whether the research objectives were met.

1.12 Chapter Summary

This chapter presented the background of the study, and also shed some light on the statement of the problem, research questions and objectives, limitations as well as the significance of the study. The next chapter (Chapter 2) will discuss the literature review.

CHAPTER 2: LITERATURE REVIEW

2. BYOD SECURITY OVERVIEW

2.1 Introduction

In the modern world, people rely on mobile devices for personal and business use. Bring Your Own Device (BYOD) also known as Dual-Use Devices is a modern concept that brings vast benefits to organisations and employees, where employers allow employees to use their personal devices to execute official duties. Such organisations experience reduced IT costs, increased productivity and efficiency (Gökçe & Dogerlioglu, 2019). Despite the benefits, BYOD cyber threats are also alarming. Spamming, online harassment, cyber stalking, and passing on viruses are common types of cyber threats (Privacy Rights Clearinghouse, 2018). This chapter defines BYOD security and further examines the existing BYOD security awareness models needed to raise BYOD security awareness among mobile device users.

2.2 Literature Review

2.2.1 BYOD Overview

According to Procedia Computer Science (2016), enterprises goals with BYOD implementation are to increase the flexibility, convenience, and portability of devices to increase the employee's productivity and morale. Improved employee mobility, greater employee satisfaction, improved employee productivity, reduced cost, reduced security risks and employee privacy are some of the advantages of BYOD implementation (RSI Security, 2020).

Based on a study steered by Tech Pro Research (2016), 60% of organizations have implemented BYOD within their organizations and some are yet to implement BYOD, figure 2.1.

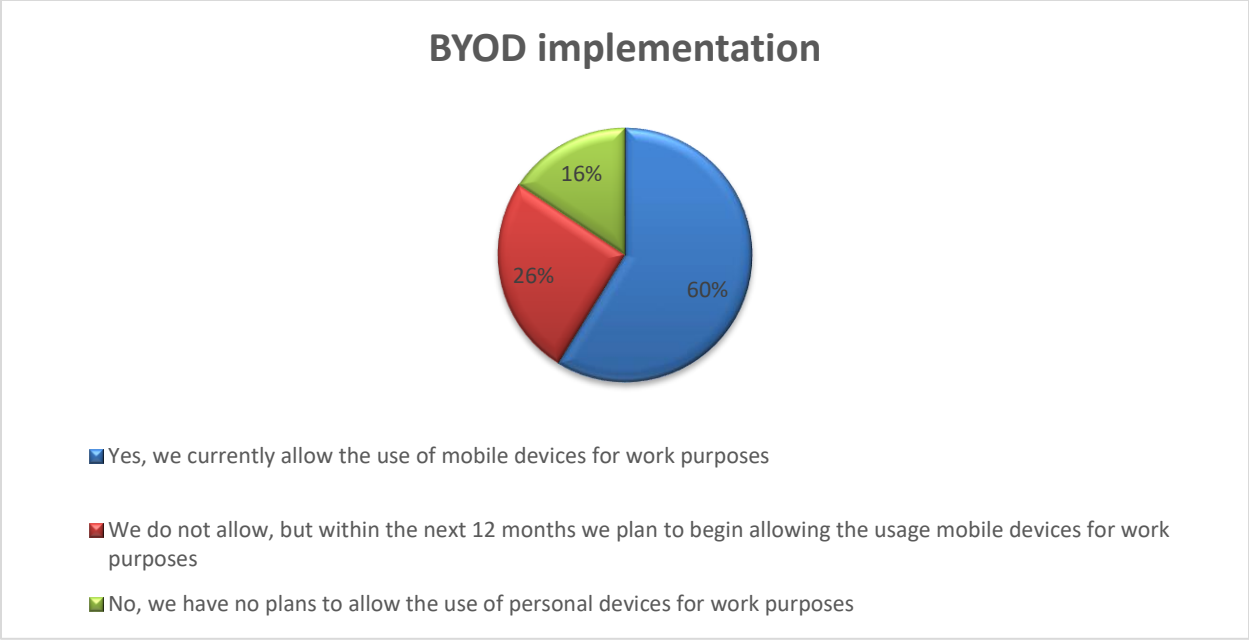


Figure 2.1 BYOD usage

BYOD security awareness describes the knowledge, attitude and behaviour that users apply in safeguarding organisational and personal information stored or transmitted using mobile devices. Users are usually aware of the benefits offered by mobile devices but are not always aware of the threats and risks that these devices pose to their information (Palanisamy & Wu, 2021).

2.2.2 Challenges with BYOD

According to Gökçe and Dogerlioglu (2019), BYOD presents a list of security concerns to businesses that have implemented it. If employees and enterprises are to reap the benefits of BYOD, then they also have to be concerned about the BYOD challenges. Technology alone cannot provide complete security solutions; thus, it is vital to consider the human factor. Most smartphone users rarely consider privacy and security when installing applications and do not protect themselves through protective mechanisms (Palanisamy & Wu, 2021). Mobile devices are prone to loss, theft and damage, which poses a significant information security risk to individuals and organisations. Flores et al. (2016) further highlighted that employees ignoring company security policies, installing unauthorised applications on their mobile device, misusing access credentials can lead to internal threats. Human error, general negligence and failure to comply with security agreements can cause risk and security breaches.

According to a study conducted by Flores et al. (2016), out of the 619 research participants, 27.03% use smartphone security software, 61.4% confirmed that they are aware of the existence of smartphone security software and 50.52% indicated that they have searched for a repository of free smartphone security software. Furthermore, only a small portion of smartphone users use smartphone security

software, which is not even half of the number of those that are aware of the existence of smartphone security software. Furthermore, it was identified that men implement security controls more on their mobile devices compared to women. Moreover, it was revealed that 35.38% of the respondents had their phones stolen, thus there is a need to present the awareness of risks among mobile users.

According to Alotaibi et al. (2016), a survey conducted in Saudi Arabia on cybersecurity awareness discovered that although users have good knowledge of Information Technology, they appear to have limited awareness on threats associated with cybercrime and cybersecurity practices. Saudi Arabia is one of the developing countries in the Middle East where the usage of mobile technologies and internet has gradually increased in the modern days. Despite the increase of cyber threats, there is no approach followed to create awareness among users apart from online information broadcasted on the government website. The occurrence of BYOD cyber threats is alarming as alluded by Alotaibi et al. (2016). Additionally, in the UK alone, the cost of cybersecurity breaches is estimated at $ 3.14 million. Additionally, it is estimated that by the year 2019, the losses of business due to cyber threats will be around $2 trillion.

2.2.3 Current status of BYOD in the African continent

Ruxwana, Msibi and Mahlangu (2018) highlighted that the adoption of BYOD is slow in African countries although majority of the employees own mobile devices. This could be attributed to the lack of enterprises readiness such as in terms of policies and infrastructures to govern BYOD adoption. As alluded by Makanyeza, Kudzai and Ngorora-Madzimure (2022), organisational and environmental readiness are factors to be considered in the BYOD implementation. Daniel (2021) highlighted that the COVID19 pandemic has caused an acceleration in many business practices in Africa and around the world including working remotely. For agile organisations, working remotely or hybrid was implemented seamlessly: however, data privacy remains a challenge. Veljkovic and Budree (2019) expressed that the fast adoption of mobile devices was observed in Africa outscoring both Western Europe and North America, with South Africa recording increasingly BYOD considerations. However, due to a lack of understanding the BYOD re]lated security risks, many enterprises are worried by the possible security threats associated with this concept.

2.2.4 BYOD security threats

According to Gökçe and Dogerlioglu (2019), BYOD cyber threats can be categorised into different categories namely: deployment, technical, policy and regulation and human aspect challenges. The human aspect is an ongoing challenge to enterprises thus there is a need to create awareness among mobile users to reduce BYOD security threats. BYOD cyber threats can result in the following losses: data, privacy, money, means of production, reputation, goodwill, wellbeing and many more (Ronwyn, 2016).

Table 2.1: Common BYOD threats, causes and implications for enterprises (Olalere, 2015)

Threat on BYOD	Causes of threat	Implications on enterprise
Data leakage	Malicious mobile device user Mobile device remote access by attacker Application vulnerabilities: • Loss of mobile device • Malicious application • Social engineering	Leaked enterprise private data in the public
DdoS	Attacker's malicious intention Exploitable vulnerabilities in enterprise network	Negative impact on the server Deny the availability of the system for legitimate. Users
Malware	Trojan apps: Malicious code can be inserted into the application by an attacker with the intention of attacking devices or enterprise applications. Social media, email, and SMS links: Links are embedded in SMS, social media posts, and emails with the intention of redirecting users to a website that hosts malicious files. Third-party app stores: Some third-party app stores may host malware that can potentially harm devices, systems, and networks.	Theft of enterprise information Enterprise applications malfunctioning Both corporate infrastructure and personal mobile devices of employee are affected by malware.

According to Mahoney (2016), 20% of cyber threats exposure occurs due to the vulnerability of technology and 80% because of people. Ronwyn (2016) further highlighted that people vulnerabilities exist because they are unaware of threats, under-invest in security, not well trained, not motivated, and rogue or slips and lapses. BYOD is subject to several threats because the devices involved do not belong nor are they controlled by enterprises. Despite the availability of security procedures put in place, mobile device users are gradually vulnerable to BYOD threats. Vrhovec (2016) revealed that many mobile device users do not mind about security threats and how they affect them. Vrhovec (2016) further highlighted data leakage, unauthorised access to company data and systems, users downloading unsafe applications or content and malware as the main concerns related to BYOD.

The same way computers get infected with viruses, there are a range of threats that affect mobile devices (Francis, 2017). Though the threats are growing, the focus and allocation of resources appears to be

insufficient to protect mobile devices against BYOD cyber-attacks. According to Britt (2017), 75 percent of mobile security breaches were through applications. Based on research conducted by Duke University/CFO Magazine Global Business Outlook Survey (2016), about 80 percent of companies in US were successfully hacked. BYOD cyber threats can result in the following loss: data, privacy, money, means of production, reputation, goodwill, wellbeing and many more (Ronwyn, 2016).

Based on Johar (2017) findings, cyber attackers can apply any of the following methods to gain access to corporate sensitive data:

- **Malicious applications:** Users normally install mobile applications from play store without an in-depth understanding of permissions required by these applications. This could lead to corporate data being exposed to unauthorised individuals without the knowledge of the user or employer.

- **Privilege escalation:** Confidential organisational information can also be accessed remotely by launching a privilege escalation attack. However, unprivileged applications might interact with enterprise applications to gain access privileged data.

- **Physical access:** Mobile devices can easily get lost or misplaced because of their mobility and small size. This can cause greater jeopardy to an organisation, because this simply means all data stored on the device can be exposed.

- **Disgruntled employees:** Former and disgruntled employees can leak confidential data to competitors, or which may expose the company, if the corporate data which was stored on their devices was not properly removed.

Despite the availability of security procedures put in place, mobile device users are gradually vulnerable to BYOD cyber threats. The fact that users can use mobile devices without prior training or basic understanding of security exposes them to cybercriminals. Vrhovec (2016) revealed that many mobile device users do not mind about security threats and how they affect them. There are a number of malwares that targets mobile devices which causes data deletion or access denial on mobile devices. Users can infect their mobile devices without noticing for instance by visiting wrong web sites, where malware might end up being installed in the background.

Based on research conducted by Francis (2017) and by Brook (2020) below are several BYOD security threats that can impact enterprises and their mobile users:

Mobile malware: Mobile devices are prospering and growing. This malicious software aims to steal data from mobile devices and make money.

Loss or theft: The fact that mobile devices are carried by users everywhere make them vulnerable to theft, loss or damage, which results in sensitive corporate or personal data accessible to criminals.

Social media: Mobile device users are invited to download applications or enter a competition or join a fake event possibly in return of a gift. Spam and phishing are ever-changing from emails into social media.
The not-so-smart user: Most mobile device users are reckless when it comes to protecting their devices. Based on the Symantec ISTR, 52 percent of mobile users store sensitive data online and only a few consider security measure such as passwords and security software's.

Mixing business with pleasure: Employers provide their employees with mobile devices with the aim to maximise productivity. The moment the staff leave the secure company network and go connect to home or public networks expose company data to criminals.

2.2.5 BYOD security best practices

BYOD allows confidential data to be retrieved and viewed on systems outside an organization's control, thus it is critical to encrypt data at rest and in transit (Brook, 2020). To safeguard the organisational data, it is pivotal for enterprises to implement the BYOD security best practices such as separating personal and enterprise data, have a solution in place for lost devices, ensure secure network connectivity and educating the users, which is the focus of this study Lord (2020). Educating the users involves having a BYOD security policy in place, and most importantly, investing time in educating the users about such a policy. Such users should be made aware of the importance of BYOD security and the consequences of violating such policy.

Figure 2.2 highlights the components of a BYOD security policy. Providing training and education to the users with the aim to create BYOD security awareness is the focus for this research. By educating the users, this will help ensure that your employees follow standard security procedures.

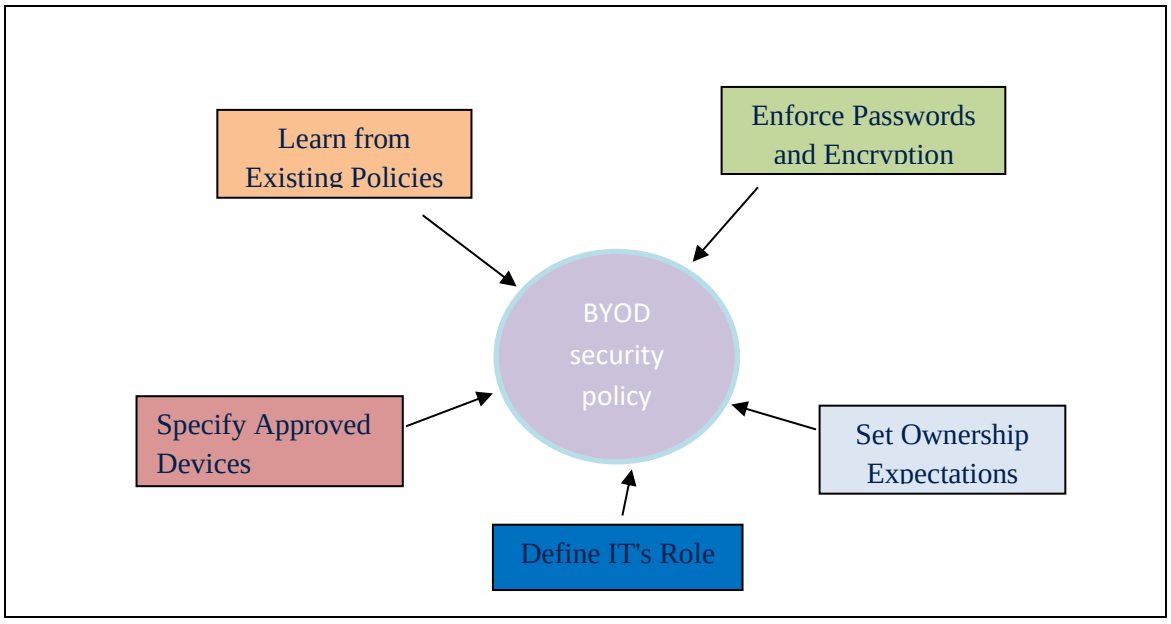


Figure 2.2 Components of a BYOD policy

According to Bambulas (2020), an effective BYOD security awareness program should take place after every 4 to 6 months. After that, users tend to forget what they have learned, however with time the intervals can be increased.

Equally, it is also important to implement authentication methods to protect the enterprise data. There are different authentication types e.g. password-based authentication, certificate-based authentication, biometrics authentication and token-based authentication (N-able, 2019). It is crucial to verify the identity of any individual who would like to access the organizational data. According to Vekua (2021), the effectiveness of any authentication solution is based on two main components, its security and usability. Those two components are important for every individual case. The authentication method for every business is dependent on the size of the business, available security budget and so forth.

2.2.6 Existing BYOD awareness models

A model is defined as a pictorial or graphical representation of key concepts Khan (2016).With the help pf allows and other diagrams, it shows the relationship between various variables. Conner (2021) state that a model is either a proposal or actually "how something works".

The next section discusses some of the existing BYOD security awareness models.

2.2.6.1 Comparisons of the existing BYOD security awareness models

This section presents the existing BYOD securing awareness models for creating BYOD security among the mobile device users. This study discussed three existing BYOD security models.

2.2.6.1.1. BYOD-Insure: A security Assessment model for Enterprise BYOD

Ratchford (2020) proposed a model to help organisations identify vulnerabilities, mitigate security risks, and strengthen the security posture in their BYOD environments. The model provides a non- assessment process that uses diagrams and tables to identify security vulnerabilities and provide recommendations for risk mitigation based on the security posture of the organization being assessed. Organizations considering the adoption of BYOD can use this model to obtain an individualized security assessment before BYOD implementation. In the same manner, organizations already in BYOD environments can use BYOD-Insure to assess their current BYOD security controls and strengthen their security posture. Auditors and other security professionals can use this tool to aid in their security assessments projects.

The research identified the user awareness gap in this model. One can have all the processes in place however, if the user awareness is side-lined, the organisational data can be at risk, which motivated the user to design the proposed awareness model.

2.2.6.1.2 User's Information Security Awareness in BYOD Programs: A Theoretical Model.

The "User's Information Security Awareness in BYOD Programs: A Theoretical Model" developed by Han (2017) objective is to investigate the user's information security awareness in bring-your-own-device (BYOD) programs. Additionally, it also highlights the influence of a user's cyber security inertia, a personal security management procrastination tendency, on the user's security awareness of organization information resources.

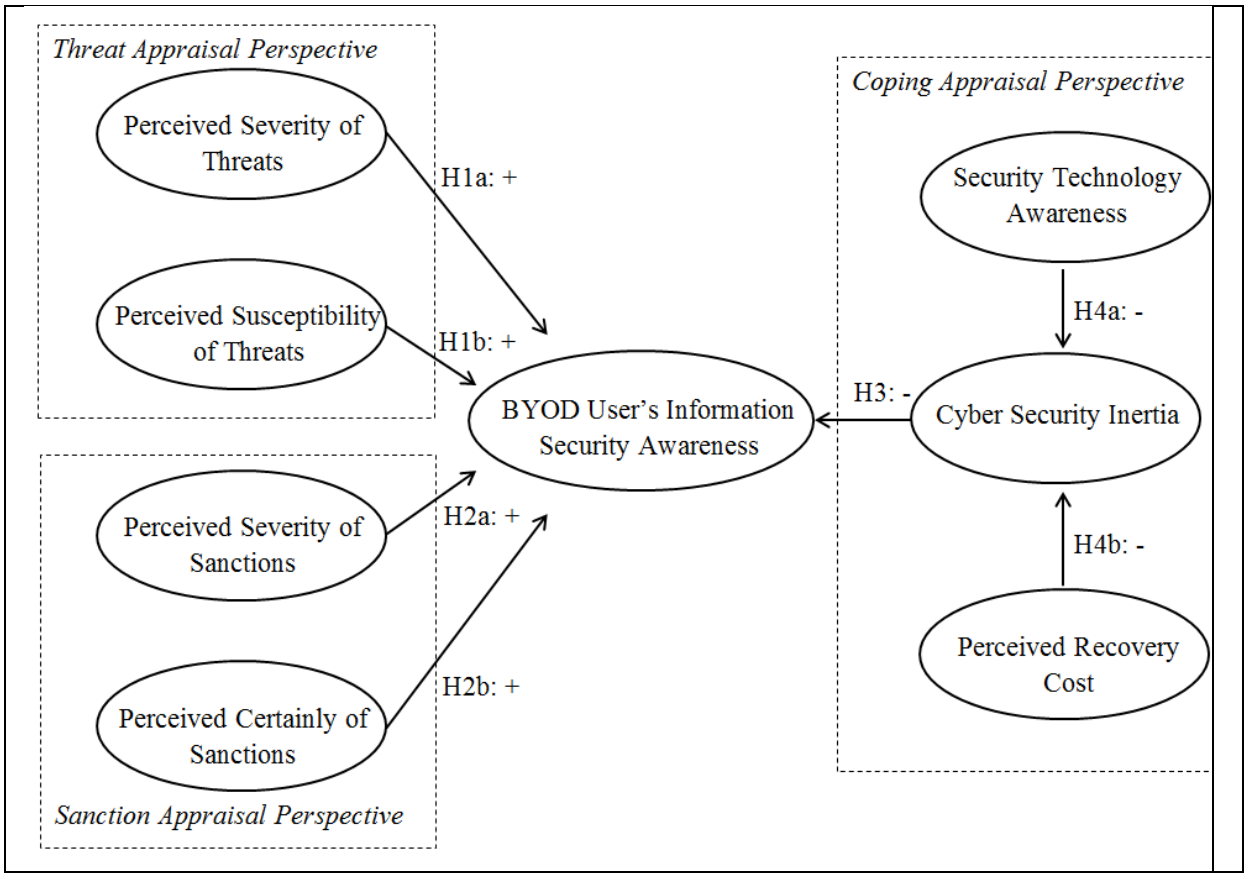


Figure 2.3 BYOD User's Information Security Awareness in BYOD Programs: A Theoretical Model (Han, (2017)

The proposed model offers an important guideline for BYOD security management and provides a clear definition of user BYOD security awareness. User awareness was studied from two lenses of research, including the protection motivation theory and the general deterrence theory. Han (2017) highlighted that the protection motivation theory focuses on studying an individual's reactions and subsequent behaviours when facing potential threats to her health. This theory believes that an individual's motivation for searching for protections is stimulated, if she believes that negative outcomes from threats are severe, and the consequences are likely to occur. However, the researcher identified some gaps in the model such as that the model focuses more on the theory, and the user's awareness component has not been adequately covered, which stimulated the need to develop the proposed BYOD-SAM.

2.2.6.1.3 Improving Security in Bring Your Own Device (BYOD) Environment by Controlling Access

Muhammad, Ayesh & Zadeh (2017) developed the "Improving Security in Bring Your Own Device (BYOD) Environment by Controlling Access" model with the aim to close-up the gaps in access control on BYOD environments. This model focus is more on enhancing security using an adaptive security technique like the multi-level security approach within the platform and the device. The model has two main techniques.

Adaptive Security Technique: This will help in mitigating security breaches with capability for continuous tracking for potential security threats on devices. Also, preventing users from advanced attacks like phishing, and social engineering among others; by balancing the approaches organizations could apply to their business processes. The technique will improve access control on devices by patterning user behaviour and context to restore trust.

Intelligent Filter: This will help improve access control by authenticating users based on patterns and context information and detecting abnormal employee behaviours based on the analysis of patterns contexts generated. Once a new user tries to access the platform, user behavioural contexts will be recorded and added to the employee policy manager. This could be achieved by setting up the value to allow access to a limit and denying access for contextual value less than the limit. In case of existing users (employees), the system checks the policies, compare the behavioural context for correspondence to known context before determining if or not to grant access. The model appears to be well details; however, it does not clearly outline how to create user BYOD security awareness, which is currently the loophole.

2.3 Literature Findings

All the existing models are unique in their own ways considering the advantages they offer. Although they aim at offering BYOD security, the user awareness domain has not been articulated in details and the users are considered the weakest link to most security breaches. With all the models that were reviewed, the users BYOD security awareness gap remains a concern, which motivated the development of the BYOD-SAM.

2.4 Chapter Summary

The chapter outlined the advantages and disadvantages offered by BYOD implementation with an organisation such as increased productivity, flexibility, and reduced costs. It further, reviewed the BYOD related security threats and their impact such as loss of organisational confidential data and bad reputation for an organisation. Three existing BYOD security awareness models were review and the user

awareness loophole was identified, which triggered the development of the BYOD-SAM, the main objective of this study.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Introduction

This chapter contributes to this study by developing a research design guided by the reviewed literature to meet the research objectives. It also outlines the research design, data collection and data analysis techniques that were used. The research aims to design a BYOD security awareness model for mobile device users in Namibia. To achieve this the following research approaches will be considered:

3.2 Research Strategy

The mono case study strategy was used to meet the research objectives and answer the research questions. Harrison, Birks, Franklin and Mills (2017) described a case study as a methodology used to explore a single phenomenon in a natural setting by means of variety of methods to acquire in-depth knowledge. Yin (2014) defines a case study as a distinctive research strategy which allows in-depth investigations about the issue at hand, and it is important to justify its use to demonstrate its suitability to the research. Moreover, according to Yin (2014), the research question: *"How can components of a BYOD security awareness among mobile device users be constituted into a model for Namibian enterprises?"* contains a "how", which qualifies it for a case study research strategy. Furthermore, the study follows the inductive research approach. Chetty (2016) highlighted that an inductive approach uses comprehensive reading of secondary data to identify themes, concepts and create a framework.

Organisational culture also has an impact on the BYOD behaviour within an organisation. According to Procedia Computer Science (2016), enterprises' goals with BYOD implementation are to increase the flexibility, convenience, and portability of devices in order to increase the employee's productivity and morale. According to Downer and Bhattacharya (2015), BYOD presents a list of security concerns to businesses that have implemented it. If employees and enterprises are to reap the benefits of BYOD, then they also must be concerned about the BYOD challenges. Technology alone cannot provide complete security solutions; thus, it is vital to consider the human factor. Thus, a mono case study strategy has been employed with the aim to demonstrate the implications of lack of security awareness among mobile device users to organisations and how to create security awareness among such users.

3.3 Research Approach

Chetty (2016) acknowledges that there are three types of research approaches, deductive, abductive, and inductive research approaches. This study follows the inductive research approach. Chetty (2016) further highlighted that the inductive approach uses comprehensive reading of secondary data to identify themes, concepts and create a framework. The formulation of the research problem statement and research questions were guided by literature. The research main objective is to design a BYOD model security awareness model for mobile device users in Namibia. Thus, this study followed the inductive approach to meet its objectives.

3.4 Design Science Research Strategy Overview

Brocke, Hevner and Maedche (2020) described Design Science Research (DSR) as a problem-solving paradigm that seeks to enhance human knowledge through the creation of innovative artefacts. Additionally, the outcome of DSR includes newly designed artefacts and design knowledge that provides a fuller understanding via design theories of why the artefacts enhance the relevant application contexts. Pries-Heje, Baskerville and Venable (2008) highlighted that DSR cater for innovative artefacts to solve real-world problems. This study deployed DSR to develop a BYOD security awareness model for mobile device users within Namibian enterprises.

3.5 Research Choice and Philosophy

A belief about the way in which data about a phenomenon should be collected, analysed and used is referred to as a research philosophy Žukauskas, Vveinhardt & Andriukaitienė (2018). This research followed the interpretivism philosophy because this philosophy requires the researcher to construe the elements of the study and thus this philosophy integrates human interest into a study (Pham, 2018). Furthermore, interpretivism philosophy recognises that human beings are not mechanistic, and thus they have multiple realities which need to be understood within their context. According to Žukauskas et al. (2018), this philosophy prefers qualitative methods which allow close interaction with the research participants although quantitative methods can be used also.

Additionally, the research followed a qualitative research choice. According to Žukauskas et al. (2018), qualitative research is useful when the researcher wants to understand motivations and perspectives of research participants, thus the researcher found this design suitable for this study. Qualitative research focuses on understanding the human behaviour from the participant's perspective. Furthermore, qualitative researchers study things in their natural settings and try to make sense of or interpret a phenomenon in terms of the meanings people bring to them (Crossman, 2019). For us to develop a

practical solution that responds to end user needs within the specific industry, a qualitative case study was the best.

3.6 Selection of Case Study Site

The mono case study has been selected to gather research data to meet the research objectives. Additionally, a mono case study can richly describe the existence of a phenomenon and for creating high-quality theory, Gustafsson (2017) supports a single case strategy. The study used purposeful random sampling method to select a case for data collection. Purposeful random sampling looks at a random sample and adds credibility to a sample when the probable purposeful sample is larger than one can handle, (Crossman, 2019). Motor Vehicle Accident Fund (MVA Fund) was selected for this research as it was considered by the researcher as a suitable site in meeting the research objectives.

3.7 Data Collection Techniques and Instruments

Rouse (2016) defined data collection as a method of acquiring and measuring data on variables of interest, in a recognised systematic manner that enables one to get a complete and accurate picture of an area of interest. In depth interviews using a semi-structured interview guide, literature and a web-based questionnaire were the data collection techniques used to collect the research data. According to Howard (2019), a web-based questionnaire makes data collection to be quicker and it is less complicated. Moreover, web-based interviews allow for rich data to be collected as the researcher has an opportunity to probe and acquire more information in the process.

For both the online questionnaire and interview guide, the following protocol was followed from developing the data collection tools till the actual data collection process. The researcher had to do extensive literature to identify the gaps and the need to conduct the research. Themes were identified and the questions were drafted. The questions were reviewed together with the research academic supervisors to vet the language and data to be collected. A pilot study was conducted with 5 people with the aim to verify the timing, any issues arising and if the data collected is in line with what the research aims to achieve. Data from the pilot study were reviewed together with the research academic supervisors, the questions were refined, and the tools were ready for actual data collection.

- **Web-based questionnaires:** The online questionnaire was developed using google forms. A questionnaire (Appendix B) with open-ended questions was used as a data collection tool for this study. The link to the questionnaire was shared with the Senior IT Manager by the researcher to be shared with the research participants. Three participants from each department within the enterprise were randomly selected using the probabilistic sampling method based on the availability of the

mobile device users in the enterprise to complete the questionnaire. The sampling was done this way to ensure that the organization meet the deadline that was agreed upon with the researcher, which was 3 weeks.

The questionnaire was used to collect data to access BYOD security awareness among mobile device users in the enterprise. Moreover, it was used to obtain additional information to support the evidence gathered through interviews conducted with the IT team. The questionnaire also reduces biasness as the responses are in the research participant's own words. The questionnaire used for this study can be found under appendix B.

- **Interviews:** Interviews were conducted with the IT officials including the Senior IT Manager. The interview guide/questions were emailed (Appendix C) to the Senior IT Manager and facilitated the completion of such interview questions by the IT officials. Seven (7) officials completed the interview questions. Due to the nature of the enterprise and the workload within the enterprise, the Senior IT Manager proposed that the researcher emails the question for the team to complete. The Senior IT Manager expressed the time constraint issue and thus why the interviews were completed in the absence of the researcher. Interview guide used for this study are provided in appendix C.

3.8 Data Analysis

Sridhar (2018) described data analysis as a process of examining, cleaning, converting and modelling data with the aim to obtain useful and meaningful information. Narrative analysis was used to analyse the collected research data, a qualitative data analysis technique. According to Seelman, Lewinson, Engleman, Maley, & Allen (2017) narrative analysis involves a research interpreting what was shared within the context of the research. Data collected through interviews and questionnaire were analysed collectively with the intent to obtain meaningful descriptions. Kelly (2023) maintains that data analysis involves examining, categorising, tabulating and testing data for it to meaningful and aid in decision making.

The study implemented qualitative content analysis. Each participant's response was analysed separately to identify relevant information then collectively analyse all responses to identify matching and unique emerging themes. Gibson (2016) highlighted that qualitative data analysis is more concerned about meaning. Table 3.1 outline the steps followed during data analysis:

Table 3.1: Data analysis process

Step no	Step	Description
Step 1	Organising the data	Questionnaire responses were coded Interview responses were transcribed to identify and differentiate between the questions that the research is trying to answer
Step 2	Finding and organising ideas	Themes and recurring ideas were identified
Step 3	Ensuring data reliability and validity	A consistent and systematic way of analysing the data was maintained
Step 4	Finding possible explanations of the findings	Findings were summarised, themes and related them to literature
Step 5	Report methods and findings	Meaningful data was presented into graphs and charts

- Questionnaire's data analysis: The software automatically collected the data then the researcher downloaded the spreadsheet with the data. The researcher then had to count the number of participants that have selected each response. The software also provides some graphical presentation of the data such as graphs and tables, however the researcher had to clean this up since there are a lot of repetitions.

- Interview data analysis: Since the interview guide was manually completed by the participants, the researcher had to transfer the responses to a spreadsheet. The researcher then had to identify the part of the data to be used for further analysis.

3.8.1 Unit of analysis

According to the Open University of Hong Kong (2016), the unit of analysis is the entity that you wish to say something about at the end of your study, perhaps what you consider to be the main focus of the study. Yin (2014) stated that the unit of analysis relates to the case to be studied and it derives from the key words that form the main research question. This research study adopts a mono-case design containing a single unit of analysis.

> *"How can components of a **BYOD security** awareness among **mobile device users** be constituted into a model for **Namibian enterprises**?"*

Considering the research main question keywords above (in bold), the unit of analysis for this study are the mobile device users that uses mobile device within enterprises. Meaning, the study targeted mobile device users in the organisation.

3.8.2 Data triangulation

Liberman (2018) defines triangulation as using multiple methods or data sources to develop a comprehensive understanding of a phenomena. The aim is to test the valid of the data from different sources. The study implemented data triangulation through literature review, interviews and online questionnaire, to validate, strengthen and ensure consistency of the research findings. A better understanding of the research topic was also attained through data triangulation.

3.9 Ethical Consideration

Bhasin (2020) described ethical consideration as inclusive of values and principles of what is considered good or bad, right or wrong in human affairs. According to the University of Stellenbosch (2018), ethical clearance involves the ethical clearance committee reviewing the research objectives and methodologies to ensure that the research is conducted in a manner that protects the research participant rights, dignity and that the research design is ethical. Furthermore, the ethical clearance is sought to ensure that the research is conducted in an ethically accountable manner, to minimise risks and to ensure that the research ultimately leads to the valuable outcomes. The ethical approval is required for any research that involves human participation (Resnik, Rasmussen, & Kissling, 2015).

An ethical clearance was sought from the Namibian University of Science and Technology, Faculty of Computing and Informatics Research Ethics Committee before commencing with data collection. Consent was also sought from each research participant, and these were the opening statements of the online questionnaire and interview guide. The consent clearly highlighted the aim of the study and that the collected data will be used solely for the purpose of this study and will be kept confidential. If a participant took part in the study, this simply means they agree and have given consent. Additionally, the enterprise that gave consent for the study to be conducted within their organisation was kept anonymous and confidential.

3.10 Chapter Summary

The chapter outlined the research methodology that was followed to address the research questions and meet the research objectives. Below Table 3.2 summaries the research design.

Table 3.2: Summary of the research design

Level of decision	Choice
Research choice	Qualitative
Research philosophy	Interpretivism
Research approach	Inductive
Research strategy	Mono case study
Data collection tools	Online questionnaire, interview and literature review
Sampling	Purposeful random sampling
Data analysis	Qualitative content analysis

CHAPTER 4: RESEARCH FINDINGS AND DISCUSSIONS

4. TOWARDS A BYOD SECURITY AWARENESS MODEL FOR MOBILE DEVICE USERS

4.1 Introduction

The chapter presents the findings from the data collected from the enterprises. Research data collection was carried out using qualitative data collection methods namely interviews and an online questionnaire as outlined in chapter 3. Views expressed by those that access work resources through mobile devices within the enterprise through online self-administered questionnaire are presented in this chapter. Furthermore, the data gathered through interviews that were conducted with the IT officials are also presented under this chapter. The interviews were conducted to obtain an in-depth and better understanding of the level of BYOD security awareness among the employees of the enterprises.

4.2 Research Questionnaire Results

A self-administered online questionnaire to be found in Appendix B was developed by the researcher using Google forms and used as a data collection tool for the study. For data analysis, the questionnaire was categorised into 3 main categories as presented in table 4.1.

Table 4.1: Categories/focus of questionnaire questions

Question number	Focus
1 – 2	Characteristics of the study sample
3 – 12	Knowledge and awareness of BYOD cyber threats
12 – 18	Enterprise involvement in curbing BYOD cyber threats

4.2.1 Characteristics of the study sample

The first part of the questionnaire was intended to gather biographical information about the research participants. They were prompted to indicate their department name with the objective to establish whether there is a significant difference of knowledge and the opportunity of identifying BYOD security awareness levels among the mobile device users within the enterprise. Figure 4.1 summarises the participant demographics.

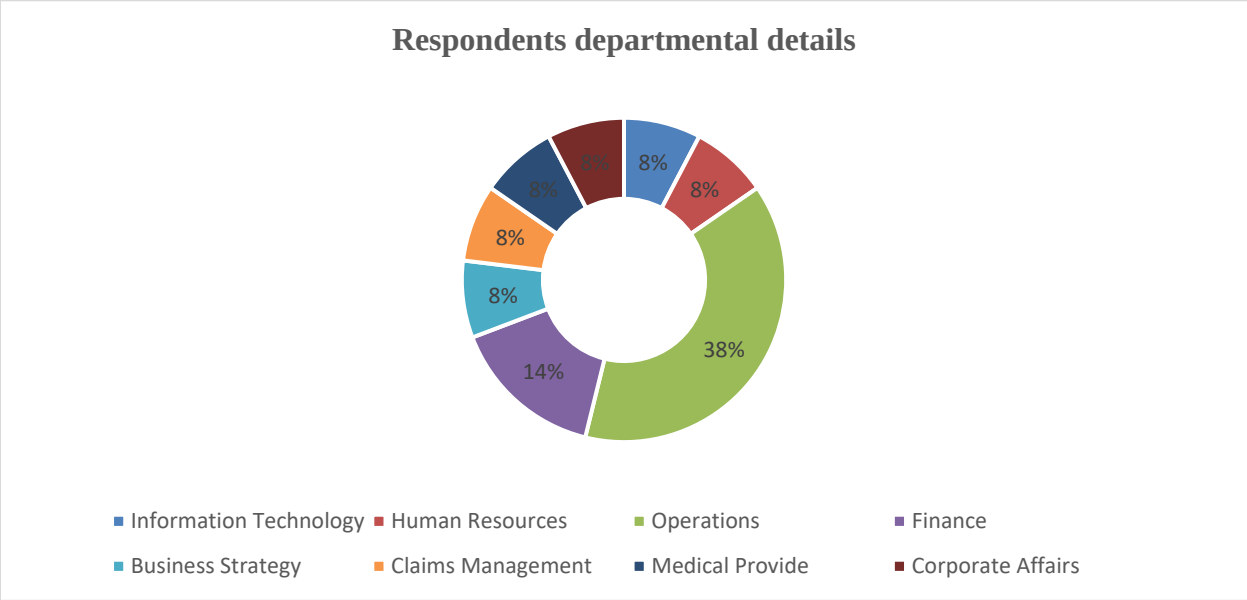


Figure 4.1 Research participants

A total of thirteen (13) respondents completed the online questionnaire. The enterprise has eight (8) departments which were all represented in this study. Majority of the research participants were from the Operations department which represents 38% of the participants, followed by the finance department which represent 14% of the participants. All the other departments namely Information Technology, Human Resources, Claims Management, Medical Provider, Corporate Affairs and Business Strategy were represented equally with 8% each. This diversity represents typical end user in security critical security positions as they handle and process Personally Identifiable Information (PII), financial data as well as ensure cooperate security. According to Rouse (2018), the most challenging elements of cybersecurity is the continually evolving nature of security risks and advanced persistent threats (APTs). The diversity within the enterprise could also have an impact on the security of the enterprise data.

All the research participants acknowledged that they own mobile devices and Figure 4.2 depicts the types of mobile devices they own. Samsung and Huawei mobile devices are topping the list with an equal

representation of 38% of the research participant responses. IPhone device users are represented with 24% and none of the respondents have Hisense or other mobile device brands. Fogden (2019), highlighted that Samsung, apple, Huawei, Motorola, Nokia, Sony are some of the best mobile device brands and that the leading global mobile device brands include leading players with a strong global presence. Overall, the enterprise reflects mobile device brand popularity.

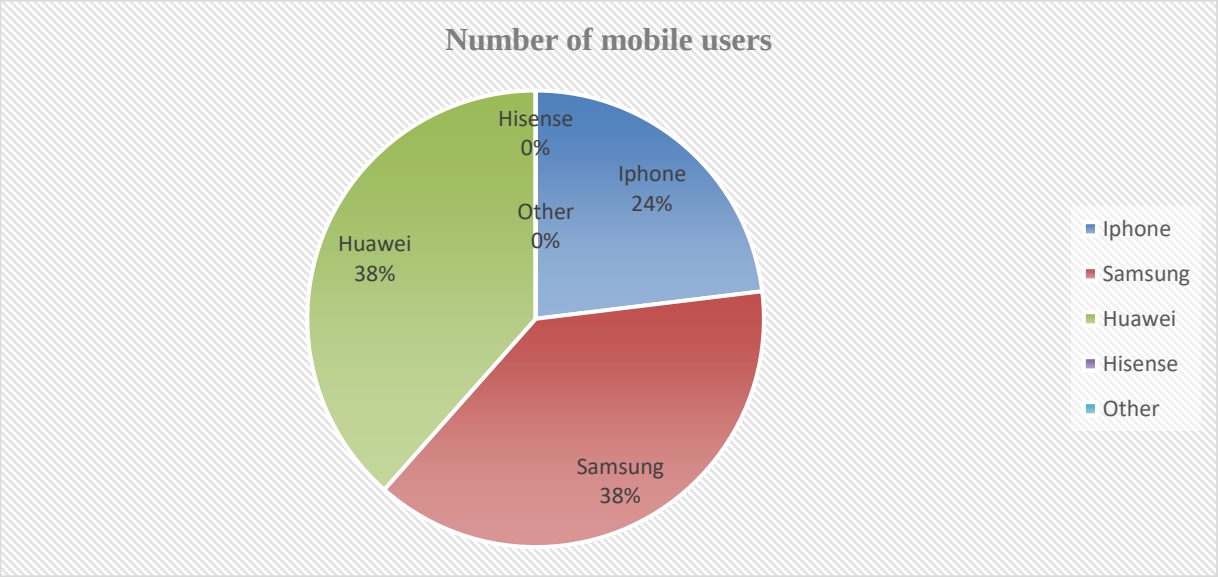


Figure 4.2 Brands of mobile devices owned by respondents

4.2.2 Knowledge and awareness of BYOD cyber threats

This section is aimed at obtaining information regarding users' understanding and awareness of BYOD. The participants' BYOD knowledge and awareness levels were assessed by evaluating their exposure to BYOD cyber threats. Question 4 to 12 of the questionnaire were designed to meet this objective.

Although all the participants own mobile devices that they take along with to work, most of them acknowledged that they are not allowed to use their personal devices to access, store or transfer the enterprise data. Based on the responses, the enterprise does not have a BYOD policy in place yet that governs this, nor the employees informed to conduct such exercises. Dunham (2018) highlighted that the security policy is the foundation of a good security program, as the users will understand the what, why, who of the enterprise security program, thus mitigating the enterprise risk. Furthermore, the goal of such a policy is to address the security threats and implement strategies to mitigate BYOD security vulnerabilities. Below are the activities that respondents perform on the mobile devices namely:

- making phone calls
- sending text messages
- accessing emails for example requesting for quotations
- social media
- web browsing
- authorising payments
- making bank transfers

The actions as listed above, that user performs on their mobile devices expose them to BYOD security threats such as malware, data leakage and *Distributed Denial of - Service* (DDoS) as shown in table 2.1 (Ronwyn, 2016). This is coupled with the fact that only one employee out of all the respondents is aware and understands Bring your Own Device and this employee is from the Information Technology department, which has adverse implications on the organisation security (Ronwyn, 2016) The other respondents from the other departments namely: Human Resources, Finance, Operations, Claims Management, Business Strategy, Corporate Affairs and Medical Provider acknowledged that they are not aware of BYOD.

The research participants' responses on whether the enterprise has an information security team, 65% of the participants are aware that there is a security team within the enterprise, 18% do not know if there is an existing security team and 5% highlighted that there is no security team within the organisation as presented in Figure 4.3. This reflects a lack of orientation among the mobile users of the enterprise which can result in security threats to the enterprise data.

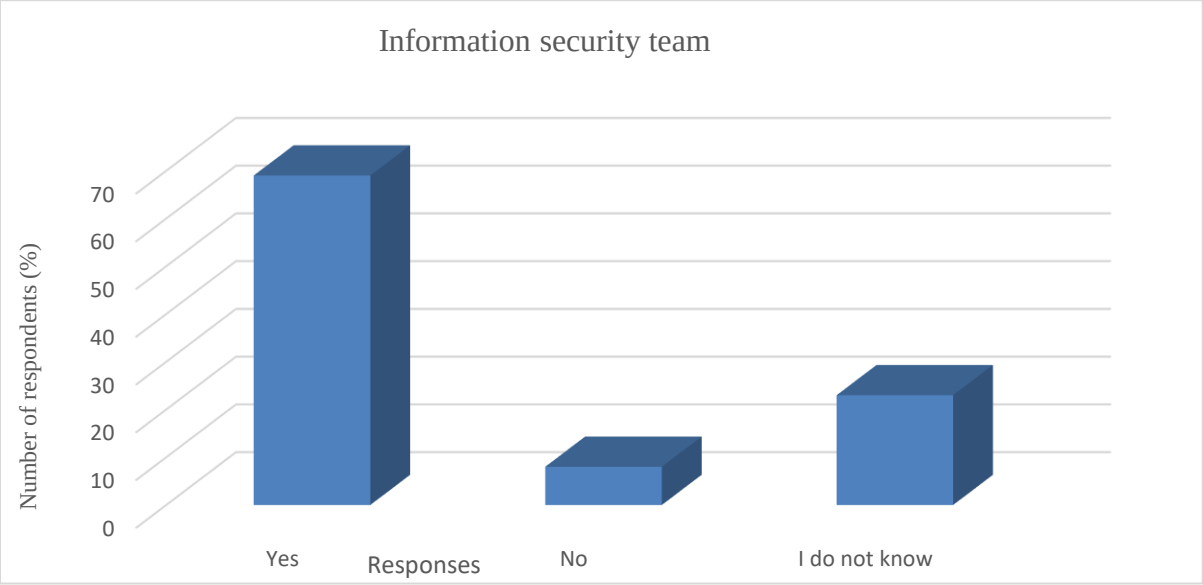


Figure 4.3 Inhouse security team assessment

Respondents were also required to share their opinions on whether they are secure from mobile threats. Of all the participants, 46% of the participants claimed that they are secure, while a substantial number are insecure represented by 39% and 15% are uncertain if they are secure from mobile threats. This compares with findings by Ronwyn (2016) that the lack of security awareness among the users can increase the security threats to an organisation. The findings are presented in Figure 4.4:

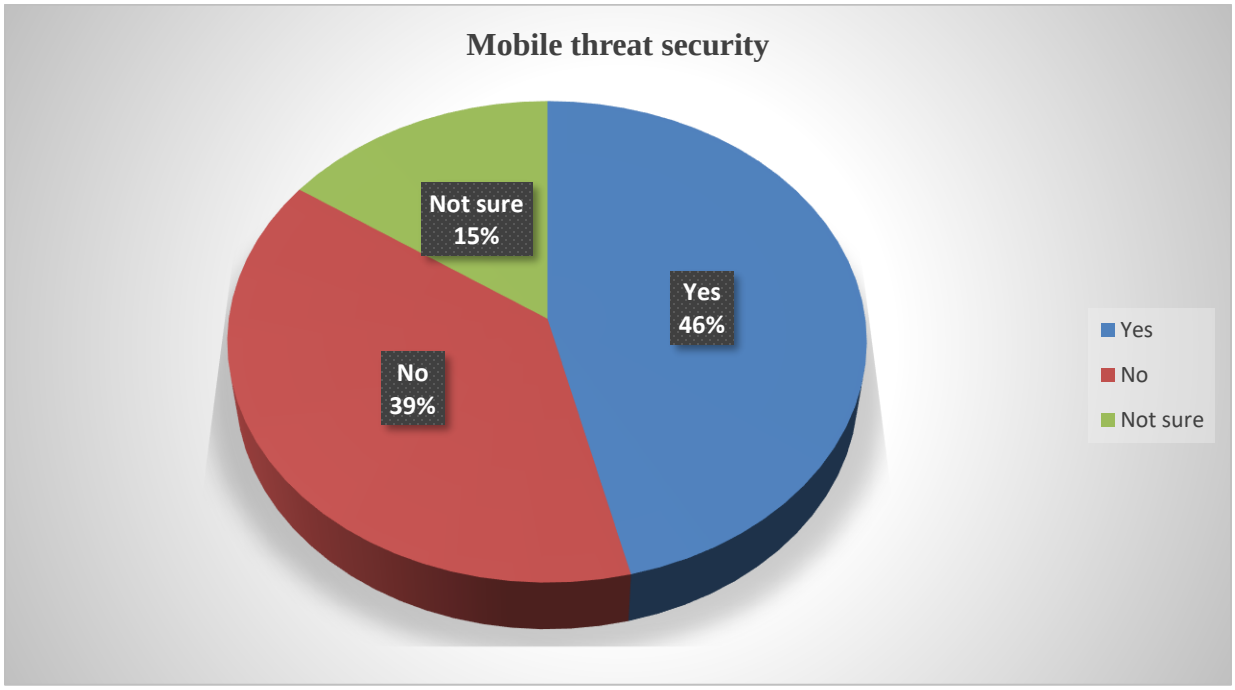


Figure 4.4 Protection against mobile security threats

Mobile security is of great concern nowadays as these devices store crucial information that no one would want to lose nor have it in the public domain**.** The respondents were asked if their mobile devices are configured to install updates automatically and Figure 4.4 shows that most of the participants have this feature enabled on their mobile devices while a minority install updates manually, of concern is a number who do not know if the feature is enabled on their mobile devices or not, which places the enterprise data at risk. This is not surprising as there is no awareness program, or a supporting policy as found in figure 4.8.

The participants were further required to highlight if they can tell when their mobile devices are hacked or infected. The study revealed that 77% of the research participants are aware and can notice when their mobile devices are being hacked or infected with threats whereas 23% are not able to do so as depicted in Figure 4.5, this can be attributed to as a lack of security awareness among the mobile users.

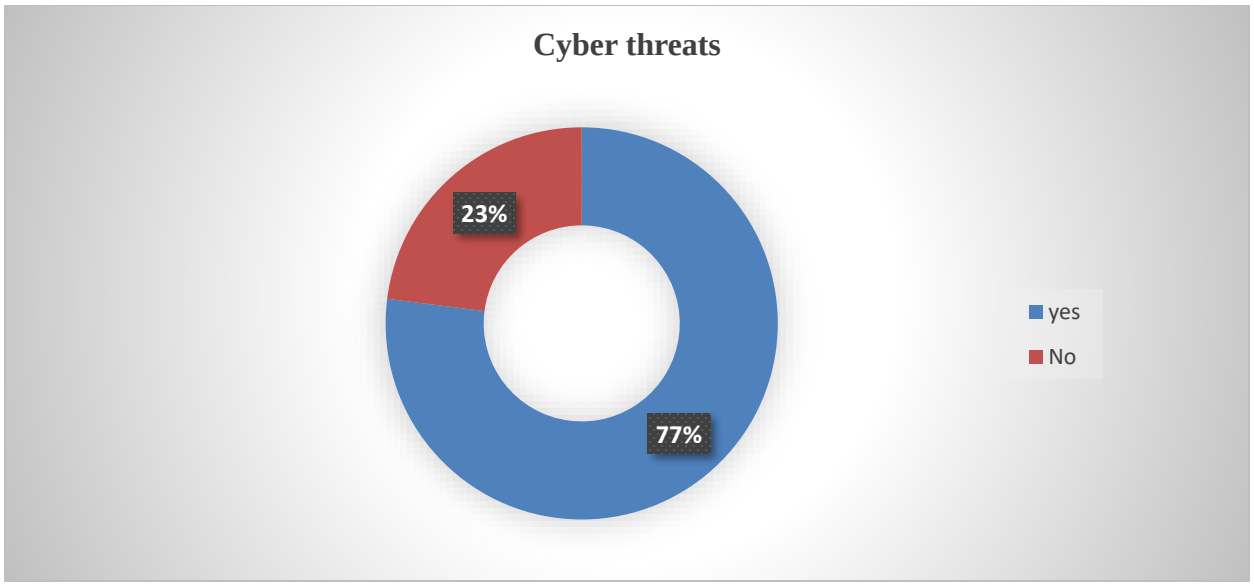


Figure 4.5 Cyber threats identification

In the event where a mobile device is infected or hacked, respondents highlighted that 31% reports to the IT department within the enterprise, 23% reports to Mobile Telecommunication (MTC), 8% reports to an IT student and 38% do not report to anyone. Figure 4.6 reflects where the respondents report malicious activity detected on their mobile devices. Respondents report malicious activities detected to different entities. All participant responses are of interest for this study. The fact that they report to different entities could be due to the lack of awareness and policies that are not in place, similarly to those that do not report at all. This reflects that the enterprise does not have a central point of reporting, or the users were not made aware of the reporting lines.

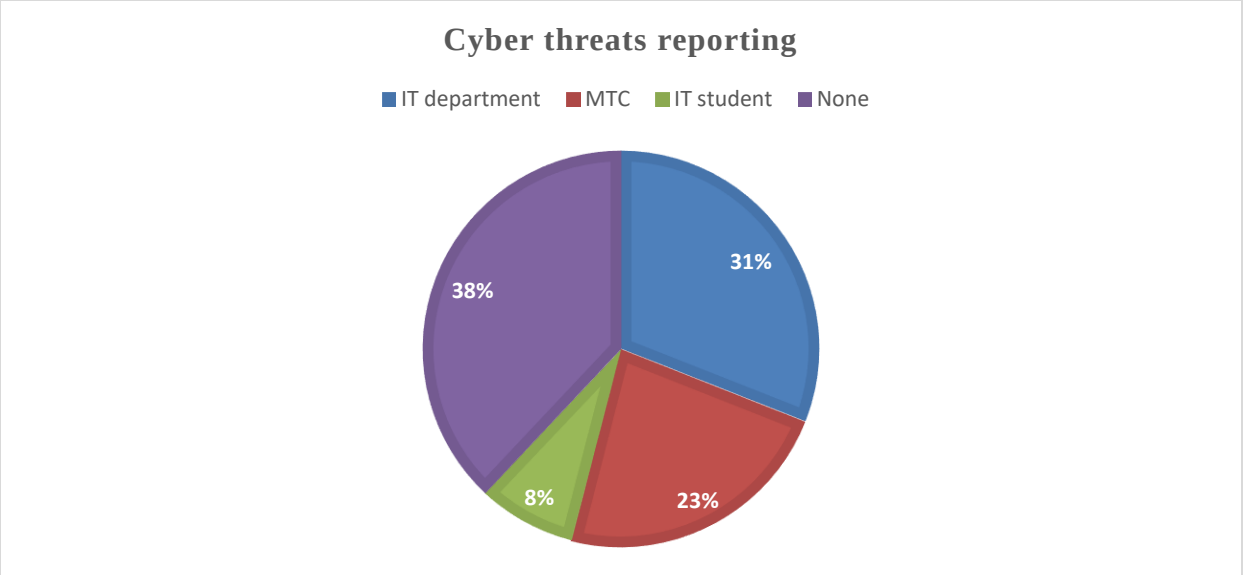


Figure 4. 6 Cyber threat/attack reporting

BYOD implementation increases the flexibility, convenience, portability and employee's productivity and morale as highlighted by Lucas (2020). Mobile devices can be considered as mobile offices as they can be used to access, store or transfer valuable data. Respondents were requested to comment if their mobile devices contain data that is valuable to mobile attackers, 54% of the respondents confirmed that their mobile devices contain such data as shown in Figure 4.7. The following list comprises of the valuable data stored on mobile devices by the respondents:

- Personal information which includes passwords and account numbers
- Emails
- Banking applications

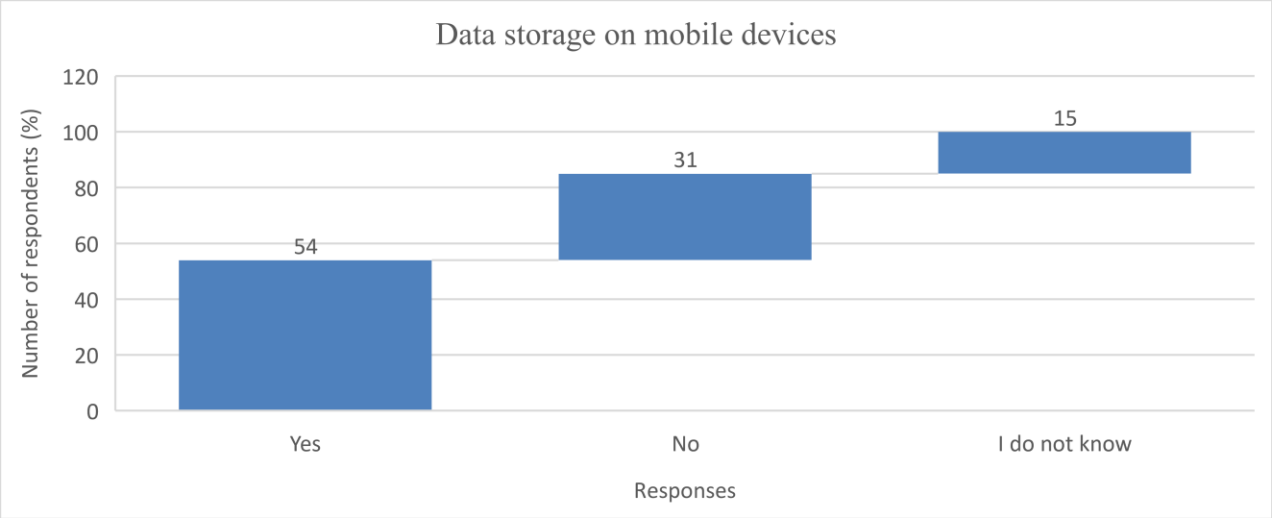


Figure 4.7 Value of data stored on mobile devices

Of the participants 31% highlighted that their mobile devices do not contain data that is valuable to attackers and 15% could not confirm whether they were interesting enough to attackers. This relates to a study by Vrhovec (2016) which revealed that of the lack of security awareness among mobile users make them vulnerable and the target for cyber-attackers.

4.2.3 Enterprise involvement in curbing BYOD cyber threats

Questions 13 to 19 of the questionnaire were designed to assess the enterprise's responsibility/initiatives towards creating BYOD security awareness within its mobile device users. BYOD cyber threats can result in great loses to the enterprise such as data, privacy, money, and means of production, reputation, many more (Ronwyn, 2016). Thus, enterprises need to put measures in place to minimise such loses.

Respondents were required to express the extent to which they know of the existence of a BYOD policy in the enterprise. Their responses are presented in Figure 4.8. None of the respondents are aware of the existing BYOD policy, as they all indicated that they do not know the content of that policy as shared in section 4.2.2. Although the BYOD concept is not formally implemented within the enterprise, this does not mean that the enterprise data is immune to security threats. The fact that employees use their personal mobile device to access enterprise data places such data at risk.

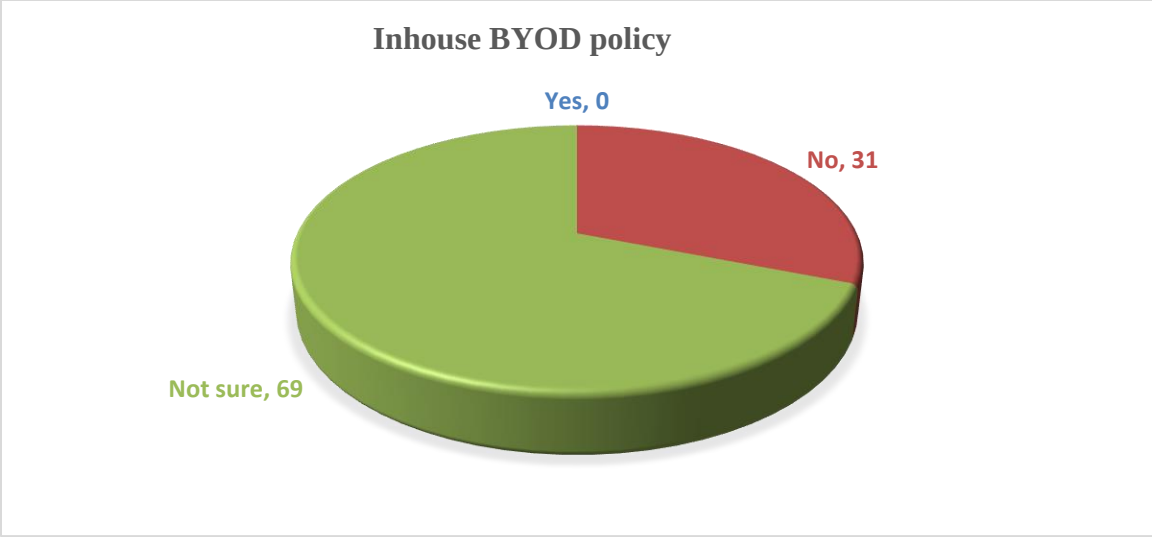


Figure 4.8 Availability of inhouse policy

When they were requested to comment on whether the enterprise offers training to the mobile device users on negative effects of BYOD with the aim to create awareness, 84% of the respondents indicate that they were never offered such training. Furthermore, 8% of the participants could not remember when last they were offered the training and an equal number indicated that training is not being offered most often. Overall, most of the participants highlighted that they were never offered training to increase their BYOD security awareness levels as presented in Figure 4.9. This implies that the security posture of the organisation is at risk. According to Mahoney (2016), 20% of cyber threats exposure occurs due to the vulnerability of technology and 80% because of people. This means, users can be considered as internal threats to an enterprise.

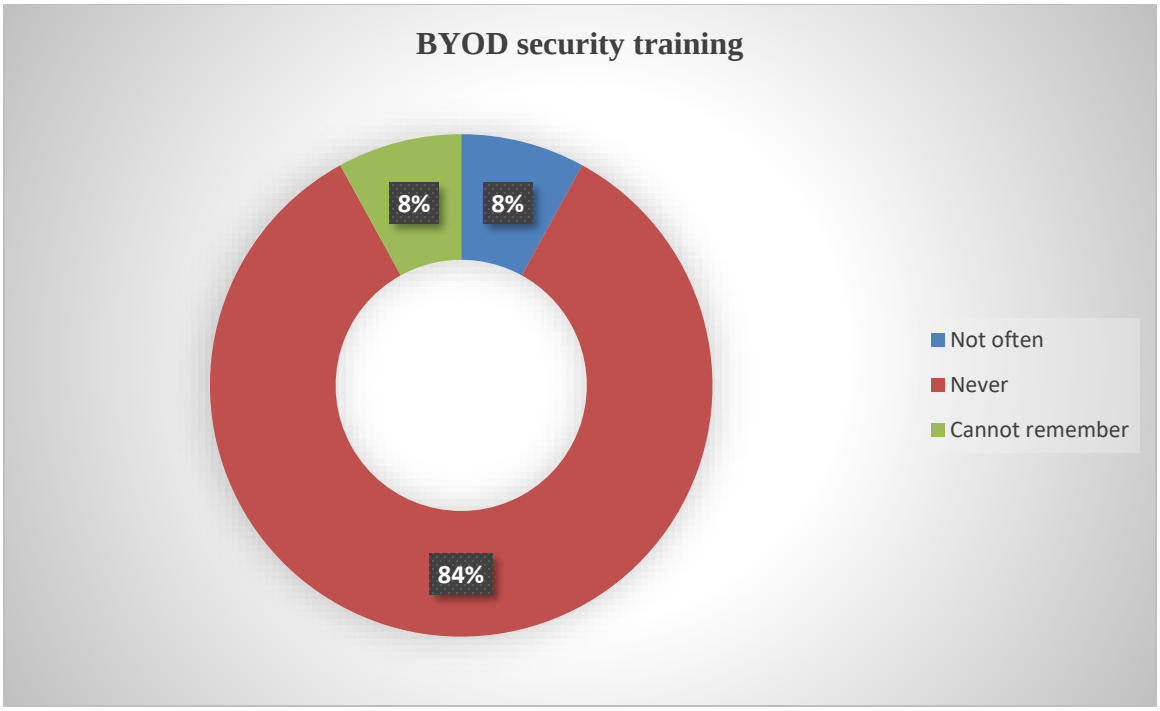


Figure 4.9 BYOD security awareness training intervals

In the section 4.2.2, employees have acknowledged that they keep confidential information on their mobile devices. They were required to share how they keep such information stored on their mobile device secure. Table 4.2 is the representation of their responses where password, pin or pattern is the most popular security strategy followed by antivirus, security settings, google drive, and those that own iPhone, were equally represented. IPhone users highlighted that they are safe from cyber threats since an iPhone is the most secure device and cannot be hacked by attackers. Worth noting is the substantial number of users who do not know how they are keeping the sensitive data safe.

Table 4.2: Means of securing data on mobile devices

Method	Number of respondents	Note
Password, pin or pattern	46%	Participants have this feature enabled when unlocking the mobile device
Antivirus	8%	Participants download and install the antivirus on the mobile device
Security settings	8%	Participants have this feature enabled on their mobile devices and avoid ticking “remember password” when setting up a password
Google drive	8%	Participants store their files on google drive
I don’t know	22%	Participants do not know how to secure the data on their mobile devices
Owns an iPhone	8%	Participants have a perception that an iPhone is the most secure device

Furthermore, the respondents were asked on the measures implemented by the enterprise to reduce BYOD threat and the findings are shown in table 4.3.

Table 4.3: Measures to reduce BYOD threats

Tip	Respondents %
Use password protected access controls	24
Control application access and permissions	11
Control wireless network and service connectivity	11
Keep OS, firmware, software, and applications up to date	7
Back up device data	15
Enrol in “Find my Device” and remote wipe services	2

Never store personal financial data on a device	7
Run mobile antivirus software or scanning tools	8
Beware of free apps	15

The same way computers get infected with viruses, there are a range of threats that affect mobile devices, Francis (2017). Of the participants 24% think the use of password protected access controls is the most secure method against BYOD security threats. The findings show that security awareness is a challenge hence there is need for creating security awareness among users (Alotaibi, et al., 2016).

Most respondents feel using password protected access controls is the safest measure of all in reducing BYOD threats which mean that the respondents do not understand that passwords cannot offer total security as studies have shown that passwords are inadequate to secure personal data (Mahoney, 2016). Based on the findings, although the protective measures highlighted by the researcher are being implemented by the users, a security gap and risk to organisation data can be observed. There is no guarantee for complete data security.

4.3 Interview Results

The interview questions were categorized into four main categories and the findings are presented per section 4.3.1, 4.3.2, 4.3.3 and 4.2.4 as defined in table 4.4.

Table 4.4: Categories of interview questions

Question number	**Focus**
1 – 5	Understanding of BYOD concept and its implementation
6 – 8	BYOD management
9 – 11	BYOD security threats
12 – 14	Preparedness toward BYOD security threats

4.3.1 Understanding the BYOD concept and its implementation

All IT officials that were interviewed have a common understanding of the BYOD concept. Table 4.5 shows extracts of responses given by participants when they were asked to give their understanding of BYOD concept.

Table 4.5: Definition of BYOD concept

"When employees are allowed to bring their electronic devices like mobile phones to work and use them on the work internet etc."
"Bringing your own devices that are not on the company domain"
"When a company permits employees to bring their own devices to work and use them to complete certain work stuff."
"When users are allowed to bring and connect their personal devices to the work network."
"Bringing your personal device to the workplace and access the work's network."
"When users are allowed to bring their personal mobile devices to workplaces and work from their own mobile devices."
"You can use your preferred device."

Despite the interviewees understanding of BYOD, several gaps have been observed from their responses. The researcher observed that there is an informal adoption of BYOD in the enterprises. Furthermore, the interviewees kept on referring to mobile devices rather than being specific. This gives the impression that access control has not been defined with the enterprise. A clear distinction on the type of mobile devices to be used within the enterprise has not been set by the enterprise.

Furthermore, the participants have a greater appreciation of what BYOD can offer to the enterprise and its advantages such as:

- Convenience as the employee is allowed to use the device they are more comfortable with.
- Reduced costs on purchases and maintenance of equipment.
- Mobility of resources as the users can access resources from wherever they are.

Interviewees were required to highlight if BYOD has been implemented in the organisation, Figure 4.10 present the responses.

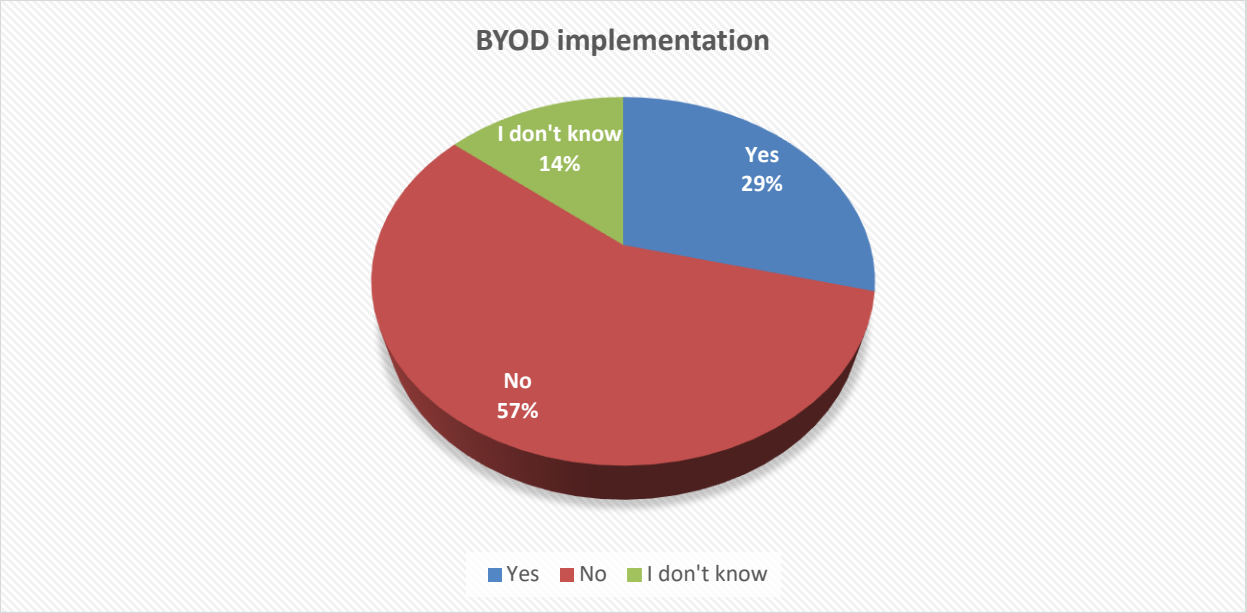


Figure 4.100 BYOD implementation within the enterprise

Of the respondents 57% acknowledged that BYOD has not yet been implemented within the organisation, 29% highlighted that the concept has been implemented and 14% do not know if it has been implemented. These responses are very interesting for the purpose of this study. It is very interesting to find out that even the technical team that is the backbone of organisational security are not sure of the issue at hand. A lack of security and understanding of BYOD was also observed among the technical team. If the technical team is not well acquainted, what more can be expected from the non-technical team. Overall, the researcher observed that BYOD has not been formally implemented within the enterprise.

4.3.2 BYOD management

Even though the organisation has implemented BYOD based on the participants' responses, a larger number of the respondents highlighted that there is no BYOD policy in place and a small number does not know if there is an existing policy in the enterprise that governs BYOD, as highlighted in Figure 4.8. Furthermore, since there is no BYOD policy implemented within the enterprise, there is also no restriction on the type and number of mobile devices that can be used within the enterprise. A BYOD security loophole can be observed among the mobile device users and thus there is a need for the enterprise to implement security measure to protect the enterprise data.

4.3.3 BYOD security threats

The interviewees are aware of the challenges that are linked to BYOD implementation within the enterprise. The following list highlights the challenges that the interviewees foresee that are linked to BYOD:

- Security, which include viruses, network attacks,
- Software and hardware compatibility,
- Maintenance of the devices,
- Enterprise data confidentiality.

Figure 4.11 is a representation of the BYOD related cyber threats as highlighted by the interview participants:

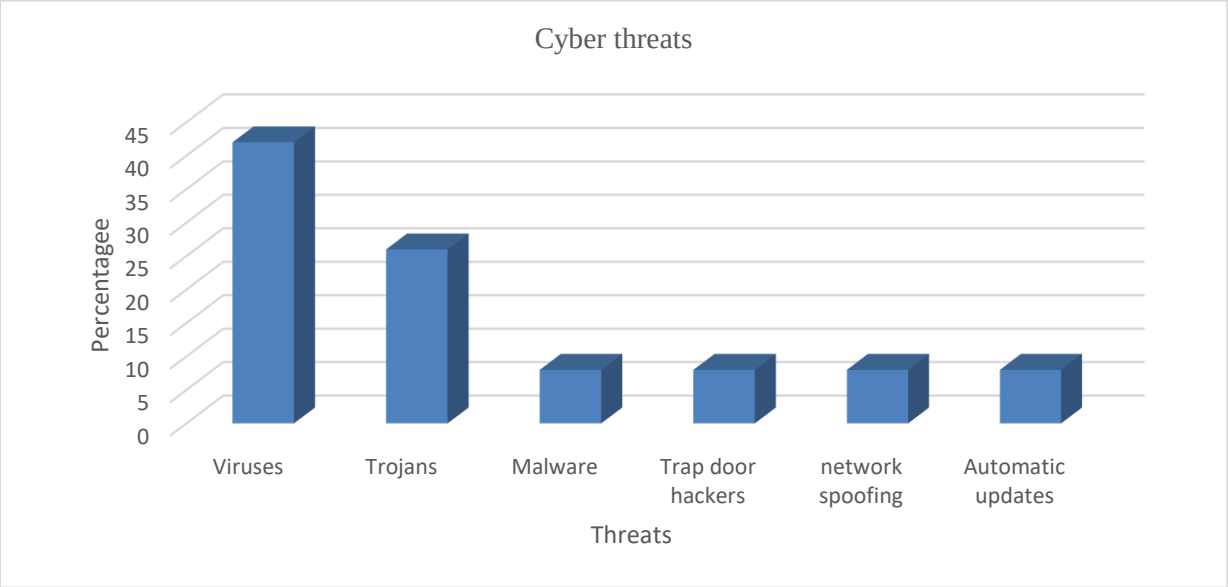


Figure 4.11 BYOD Cyber threats

Several threats have been identified by the interviewees. Based on the finding, the enterprise is prone to viruses represented by 40% of the participants more than any other type of security threat. The enterprise data appears to be at risk and unsecure.

Figure 4.12 represents the data gathered on whether the enterprise has ever experienced a BYOD security crisis.

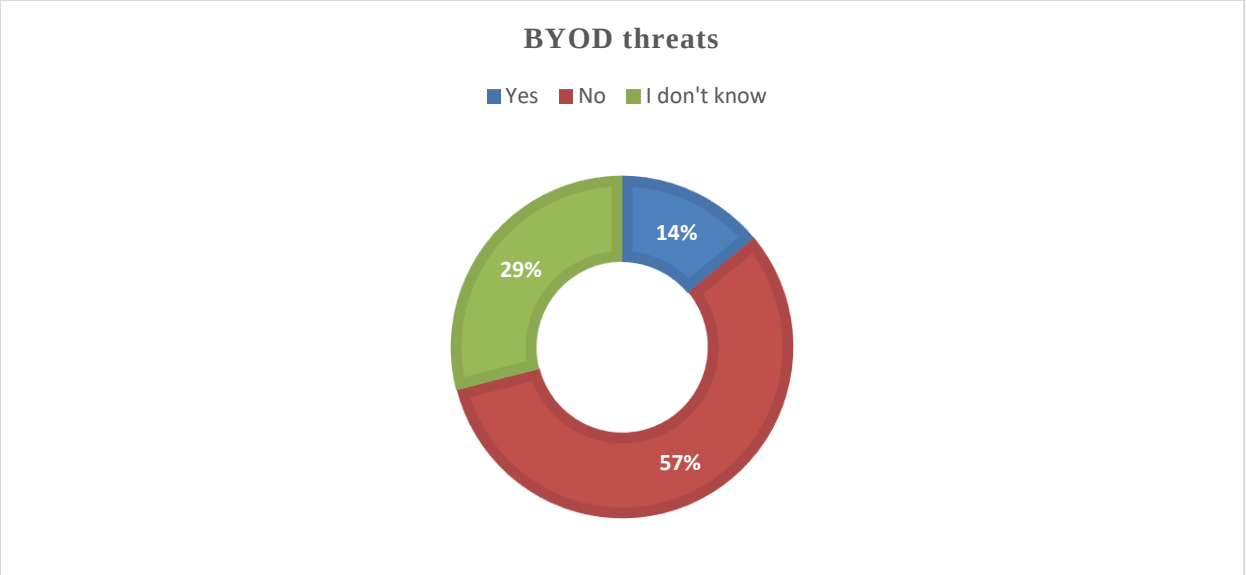


Figure 4.111 BYOD security crises occurrence

Some participants indicated that the enterprise has experienced the BYOD related cyber threats before, represented by 14%. Of interest, is the huge number of participants (57%) who have indicated that the enterprise has never and those that do not know (29%) if the enterprise has ever experienced a cyber threat. The fact that they do not know does not guarantee that the enterprise is safe from cyber threats. It could be that they just do not know because of their limited understanding of the BYOD concept. If the participants do not understand the concept, they are most likely not to be able to identify a cyber threat.

4.3.4 Preparedness towards BYOD security threats

Responding to the question:*" How is the enterprise prepared in case of BYOD security crisis?"*, below are the responses as shared by the participants.

"Still in the pipeline",
"IT team is currently controlling",
"Update enterprise antivirus regularly and perform antivirus scans",
"Enterprise has a firewall".

The participants also highlighted that the enterprise is planning to implement Mobile Device Management strategies as there is nothing in place now. Furthermore, the respondents also indicated that the enterprise has the necessary resources to secure and manage BYOD however they are not sufficient.

Respondents were also required to assess the extent to which the security controls are important as indicated in Table 4.6. Seven (7) participants value authentication over all the other security controls and is the most preferred method of securing data on mobile devices. This could be because authentication is the only security control, they are familiar with. Authentication on its own will not offer complete protection to the enterprise data, thus it must be coupled with other security controls.

Table 4.6: BYOD security controls

Control	Most important	Important	Neutral	Less important	Not important
Authentication	7				
Authorisation	5	2			
Availability	4	2	1		
Confidentiality	4	1			
Non-repudiation	1	3	3		

The participants were also expected to highlight the BYOD related security threats and below is the representation of the findings.

Table 4.7: Categories of BYOD related security threats

Physically-based Threats		Application-based Threats		Network-based Threats		Web-based threats	
Device loss/theft	15%	Malware attacks	15%	Network spoofing attacks	10%	Web browser exploits	10%
Attacks on devices intended for recycling	10%	Inadvertent disclosure of Information	10%	Network exploits	15%	Automatically downloaded applications	12%

Table 4.7 above reflects the categories of BYOD related security threats. The findings reveal that most of the BYOD related threats are application based and such treats include malware, disclosure of information and surveillance attacks. Such threats may occur, and the users might be unaware.

4.4 Discussion of Research Findings

4.4.1 Characteristics of the study sample

Both the respondents for the online questionnaire and interview were selected using simple convenience sampling method, a qualitative sampling technique. This is to ensure that all employees have an equal chance of taking part in the study provided they own a mobile device. Based on GSMA (2017), two thirds of the world population are mobile subscribers. Deloitte (2016) further highlighted that four decades after the introduction of mobile phones, almost every developing country has 90 percent mobile phone penetration. It was anticipated that three respondents from each department should answer the online questionnaire; however, this was not the case as some departments were represented by fewer participants than anticipated, as depicted in Figure 4.1. The simple random sampling technique was implemented to ensure that there is different knowledge that can be used to test mobile device user's BYOD security awareness levels within the enterprise.

In addition to data collected using the questionnaire, 7 IT officials within the enterprise were also interviewed to acquire additional information and verify the information given by the questionnaire respondents. The enterprise deals with confidential data thus it was found fit for this study to be conducted to access the security awareness level of its employees and develop a model that will aid in creating awareness among the users.

4.4.2 Knowledge and awareness of BYOD cyber threats

Security awareness is very crucial in the world of evolving technology as cyber attackers are also trying to find ways to gain access to whatever they need. It is evident from the responses given by the respondents that there are several loopholes that needs to be addressed to ensure the information security of the enterprise. Employees use their personal devices for work purposes; however, they do not know the negative impact of their action can have on the enterprise if not properly handled.

Out of all the questionnaire respondents, only one person is aware of the BYOD concept and this individual is from the IT department. This is a clear indication that participants from the other departments across the enterprise are unaware of the concept which raises a red flag on the security of the enterprise data. Furthermore, employees perform different tasks on their mobile device including work related such as accessing emails for instance to request for quotations, which is also included in the BYOD concept. Based on the findings, it is evident that majority of the employees do not know what BYOD entails and expose the organisation to BYOD related security threats as shown in section 4.3.3.

4.4.3 BYOD implementation within the enterprise

The fact that most of the respondents are not aware of the BYOD concept made it difficult for the non-technical staff to assess if the enterprise has implemented BYOD. The technical staff highlighted that employees are allowed to use their personal devices; however, the concept has not been implemented fully and there is no policy in place to administer this. Since the concept is already in use although it is not formal and some employees are not aware, there is a need to raise awareness among the mobile users because a single inappropriate action can have a devastating effect to the enterprise.

4.4.4 BYOD security threats

Despite a lot of advantages being offered by BYOD such as convenience, mobility, reduced costs increased productivity and many more, BYOD implementation can come or cause security risks or threats also to the enterprise that have implemented it as highlighted under section 4.3.3. Respondents are aware of the potential security threats that are associated with BYOD. The enterprise in which the study was conducted cannot be isolated from this. There are potential threats that can affect the enterprise security considering the activities that the employees are allowed to perform on their mobile device. These activities are listed under section 4.2.2.

4.4.5 Enterprise preparedness towards BYOD related threats

Since the concept is not yet fully implemented, the respondents highlighted that the enterprise does not have anything in place to administer BYOD. The enterprise does not have a BYOD management strategy nor a policy in place to govern this. Based on the responses from the respondents, it is evident that there are several gaps or loopholes that need to be addressed one of them being mobile user awareness as this is the weakest link to BYOD security threats. The human aspect cannot be ignored when addressing BYOD security threats, as users are considered to be the weakest link as highlighted by Flores et al. (2016).

4.5 Conclusion

The data presented above was collected using interviews and an online self-administered questionnaire conducted with the mobile device users within the enterprise. The researcher has observed the lack of end user awareness on BYOD security. Furthermore, their responses reflected a little bit or limited knowledge of BYOD and its effect to the enterprise. Both the technical and non-technical staff reflected a limited level of BYOD security awareness. More interestingly, the technical team is the backbone of the enterprise's security, and if it has limited understanding of the BYOD concept, then it will not be able to address the security loopholes within the enterprise.

The enterprise does not have an existing BYOD policy, and this could be because of the limited understanding of the concept by the technical team. The fact that the BYOD concept has not been formally implemented within the enterprise does not mean that the enterprise data is not prone to attackers. The enterprise appears to be at risk of BYOD threats and Figure 4.12 supports this finding. Users are the weakest link and by allowing mobile users to use personal devices within the enterprise poses a great security risk to the enterprise.

Some security risks and loopholes were identified that needs to be addressed for the enterprise to be prepared and safe from BYOD related security threats. Based on this, it is evident that there is a huge gap and need to create BYOD security awareness model to create awareness among mobile device users of the enterprise.

Safeguards and risk awareness are the first line of defence for the information systems security, as highlighted by the European Network and Information Security Agency (2018). Awareness is understanding the risk.

The components of the model informed by these findings are:

1. **Policies:** This refers to the importance of the security policy that mobile users should adhere to for effective security of their personal and enterprise data accessed or stored on their mobile devices. Alton (2017) highlighted that a recent survey that was conducted suggests that 39 percent of businesses have a formal BYOD policy, a number that is considered low and still growing, while other businesses allow their employees to use personal mobile device with no formalised policies. This is also the case in this study, the enterprise does not have existing policies to govern the BYOD usage within the enterprise.

2. **Users:** The users need to be aware of the BYOD related threats they are exposed to. Human error is a huge risk to an organisation; thus, users should be aware of how to mitigate the threats they are exposed to, Bapat (2018). Based on the findings in this study, it was observed that the users within the enterprise are unaware of the threats they are exposed to, which is risky to the enterprise and their personal data stored on mobile devices.

3. **Security controls:** Mobile device users must be aware of the security measure they can implement to secure the information. The organization should also define the number and types of mobile devices to be connected and when to connect on the enterprise network. Currently, the enterprise has not clearly defined such control.

4. **Awareness:** This involves acceptable and secure behaviour expected from the mobile users for increased security. A lack of BYOD security awareness has been observed among the mobile users in the enterprise, thus there is a need to raise awareness among such users.

4.6 Chapter Summary

The present chapter presented the findings which where extracted from the collected data. A thorough discussion was also provided. The next chapter (Chapter 5) presents the Model Design process.

CHAPTER 5: MODEL DESIGN PROCESS

5.1 Introduction

The chapter focuses on defining the components for and the development process of the BYOD model for creating security awareness among mobile users within Namibian enterprises. It begins by identifying the components of the model based on the findings highlighted in chapter 4, these are presented in section 5.3. Following on that is a description of the Design Science Research (DSR) method, the model is then designed in section 5.4.

5.2 The Model's Rationale

BYOD implementation offers great benefits such as increased productivity, reduced costs, flexibility and convenience to enterprises that have implemented the concept Procedia Computer Science (2016). However, little attention has been paid to the security aspect associated with BYOD implementation and the security threats it imposes on the enterprise. Most companies leave security to the end user (Alotaibi et al., 2016). Brook (2020) highlighted that beside many reasons to adopt the BYOD initiative, it is equally important to consider how employee's attitudes towards BYOD affects the enterprise security posture, hence this is the motivating factor behind the design of The BYOD Security Awareness Model (BYOD-SAM). Another factor that contributed to the need for BYOD-SAM is the results highlighted in chapter 2 section 4.2.2. The results clearly show that there is lack of security awareness in the organisation that was studied. The BYOD Security Awareness Model (BYOD-SAM) will be a guideline to Namibian enterprises in creating BYOD security awareness among their mobile device users with the aim to safeguard the organisational data. Furthermore, the model is a guideline on how enterprises can raise BYOD security awareness among users within their enterprises and improve the enterprise security posture.

5.3 BYOD Awareness model building process

The BYOD-SAM development was guided by literature review and primary data collected through interviews conducted within Namibia Motor Vehicle Accident Fund (MVA) and a questionnaire distributed within the said enterprise. The proposed model will be instrumental towards creating BYOD security awareness among employees within the enterprise. Figure 5.1 illustrates the research design followed in the development of the model:

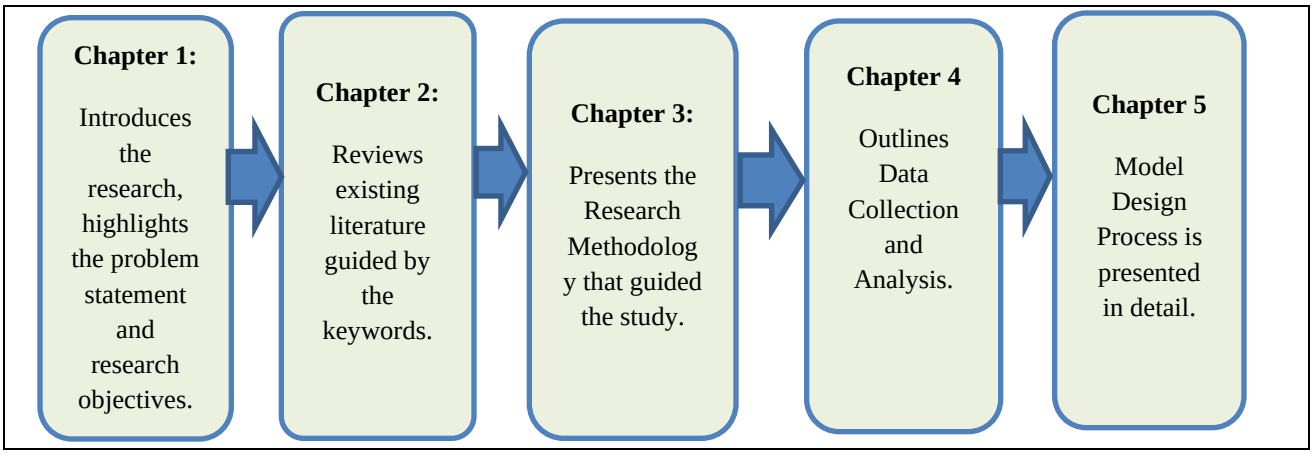


Figure 5.1 Steps for developing the BYOD security awareness model

Figure 5.2 outlines the application of Design Science Research (DSR) by Peffers (2006) that was used to design the BYOD-SAM.

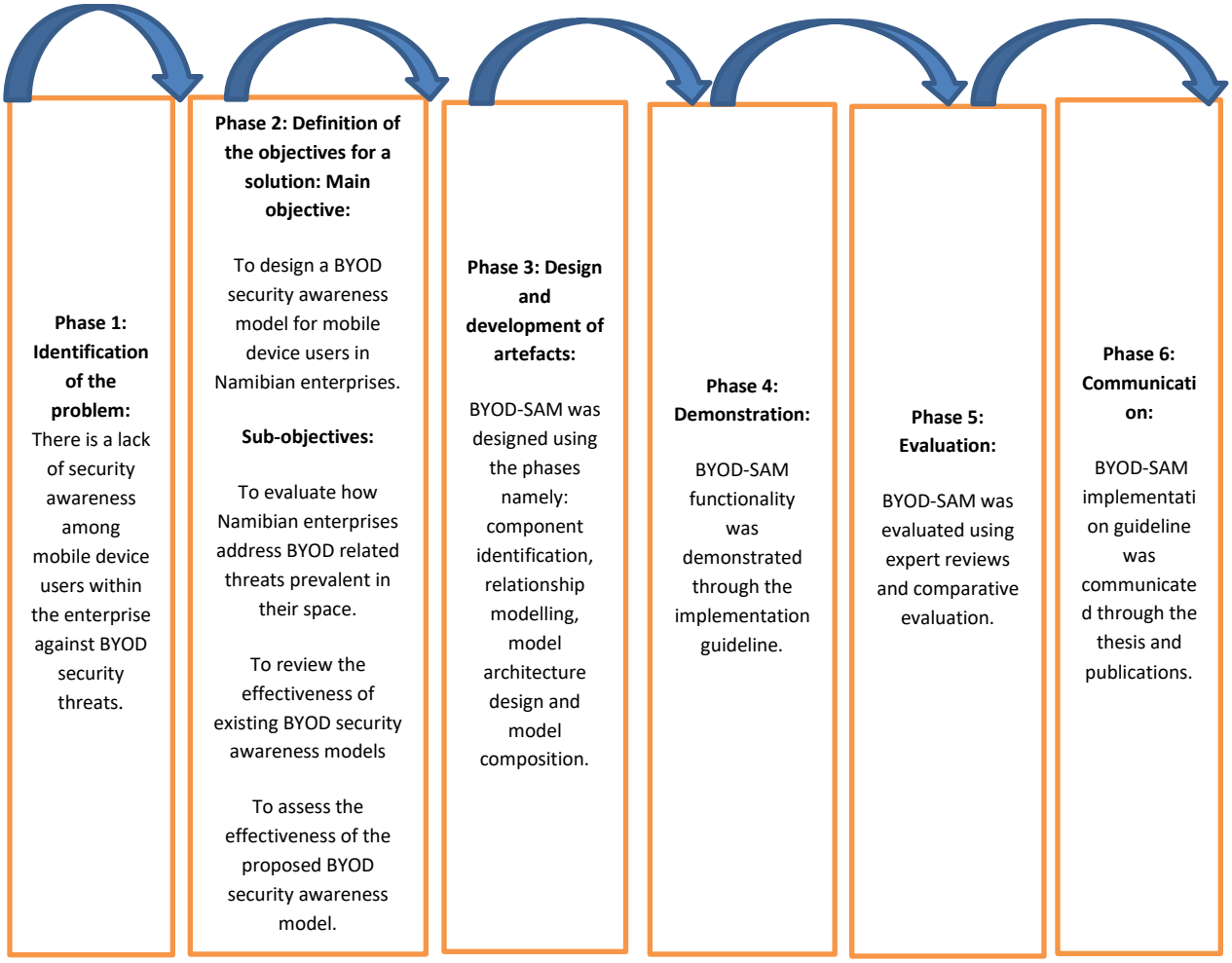


Figure 5.2 The Design Science Research

5.3.1 Phase 1: Identification of the problem

From literature, it was established that enterprises are enjoying the benefits of BYOD, which allow them to cut operational costs as they do not need to purchase computers for their employees. Employees are enjoying the comfort and convenience offered by BYOD; however, as they access company resources this exposes organisation to security breaches through poorly secured personal devices introduced to the work environment.

It was established that despite the benefits mentioned above:

There is a lack of security awareness among mobile device users within enterprises against BYOD security threats.

After identifying the problem, ways in which to advance awareness amongst mobile users were explored.

From literature it was established that to increase BYOD security awareness then:

1. Mobile device users should be educated of the BYOD related security threats they might be exposed to.
2. Mobile device users should be educated of BYOD security measures to safeguard the enterprise data.
3. Mobile users should also be educated on the mobile usage protocols within the enterprise.

How then can an enterprise educate mobile device users about BYOD security threats? How can enterprise advance knowledge on BYOD security measures and train mobile device users on the proper mobile device usage protocols? To comprehensively address the questions, it was imperative to design the BYOD-SAM that will assist in advancing BYOD security awareness.

5.3.2 Phase 2: Definition of objectives for a solution

The second stage was to determine what the model should do. To find out what the model should do, the following questions were answered using literature, interviews and questionnaires as described in chapter 2 and chapter 4 respectively.

- How do Namibian enterprises address BYOD related cyber threats?
- How effective are the existing BYOD security awareness models?

Literature informed the researcher that the model should:

1. Help mobile device users understand the challenges linked to BYOD implementation within an enterprise, chapter 2, section 2.2.2.

2. Make mobile users aware of the BYOD security related threats and its implications on the enterprise, chapter 2, table 1.

3. Educate mobile users on how to preserve the data store/accessed with their mobile devices, chapter 2, section 2.2.4.

From the interviews and questionnaire, it was established that the model should:

1. Help mobile device users understand and appreciate the importance of BYOD security implementation in an enterprise, regardless of their role in an organisation, chapter 4, section 4.2.2.

2. Educate mobile users on the means for securing data on their mobile devices to reduce BYOD security threats, chapter 4, table 4.2 and 4.3.

3. Educate mobile users on the BYOD security threats they are faced with and how to identity such threats, chapter 4, section 4.3.3

Putting all this together shows that the model was supposed to:

- Educate mobile end users of the BYOD related security threats,
- Help enterprises develop adequate BYOD security policies,
- Raise BYOD security awareness among users within enterprises,
- Educate mobile users on the means for securing data on their mobile devices to reduce BYOD security threats.

5.3.3 Phase 3: Design and development of BYOD awareness model

This phase comprises of:

1. Component identification
2. Relationship modelling
3. Model architecture design
4. Model composition

1. Component identification

The components of the proposed BYOD awareness model were derived from the data collected via the research findings discussed in chapter 4. The model components were identified from the primary and secondary data sources. Primary data sources included the interviews and questionnaires described in chapter 4, whereas secondary data source is literature review. Based on the research findings highlighted in chapter 4 section 4.4, the components of the awareness model that were identified include:

- Policies as found in sections 2.2.2 and 4.2.2,
- Users section as established in 2.2.2 and 4.4.5,
- Awareness program highlighted in sections 2.2.2 and 4.2.3,
- Technical controls as presented in sections 2.2.4 and 4.2.3,
- IT Administration as found in sections 2.2.4 and 4.3.1.

Component validation defines the validation of each construct used during the development of the model. Literature review as outlined in chapter 2 and the research findings outlined in chapter 4 validates the constructed model.

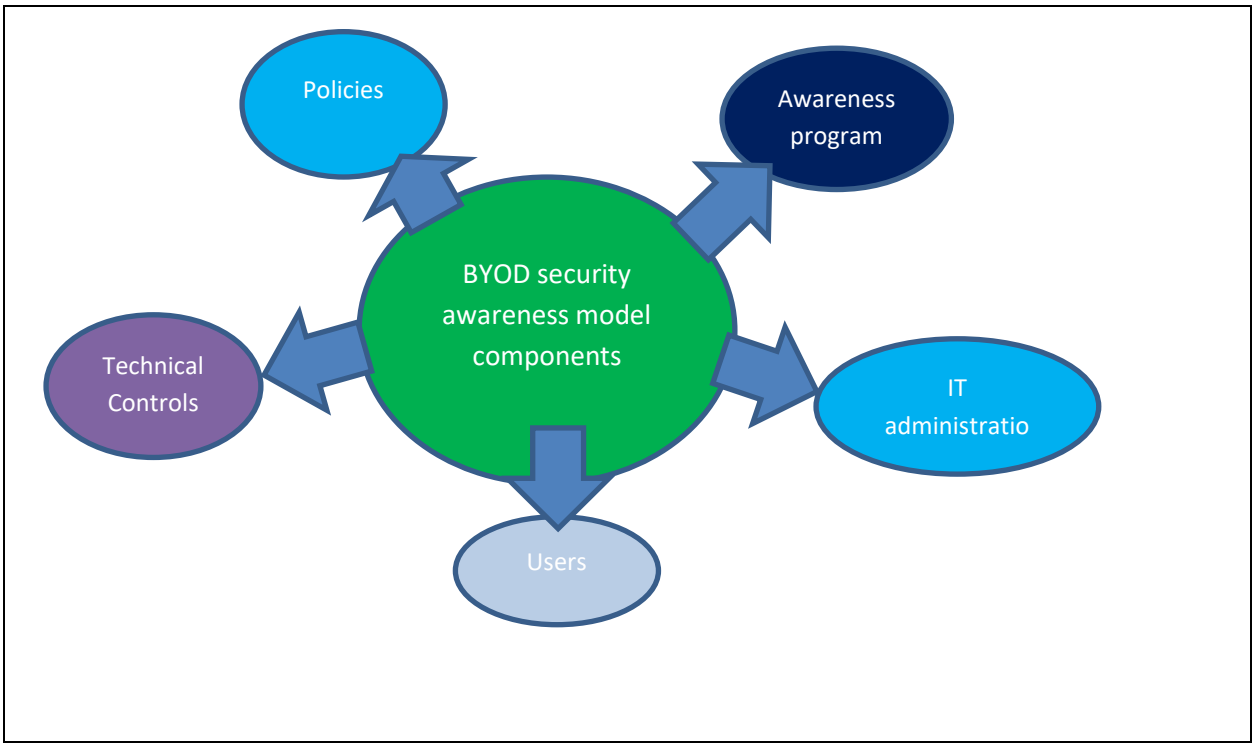


Figure 5.3 Components of the BYOD security awareness model

5.3.3.1 Policies

The BYOD policy defines the guidelines for employees' use of personal owned mobiles devices for work related activities (Cheatham, 2019). Information Technology consumerisation has pointed out the necessity of BYOD policy development. Such policies offer great benefits to enterprises that have implemented BYOD such as reduced costs, convenience, up-to-date technology, preference and efficiency. It is always critical to think about how these policies will have an impact on the enterprise. The policies should always reflect the enterprise needs.

It was observed that the case enterprise does not have BYOD policies in place although the concept has been partially implemented within the enterprise as outlined in section 4.3.2. The employees are using their personal devices for work purposes although they have not received authorisation in writing which can cause potential risks to the enterprise data. However, having well defined policies and procedures can reduce security threats and misuse of resources. As highlighted in section 2.2.2, mobile device users must be aware of the security measures they can implement to secure the information. BYOD is subject to several threats because the devices involved do not belong nor controlled by the organisation.

By not having a BYOD policy in place, this means the enterprise has limited or no control over the data that is being accessed or stored on such mobile devices. The traditional workplace is becoming a thing of the past thus, enterprises need to be prepared for security risks associated with BYOD implementation.

Furthermore, the COVID-19 pandemic has disrupted the way of doing business resulting in teleworking and thus most employees were forced to use their own devices and networks to do their office tasks. The purpose of the policies will be to: *educate the mobile users on the types of BYOD related security threats and the acceptable BYOD usage protocols within the enterprise, the custodians ideally will be the IT department and should be reviewed every 6 months. The policies should cover acceptable use, devices and support, security, risk/liability and reimbursement as established in section 2.2.4.*

5.3.3.2 Users

Users are one of the inherent downsides of BYOD implementation as established in sections 2.2.4 and 4.1.2. The same way computers get infected with viruses, there are a range of threats that affect mobile devices (Francis, 2017). Vrhovec (2016) revealed that many mobile device users do not mind about security threats and how they affect them. Without any doubt, there is an increase in mobile device threats and attacks. As highlighted in section 4.2.2, it was observed that the users within the enterprise are unaware of the threats they are exposed to, which is risky to the enterprise and their personal data stored on mobile devices. Furthermore, BYOD adoption presents network security threats. *The purpose of this component will be to uplift and maintain BYOD security awareness with the aim to safeguard the enterprise data.*

5.3.3.3 Awareness program

NIST Publication 800-53 (2020) maintains that training helps ensure that the authorised individuals do not abuse their authority whereas awareness's primary purpose is simply to focus attention on security by allowing individuals to recognise potential threats and respond accordingly. ISO27001 focuses on how to be a secure user and how to respond to various security incidents, which overall protects the organisational data. This component primarily focuses on promoting risk and threat awareness among the mobile users within the enterprises. The enterprise is recommended to consider organising quarterly sessions with the staff member to remind them about BYOD security and other developments that evolves around it based on new developments in the information technology field. According to Hoenich (2019), most organisations bind to a yearly awareness program at the very least whereas many are shifting to monthly training.

With the popularity of BYOD implementation over the past decade, awareness is a key aspect to be considered by enterprises that have implemented it (Rice, 2016). Based on primary findings, as outlined in Figures 4.4 and 4.5, a lack of BYOD security awareness has been observed among the mobile users in the enterprise and it is very crucial for the enterprise to enhance user BYOD security awareness since the BYOD concept has been partially and informally implemented within the organisation as discussed in section 4.3.1. The purpose of this component is to enhance the BYOD security awareness levels of the mobile device users within the enterprise.

5.3.3.4 Technical controls

1. Access Control

Allowing unmanaged mobile devices to access the enterprise network without security measures in place poses huge security threats to the enterprise as demonstrated in section 4.2.3. Access control should be enforced on the enterprise network. Currently, the enterprise has not clearly defined such control as highlighted in section 4.3.1. The enterprise should consider using the Mobile Device Management (DMD) for this purpose Ferrill & McAllister (2023). RSI Security (2019) highlighted that access control regulates the flow of data and orders how a user or system can access with other systems or resources. *The purpose of this component is to confirm that any user that attempts to access the enterprise data confirms that they are who they say they are and have been approved to access such data.*

2. Software updates

This is a very crucial safeguarding strategy as it updates patch vulnerabilities with the device operating system and applications installed on its sources. It was observed that 54% of the users within the enterprise being studied do not appreciate the importance of software updates, as presented in table 4.3. Some users dismiss these updates and see them as a potential waste of time. By simply clicking "update now" users can prevent many security breaches, Savage (2018). Mobile users will need to be informed about the importance of software updates and be advised to schedule it on their mobile devices. Automatic updates will be enabled on users' mobile devices and it is the responsibility of IT administration to monitor this. According to Infoguard Cybersecurity (2017), software manufactures continuously identify loopholes in their applications and release patches or updates to close such loopholes. *The purpose of implementing software updates is to close any existing loopholes to prevent the attackers from exploit the enterprise resources.*

3. Authentication

Mobile device authentication simply means verifying the user's identity or the device itself for secure access Campagna, Iyer, Krishnan & Bauhaus (2016). Since mobile devices have become smarter, they are now filled with vital data that need to be kept confidential, thus they need to be secured from unauthorised use. Gebel (2018) defined authentication as a method of validating the identity of a registered user trying to gain access to data resources. Such methods of validating the identity includes passwords, patterns, fingerprints, facial recognition, pin number and the enterprise needs to enforce such authentication methods on users' mobile devices. IT Administration will ensure that all mobile devices connecting to the enterprise network are authenticated with a password as highlighted in section 2.2.4. *The purpose of this component is to ensure that only the authenticated users have access to the enterprise data, which will help keep the enterprise network secure.*

4. Firewall

Firewalls act as a shield to prevent unauthorised access to and from the enterprise network (Damjanovic, Korać & Simić (2020). The size of the network does not matter, whether small or big, they both have the

same security risks. Based on section 4.3.4, the enterprise does not have a firewall in place, which makes them vulnerable to security threats. The firewall should be installed on every mobile device connecting to the enterprise network to inspect incoming and outgoing traffic which will help mitigate the security threats. *The purpose of this component will be to filter all traffic entering and leaving the mobile device.*

5. Antivirus

An antivirus acts as a policeman at the gate of a mobile device system. It can protect a mobile device from online threats such as viruses, malware, phishing attacks, spyware and other cyber threats (National Cyber Security Centre, 2019). Based on the survey responses, only a small number of participants have downloaded and installed the antivirus on the mobile devices as shown in chapter 4, table 4.2. A mobile device can be compared to a house with an open door, it can attract all intruders. Similarly, a mobile device without an antivirus is prone to a lot of cyber security threats. It is thus very important for mobile device users within the enterprise to be encouraged to install and frequently update the antivirus on their mobile devices to safeguard the data stored on them as highlighted by Davis (2017). *The enterprise will need to procure a licensed antivirus to be installed on mobile devices that connects to the enterprise network. The purpose of this component is to protect the mobile devices from incoming threats.*

5.3.3.5 IT Administration

According to Loew (2018), IT Administration is the backbone to the information security of any enterprise. They will be responsible for accessing, proposing, implementing and monitoring the security needs of the enterprise. Furthermore, they will play an important role in creating BYOD security awareness among the mobile users within the enterprise. IT Administration will assist with the development of policies, choice and implementation of the technical controls for the enterprise. Additionally, they will spearhead the awareness program and monitor user's awareness levels. *The purpose of this component is to promote and enhance BYOD security awareness among the mobile users through the awareness program, defines, implements and owns the technical controls and policies set by the enterprise*.

2. Relationship between components

This section presents the relationship between the components used to develop the model as depicted in Figure 5.4.

R1: IT administration will influence and assist with the development of policies for the enterprise.

R2: IT administration will also assist with the choice and implementation of the technical controls.

R3: The policies will clearly define the technical controls as approved by the enterprise.

R4: Policies will define what IT administration should secure and how it should be done.

R5: Technical controls will be applied on the user's devices and enterprise network, thus helping to minimise the threats.

R6: Policies are going to guide the mobile users on the do's and don'ts. IT vulnerabilities will be minimised if the users understand and comply with the enterprise security policies.

R7: The policies will define what should be included in the awareness program.
R8: IT Administration will be leading the awareness program.
R9: Awareness program is then going to enlighten the users about the threats and how to mitigate them. Mobile users will realise the BYOD security concern and respond according if they are made aware of the security threats which will lead to acceptable secure mobile user behaviours.
R10: IT administration will monitor user's progress/awareness levels.
R11: Users will prompt the need for the amendment of the awareness program.
R12: Users will prompt the need for the amendment of the policies based on user's behaviours.
R13: The technical controls will define the types of access control to be implemented by IT Administration.
R14: Users will prompt the need to amend the awareness program as a result of monitoring user progress by IT Administration.
R15: The awareness program will inform IT Administration about the security gaps that needs further attention.
R16: The users will trigger the revision of strategies and processes implemented within the enterprise by IT Administration.

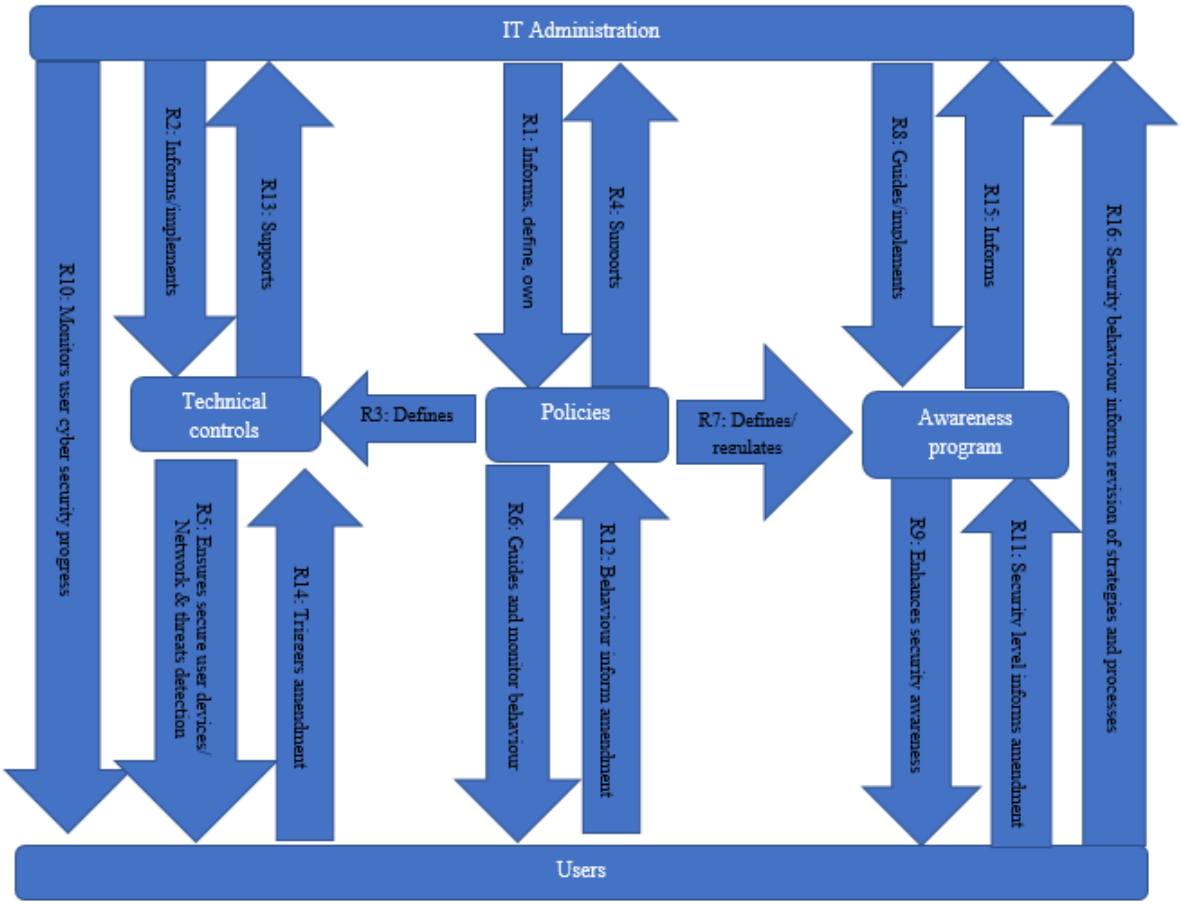


Figure 5.4 Components relationship

3. Model architecture design

IT administration will be responsible for defining, implementing, assessing and monitoring the technical controls and policies within the entire enterprise as approved my management. Software updates, antivirus, firewalls and access control are the proposed technical controls to be implemented. Once the technical controls and policies have been implemented by the enterprise, IT administration will continue to monitor users' behaviours through the awareness program. Based on the findings, they will then develop the user awareness program that will be reviewed after every 6 months. Quarterly sessions will be conducted by IT administration to constantly remind the mobile users of what is allowed and what is not allowed with the aim to safeguard the enterprise data.

The model architecture design is presented in figure 5.5:

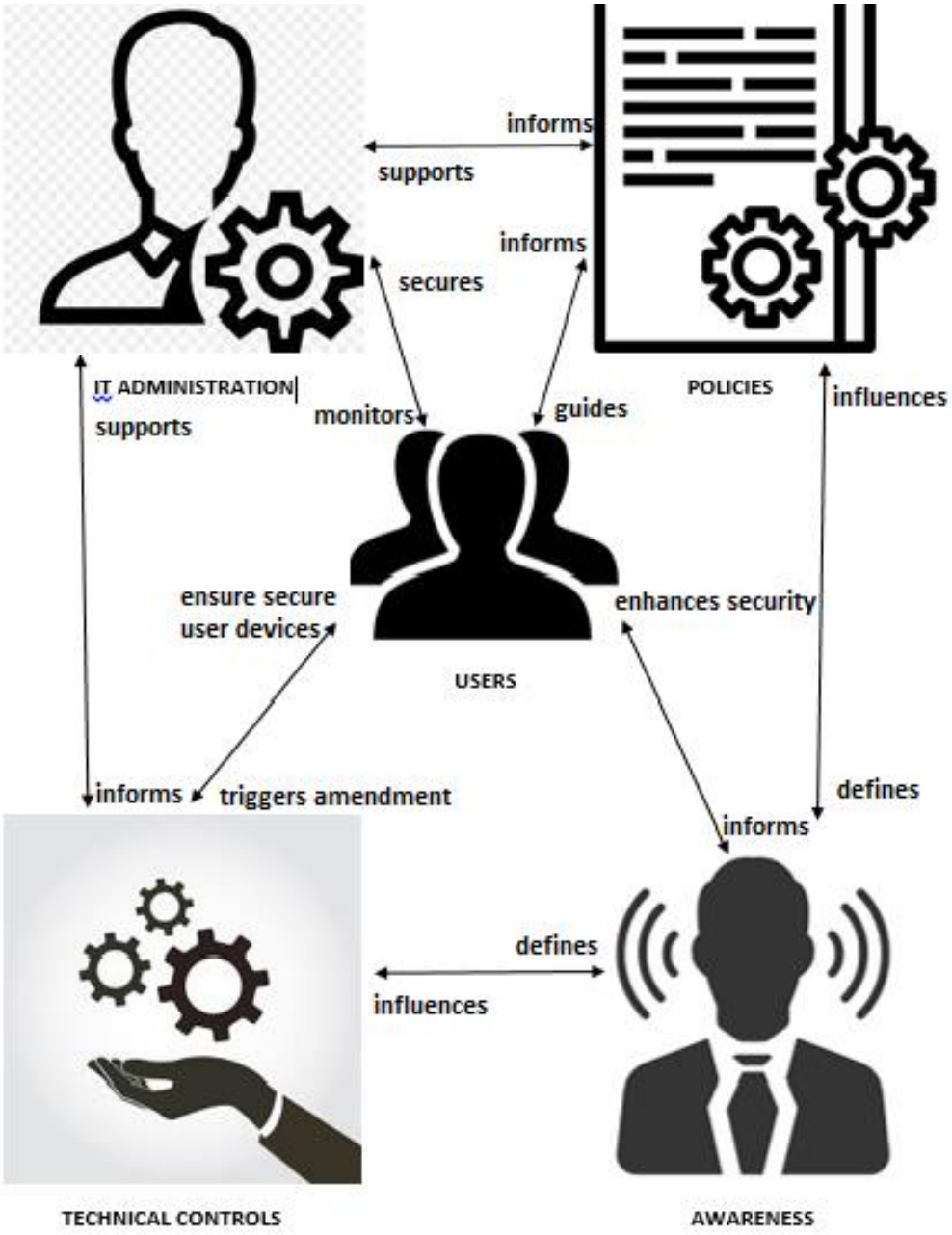


Figure 5.5 The model architecture design

4. The tentative design

The proposed BYOD awareness model in Figure 5.6 will help mobile device users within the enterprise realise the importance of BYOD security awareness. The model was designed using stage 3 the DSR model outlined in Figure 5.2.

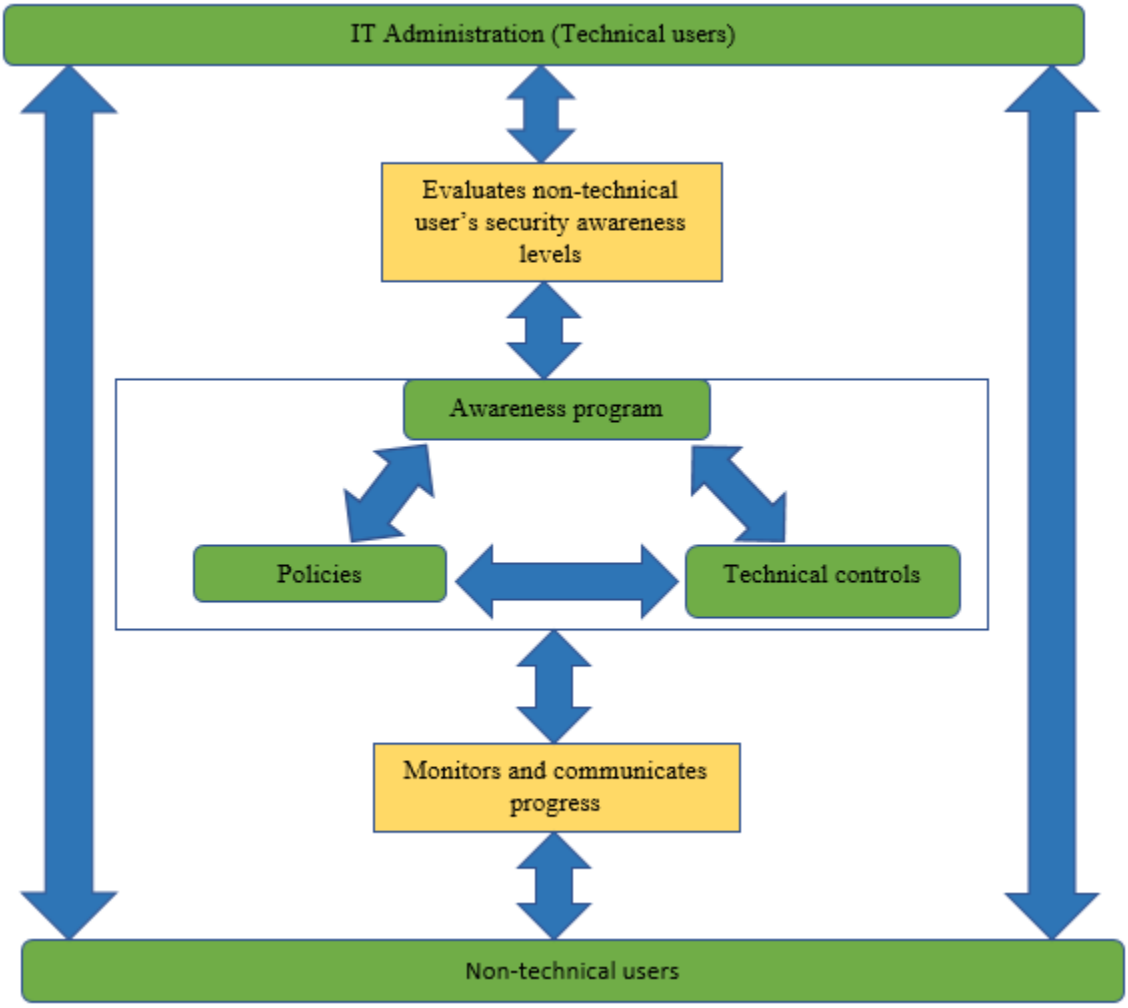


Figure 5.6 BYOD security awareness model (BYOD-SAM)

IT Administration, who are the technical users will evaluate the security levels of the mobile device users (non-technical users) within the enterprise against existing policies and technical controls. If there are no existing policies and technical controls, IT Administration will have to develop them and assess the users' security awareness levels. Based on the outcome of their assessment, a BYOD security awareness program will be developed and implemented within the enterprise. The technical users will then continue to monitor the non-technical user (mobile device users) awareness levels and communicate the progress made.

5.3.4 Phase 4 Demonstration

Figure 5.7 illustrates the implementation guideline of how to use the artefact to solve the problem. The researcher highlighted the importance of creating BYOD security awareness among mobile device users within an enterprise, which is to safeguard the enterprise data. The model provides guidelines on how create BYOD awareness among the mobile device users.

IT Administration will play a major role in the process of creating BYOD security awareness among the users. They will be responsible for defining the technical controls and informing on the policies to be implemented within the enterprise. The policies will clearly define the technical controls to be implemented and what should be included in the awareness program to guide users' behaviours and enhance users' behaviours. Furthermore, IT administration will be responsible for monitoring users progress in terms of awareness and if need be, based on their assessments, they will have to revise their strategies, processes, policies and technical controls. Figure 5.7 demonstrates the implementation of the proposed model.

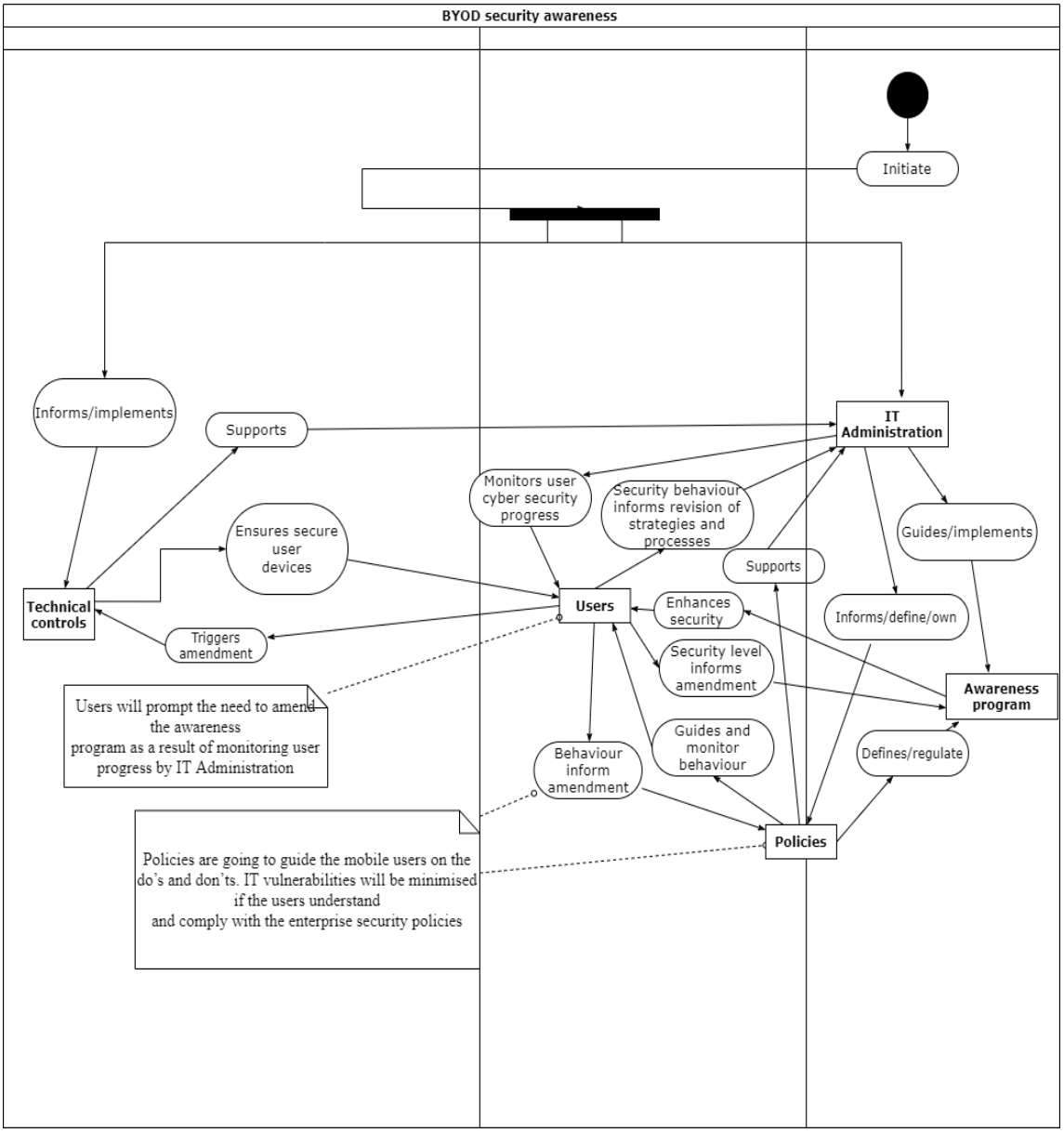


Figure 5.7 BYOD awareness for mobile device user's implementation guideline

5.3.5 Phase 5 Evaluation

According to Sonnenberg and Brocke (2012), the purpose of evaluation in DSR is to assess the progress reached by designing, constructing, and using an artefact in relation to the identified problem and the design objectives. Furthermore, to methodically demonstrate if such a progress is attained, evaluation should be guided by the evaluation criteria. Evaluations can also be crucial at highlighting areas of the artefact that may require further testing (Hall, 2017). Case studies, experiments, experts review are

examples of evaluation techniques Sonnenberg and Brocke (2012). The evaluation of the model was conducted to assess how well the proposed artefact addresses the objective it was intended to support, which is to create BYOD security awareness among the mobile device users within an enterprise.

Expert's review, Case studies, experiments are examples of evaluation techniques. The proposed BYOD security awareness model was evaluated using comparative evaluation and expert reviews. Due to time constraints, two methods of review were deemed to be appropriate: expert reviews and comparative evaluation. Expert reviews reveal measures and observations that are reliable, valid and accurate. Additionally, expert reviews were deemed relevant as it gathers evidence methodologically that the proposed model is fully developed, needed, meets the needs of those that will be using it and gather suggestions that would improve the model. The advantages of expert review include the following:

- Shortest and speediest technique
- Less expensive
- No users involved, thus cutting out cost, effort, and time involved in scheduling and conducting user sessions.

Comparative evaluation was used to evaluate the model's performance and relevance against other models, whereas expert review was used to evaluate its usability, security, understandability, and adaptability.

5.3.5.1 Expert reviews

Hall (2017) defined an expert review as the technique where an expert reviews an artefact and notes potential usability issues. He further highlighted that such reviews can be effective at giving meaningful feedback in less time and at a reasonable cost than other methods. According to Tory and Moller (2005), in an expert review, the reviewer brings in his/her expertise in a given substantive domain, and at times his/her personal choices or biases. Expert reviewers were drawn from professionals in the area of information security and cyber security. The reviewers are Information Technology Security experts from the academia and the industry, and the researcher concluded that their expertise and skills are relevant to evaluate the artefact against the set criteria. Ten (10) experts were selected to evaluate the proposed model. All experts selected had not participated in this study before thus the selection of the participants was unbiased. Expert review focused on evaluating the model's:

- Relevance
- Usability
- Security
- Applicability
- Understandable

5.3.5.1.1 Model evaluation tool

An evaluation tool in the form of an online questionnaire was developed, reviewed by the research supervisors, and piloted with three experts before being shared with other expert reviewers. After piloting, the evaluation tool was then shared with the experts from both the academia and industry. The evaluation tool was divided into four main sections. The first section focused on introducing the purpose of the evaluation and the ethical consideration. Section two of the evaluation tool aimed at gathering the biographical information of the participants and the third section was the actual artefact evaluation, mainly focusing on the security, relevance, usability, applicability, and understandability of the proposed BYOD SAM model. Finally, the tool evaluated the overall model and any identified proposal from the reviewers. The evaluation tool is presented in appendix D.

5.3.5.1.2 Evaluation findings

Information Technology Security experts from the academia and the industry were selected to be the expert reviewers for the proposed BYOD security awareness model. All expert reviewers have not participated in the study before; hence the selection process was unbiased. Table 5.1 presents the expert reviewer's profiles.

1. Biographical information of the reviewers

The biographical details of the participants are presented in table 5.1. It is critical to note that 2 of the 10 participants have between 11 to 20+ years of experience, 4 participants have between 6 - 10 years of experience and the other 4 participants have between 0 – 5 years of experience in their field of expertise. This are information security experts with both the theoretical and hands-on experience in their field of expertise.

Table 5.1: Expert reviewer's profiles

No.	Reviewer's position	Years of experience in information security	Qualification (s)
Reviewer 1	Head of Information Security	6-10	Masters in Computer Science
Reviewer 2	Head of Information Security	6-10	Honours Degree in Computer Science CISSP, CEH
Reviewer 3	Security Specialist (academia)	6-10	PHD in Computer Science PostDoctoral Fellow
Reviewer 4	Security Specialist	0-5	Masters in Computer Science CEH
Reviewer 5	Head of Information Security (academia)	11-20+	PHD in Computer Science CISSP
Reviewer 6	Information Security Engineer	0-5	Honours Degree in Computer Science ISO 27001
Reviewer 7	Program Lead: Cybersecurity and Forensics (academia)	11-20+	PHD Interdisciplinary degree of IT and Legal PTE – Certified Pen Test Engineer
Reviewer 8	Head of Information Security	6-10	PHD in Computer Science CISSP
Reviewer 9	Manager: IT Infrastructure	0-5	Bachelor's Degree in Computer Science ITIL, COBIT 2019
Reviewer 10	Head of Information Security	0-5	Bachelor's Degree in Computer Science CompTIA Security+

Figure 5.8 represents the experts academic and other qualifications in the field of computing. Apart from the academic qualifications, one reviewer has an Interdisciplinary Degree of IT and Legal and the other reviewer Postdoctoral Fellow.

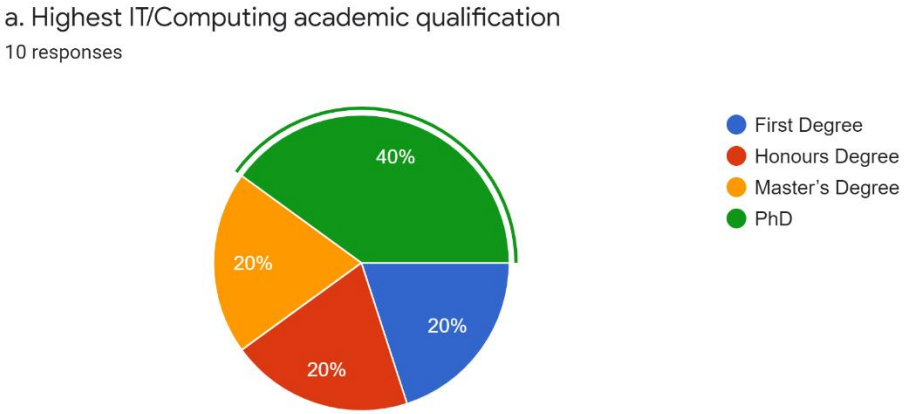


Figure 5.8 Expert reviewer's academic qualifications

Additionally, the reviewers also have professional certificates in information security as presented in Figure 5.9. One of the reviewers also has a certificate in Information security Awareness – advanced.

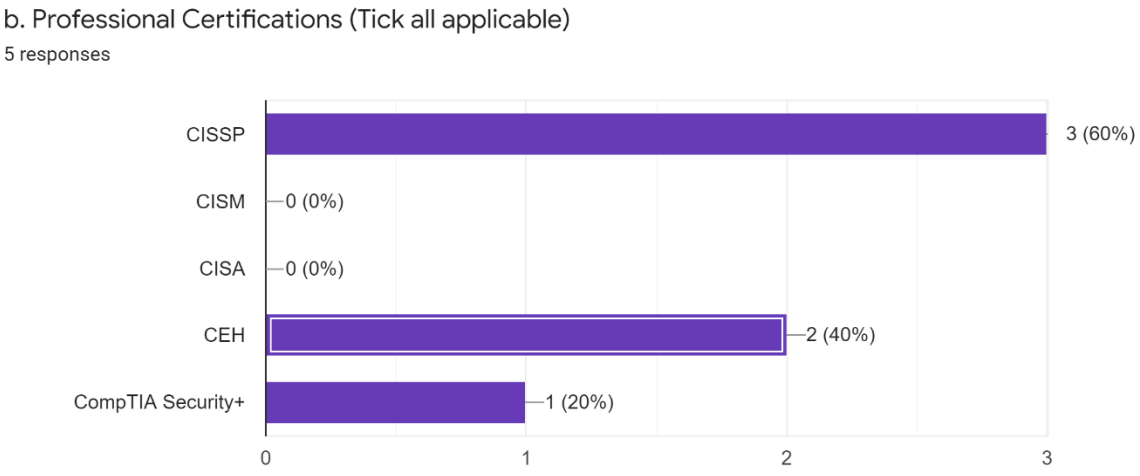


Figure 5.9 Expert reviewers' information security certificates

Figure 5.10 outlines the reviewer's positions. To note is the fact that some of the reviewers are serving in more than 1 positions. Some have additional roles such as Young Information and Communication Technology Fellow, BAS Program Lead Cybersecurity and Forensics and Manager IT Infrastructure.

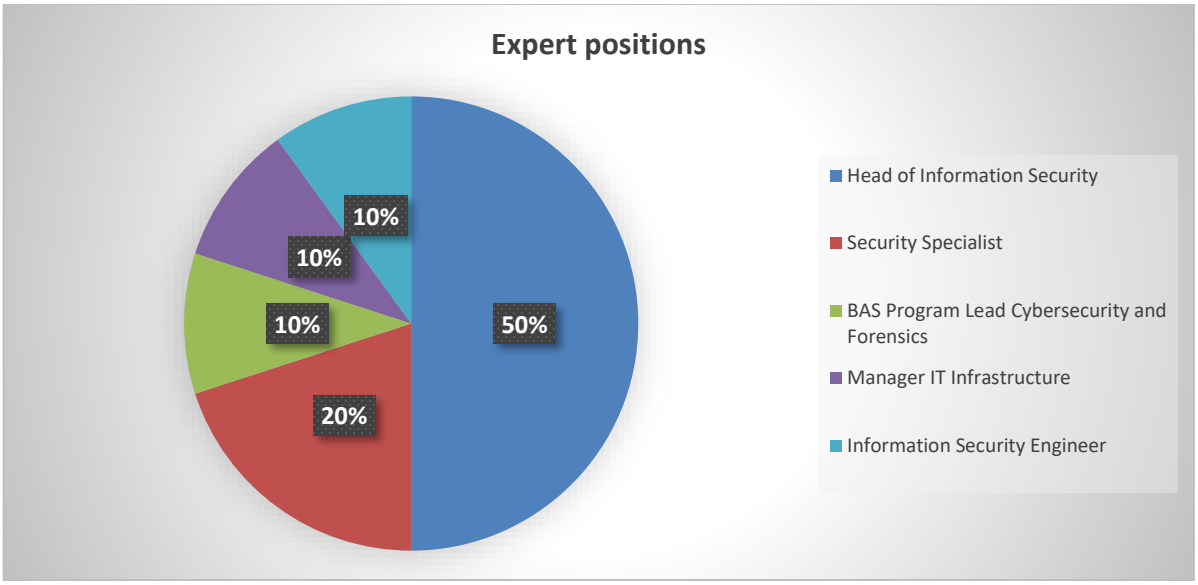


Figure 5.10 Expert positions

2. Model evaluation

2.1 Security

The findings revealed that 60% of the reviewers realised that the proposed BYOD-SAM model provides a technical aspect of BYOD security that will help enterprises in reducing BYOD related security threats within Namibian enterprises and shown in Figure 5.8. The other 4 participants representing 40% of the reviewers do not agree and 1 of them did not provide further input as to why they do not agree.

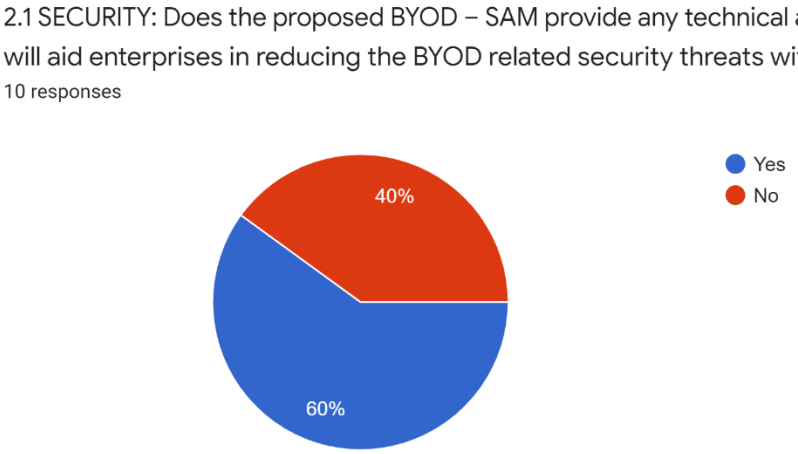


Figure 5.11 Technical aspect of BYOD security

Comments and recommendations

Table 5.2: Reviewers comments and recommendations

Reviewer no	Comments
Reviewer 1	Help improve organizational IT security controls
Reviewer 3	It covers the awareness, policies, monitoring and communication and security awareness levels
Reviewer 5	Your model provides the interactive framework of an engagement process between technical and non-technical users. It is a generic framework applicable to BYOD or non-BYOD environment
Reviewer 7	It appears to evaluate the technical skill level of the user
Reviewer 8	The model will probably need to also cater for different levels of users (e.g. technical, non-technical, and management)
Reviewer 9	There is no BYOD policy that is specific in our organization. but going into the future one would consider that we invest time and resources in that aspect of the business

Overall conclusion from the comments and data gathered.

Overall, all the reviewers have the necessary qualifications and information security background as they all have some years of experience in their field of expertise. Based on the findings, majority of the reviewers agree that the proposed BYOD security model will help enterprises in reducing BYOD related security threats.

2.2 Relevance

The section focused on evaluating the relevance of the following security controls namely IT administration, policies, technical controls and awareness program in creating BYOD security awareness among mobile device users within an enterprise. Most of the reviewers confirmed the findings of the study the relevance of the security controls as shown in table 5.3.

Table 5.3: Relevance of the security controls

Components	Much irrelevant	Irrelevant	Neutral	Relevant	Much relevant
IT Administration (Technical users)	20%	0%	10%	30%	40%
Policies	10%	0%	0%	20%	70%
Technical controls (Access control, software update, authentication, firewall and antivirus)	0%	20%	0%	10%	70%
Awareness program	10%	10%	0%	20%	60%

Furthermore, the reviewers were also required to evaluate if it is necessary for IT administration to constantly evaluate the mobile user's security awareness level. Of the participants, 80% agrees with the motion whereas 20% are against the constant review of user's security awareness level. Table 5.4 shows the reasoning for the need to review user awareness level regularly.

Table 5.4 Relevance of mobile device user's security awareness level review

Reviewer no	Comments
Reviewer 1	The attack surface keeps changing and evolving and the users need to be prepared.
Reviewer 3	The fact that security issues are dynamic and the inconsistencies in human behaviour. Also considering that new users may join the organisation at any given time.
Reviewer 4	If it's not evaluated, the IT Administration might not visualize return of effort.
Reviewer 7	It would be good to have regular (quarterly / biannual) quizzes that test awareness.
Reviewer 8	Over and above just IT Administrator, this role should be responsibility of managers and supervisors including HR since security is not only an IT responsibility in organisations.

For every question under this section 70 – 90% (combination of relevant and much relevant) of the reviewers seconded the researcher's idea of implementing the technical controls within the enterprise and constantly evaluating the user's BYOD security awareness levels constantly. Some reviewers highlighted the need to conduct quarterly evaluation sessions with the users as proposed by the researcher in this study.

Overall conclusion from the comments and data gathered.

The highlighted security controls namely: IT administration, policies, technical controls and awareness program are necessary in creating BYOD security awareness among the user and there is a need to review this security controls quarterly as the security threats keeps on evolving. Reviewing these security controls regularly is a critical part of the security threats management process, due to the constantly evolving security threats.

2.3 Usability

The reviewers were requested to rate the extent to which the following properties: detailed, learnability, consistent, offer good security will influence the usage of the proposed BYOD-SAM model and reflected in Figure 5.9.

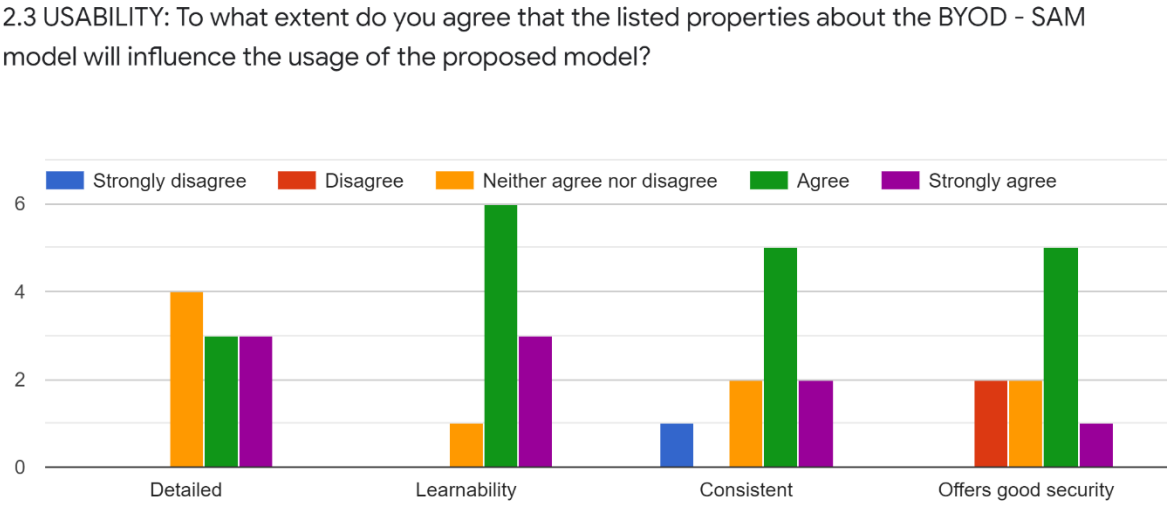


Figure 5.12 Model usage influence

The reviewers agree that the proposed model has properties that will influence its usage. Table 5.5 shows some of the additional comments from the reviewers.

Table 5.5: Influence of the model usage

Reviewer no	**Comments**
Reviewer 3	There is need for clarity in terms of what the arrows are representing (either give the labels in terms of the actions being done by each of the two key actors in both directions as you are showing on the model). Who is the custodian of the monitoring and communication of progress? From the way it is represented on the model, it's a little tricky to determine that.
Reviewer 5	I am not clear on the correlation between usability with the listed properties. There could be other fundamental properties miss out from this list. Nowhere to tell.

Overall conclusion from the comments and data gathered.

Based on the findings, most of the reviewers agree that the listed properties will influence the usage of the proposed BYOD security awareness model. As proposed by reviewer 3, the actions on the two actors

(technical and non-technical users) were labelled to ensure that the model is more understandable and this is reflected in the revised model, Figure 5.14.

Reviewer 5's concern was cleared by highlighting the aim of the question which is to rate the usability of the model mainly focusing on the listed properties which are: detailed, learnability, consistent and offer good security. The primary purpose of this question is to access if the proposed model is operational.

2.4 Applicability

Most of the reviewers strongly agreed and agreed that an awareness program, policies and technical controls are applicable in boosting mobile user's BYOD security awareness levels as depicted in table 5.6, however 10% of the reviewers disagreed and feel that awareness program, policies and technical users on the proposed BYOD awareness model should be rearranged as they need to be directly linked to what IT Administrator should do. The researcher acknowledges reviewer 3's views and associated reasoning, however the researcher maintains that the technical users are responsible for implementing and monitoring the awareness program hence the representation in the model and this is corroborated by Ronwyn (2016) in chapter 2 section 2.2.4. The proposal was considered when revising the proposed awareness model.

Table 5.6: Effects of security control's implementation

Security control	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
Awareness program	10%	0%	0%	40%	50%
Policies	10%	0%	10%	20%	60%
Technical controls	10%	20%	10%	20%	40%

Comment:
Reviewer 3 said: I would rather have a flipped approach of the triangle representation, where the policies and technical controls are more linked to what IT Administrators are supposed to do (actions) for the 3 aspects actually, i.e. awareness program, policies and technical controls, then one arrow that links the awareness program to the non-technical users, which should be labelled properly in terms of what actions they are expected to do.
Considering the reasoning given above, the researcher concluded that the proposed changes will be considered when refining the BYOD security awareness model.

Reviewer 5 said "Technical controls may not be the answer to everything".

The researcher agrees that this will not offer total security however technical controls are considered as the greatest catalyst in promoting information security. Additionally, the technical controls are supported by human security and policies to strengthen the line of defence.

Reviewer 9 said “For non-technical user, you best options in my view is to go through this awareness program”.
The researcher agrees with the reviewer as this is aligned with the model design covering the human and technical security controls.

Overall conclusion from the comments and data gathered.

The components listed above are deemed necessary and applicable to be part of a security awareness model as they complement each other to enhance information security. These components were considered appropriate to be part of the model by the researcher and seconded by the reviewers.

2.5 Understandability

The following aspects of the model were rated: comprehensive, reasonable, concise and complete. The findings are presented in table 5.7.

Table 5.7 Understandability of the BYOD SAM

Aspects	**Strongly disagree**	**Disagree**	**Neither agree nor disagree**	**Agree**	**Strongly agree**
Comphrehensive	10%	10%	20%	30%	30%
Reasonable	0%	10%	30%	30%	30%
Concise	10%	0%	20%	30%	40%
Complete	10%	10%	20%	30%	30%

Comments:
Reviewer 3 said “You could make use of the two outside arrows to represent - Evaluates non-technical user's security awareness levels and monitors and communicates progress. You then leave the middle section to represent fully the actions/processes that builds to the awareness program, considering the comments I recommended in 2.4. Precisely make sure your arrows are all labelled, that makes the model easy to follow hence understandable”. To address this, the proposed changes were implemented in phase 5.2.6.

According to Reviewer 8, “It is difficult to judge since I don’t have all the information regarding the framework”. A brief background about the model was provided in phase 5.2.4 to address this concern and it is reflected in the following section. The model evaluation tool can be found in appendix D.

The primary purpose of the BYOD-SAM is to create BYOD security awareness among mobile device users within Namibian enterprises. IT Administration will play a major role in the process of creating BYOD security awareness among the users. They will be responsible for defining the technical controls and inform on the policies to be implemented within the enterprise. The policies will clearly define the technical controls to be implemented and what should be included in the awareness program to guide user’ behaviours and enhance user’s behaviours. Furthermore, IT administration will be responsible for monitoring users progress in terms of awareness and if need be, based on their assessments, they will have to revise their strategies, processes, policies and technical controls.

Overall conclusion from the comments and data gathered

Based on reviewer 3 and 8, the proposed model appears to be incomplete, which means there are some amendments to be made specifically the labelling of the model allows to ensure its completeness and this will be reflected in the final model. The arrows on the proposed model will be labelled as proposed by reviewer 3, to ensure that the model is more understandable and easier to follow.

2.6 Overall model evaluation

This section is meant to evaluate the overall performance of the model. All reviewers agreed that BYOD security awareness is important with 70% saying it is very important and 30% highlighted it is important among mobile device users in Namibia who use their gadgets for work or within work premises as depicted in Figure 5.10. The primary purpose of the study is to create BYOD security awareness among mobile users because based of the actual study objectives and findings it was observed that although the organisation has partially implemented BYOD, there is nothing in place that would aid the enterprises address BYOD related cyber threats prevalent in their space, hence the need to create BYOD security awareness among the mobile device users who are considered to be the weakest link.

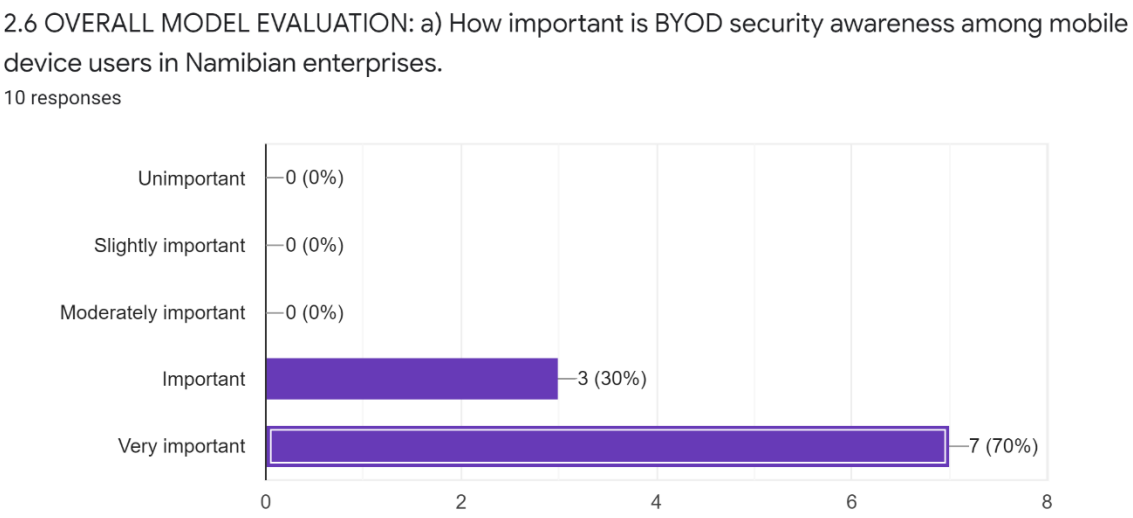


Figure 5.13 Importance of BYOD security awareness among mobile device users

Table 5.8: Importance of BYOD security awareness among mobile device users

Reviewer no	Comments
Reviewer 3	Given the popularity of mobile devices usage in workplaces, these are becoming the first line of attacks and weapons towards compromising organisational networks.
Reviewer 5	BYOD is the strength and weakness at the same time, as it is a private property.
Reviewer 7	Namibian enterprises rely heavily on mobile devices.

The researcher agrees with reviewer 3 and 7 that mobile devices are widely used nowadays to conduct business and are sometimes the first line of attack toward organisation's information security, this is also seconded by Wlosinski (2016). Sheldon (2019) also highlighted that for most organisations, mobile devices have become an integral part of every business processes. Considering the current COVID-19 pandemic, most organisation are heavily relying on mobile devices to execute business as usual, which poses a huge risk to the organisation's data. Additionally, as highlighted by reviewer 5, without abandoning the benefits offered by BYOD, organisations also do not have full control over the devices used for work purposes which places the organisational data at risk, hence the need to invest more in BYOD security awareness.

Furthermore, the reviewers were expected to evaluate the model using the following aspects: useful, relevant and needed, understandable, applicable, usable and requires improvement. The outcome of the evaluation is presented in table 5.9. Of the reviewers, 50% strongly agrees that the proposed BYOD model requires improvement. The researcher considered the reviewers input to revise the proposed model to ensure that the proposed model is complete, usable, and understandable. The improvements made on the model includes rearranging the model components and labelling all the arrows to ensure that the model is easy to follow. Figure 5.14 depicts the revised BYOD security awareness model.

Table 5.9: Overall model evaluation

Overall, the model is:	**Strongly disagree**	**Disagree**	**Neither agree nor disagree**		**Agree**	**Strongly agree**
Useful	0%	10%	20%		30%	40%
Relevant and needed	0%	0%	30%		30%	40%
Understandable	0%	20%	20%		30%	30%
Applicable	0%	0%	40%		40%	20%
Usable	0%	10%	30%		30%	30%
Requires improvement	0%	20%	30%		20%	30%

Comments:

The fact that security issues are dynamic, the inconsistencies in human behaviour and considering that new users may join the organisation at any given time as alluded by reviewer 3, there is a need to have a BYOD model in place to safeguard the enterprise data by minimising the BYOD security threats. Based on reviewer 8, the model clearly articulates the people aspect which the main objective of the study, to create BYOD security awareness among the users.

Overall conclusion from the comments and data gathered.

50% of the reviewers highlighted that the proposed model requires further improvement, and their ideas were considered by the researcher to identify the areas that need further improvements in revising the model as follows:

- The outside arrows were labelled as proposed by the reviewer to clearly highlight what they represent.
- The triangular presentation of data in the draft model was re-arranged to make the model more meaningful as shown in Figure 5.14. This was also motivated by reviewer 3 logical flow of ideas and reasoning. These changes were also deemed necessary by the researcher.

Additionally, reviewer 3 proposed to make use of the two outside arrows to represent: ‘’Evaluates non-technical user's security awareness levels” and ‘’monitors and communicates progress’’. Although the reviewer’s reasoning is valid, the proposal was not implemented since it would not really make much of a difference from the initial concept.

5.3.5.2 Comparative evaluation

The relevance and component construction of the proposed artefact against the existing artefacts with the same objective was assessed using comparative evaluation. In this study this was achieved through comparing the existing BYOD awareness models again the proposed BYOD-SAM.

5.3.5.2.1 Relevance

Users play a critical role in BYOD security management and are considered a security risk to information security. Policies, technical controls and awareness program can be implemented however a blind eye should not be turned against the users to fully manage BYOD security.

Table 5.10 presents the evaluation of the proposed model against the other existing 3 models. These models were selected because they strive to offer the same concept which is user BYOD security awareness as the proposed BYOD-SAM. The detailed evaluation of the existing models can be found in chapter 2 section 2.2.4.

Model	Metric 1 Definition of user BYOD security awareness	Metric 2 Implementation guideline	Metric 3 Continuous monitoring
BYOD-Insure: A security Assessment model for Enterprise BYOD (Ratchford, 2020)		✓	✓
User's Information Security Awareness in BYOD Programs: A Theoretical Model (Han, 2017)		✓	✓
Improving Security in Bring Your Own Device (BYOD) Environment by Controlling Access (Muhammad, Ayesh & Zadeh, 2017)		✓	
BYOD-SAM	✓	✓	✓

Table 5.10: BYOD security models comparison

Good work has been done by previous researchers; however, a need still exists to strengthen user's BYOD security awareness to mitigate BYOD related security threats. Implementing security controls would not be enough to maximize BYOD security. The main domain to be investigated is the user aspect. Employees

joins and leaves the company at any point in time and to minimise the vulnerabilities, it is critical to always enhance user awareness.

5.3.6 Phase 6 Communication

The findings of this study will be communicated through this thesis and peer reviewed scholarly publications. Furthermore, the proposed model will be shared with the enterprise used as a case study. The revised BYOD - SAM model including the changes informed by expert reviews is depicted in Figure 5.14.

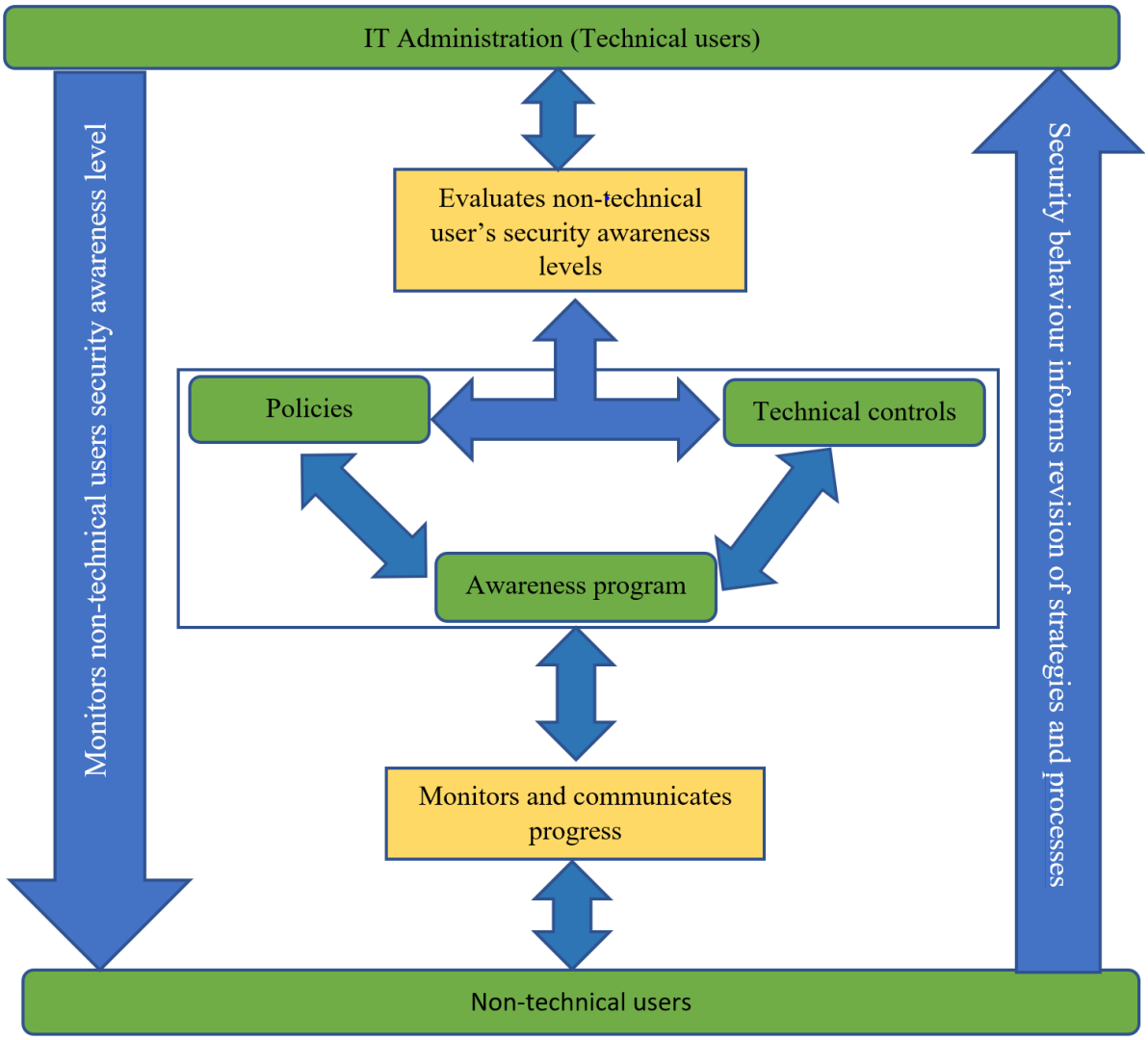


Figure 5.14 Revised BYOD security awareness model (BYOD-SAM)

5.4 Chapter Summary

The chapter presented the BYOD security awareness design process. It outlined the rationale behind designing a BYOD awareness model for enterprises in Namibia, which is to create BYOD security awareness among the mobile device users. The rise in BYOD related threats motivated the development of this model based on findings presented in sections 2.2.4 and 4.3.3. The model development process involved literature review, engaging a Namibian enterprise through data collection, and identifying the major components of the model. The main components of the proposed model namely policies, users, awareness program, technical controls and IT Administration were identified in sections 2.2.2, 2.2.4, 4.4.2 and 4.2.3. Figure 5.6 depicts the proposed BYOD security awareness model (BYOD – SAM). Furthermore, the proposed BYOD security awareness model was evaluated using comparative evaluation where similar models such as BYOD insecure and BYOD User's Information Security Awareness Model were used as benchmarks, the findings reflected that there is still a loophole to be addressed when it comes to BYOD security awareness among the users. Furthermore, expert reviews were used to evaluate the model relevance, usability, security, applicability and understandability. The key were findings reflected in section 2, these were used to refine the draft model and Figure 5.14 presents BYOD-SAM after the expert reviews**.** The experts considered the proposed BYOD security awareness model as applicable, relevant, and needed. The next chapter, chapter 6 highlights the overall research conclusion and recommendations.

CHAPTER 6: CONCLUSION AND RECOMMENDATIONS

6.1 Introduction

The chapter concludes the research study by presenting the research contributions, reflection, lessons learnt, research limitations, future directions and concluding remarks. The study researched on BYOD security with the aim to create BYOD security awareness among mobile device users within Namibian enterprises. In chapter 2, the research explored literature on existing BYOD security awareness models. Chapter 3 of this study outlined the data collection tools design, data collection process, analysis and all protocols followed throughout the research. The analysis of data collected for this study was conducted in chapter 4. Furthermore, the study outlined the procedures followed in designing the BYOD security awareness model for mobile device users within Namibian enterprises in Chapter 5. Accordingly, this chapter concludes the study by highlighting the research contributions, reflection, lessons learnt, research limitations, future directions and concluding remarks.

6.2 Research contributions

The study will contribute to the new technology horizon of Namibia's future BYOD security awareness by motivating enterprises to implement mechanisms that will protect the enterprise confidential information. Since Namibia is reported as one of the least ranked countries in Africa in terms of cyber security, the model is a guideline on how enterprises can create BYOD security awareness among users within their enterprises and improve their security posture as well as that of the nation. The following contributions are included in this research work:

- The identification of the BYOD security threats associated with BYOD implementation with Namibian enterprise as presented in chapter 2, section 2.2.4. Some of the BYOD threats identified includes data leakage, malware, device management challenges, lost or stolen devices etc.

- Analysis of the effectiveness of existing BYOD security awareness models as outlined in chapter 2, section 2.2.6.1. With all the three (3) models that were reviewed, the users BYOD security awareness gap remains a concern, which motivated the development of the BYOD-SAM presented in this study.

- Namibian enterprises' response to BYOD related security threats prevalent in their space highlighted in chapter 4, section 4.3.3. The study revealed that the enterprise does not have the security measures in place e.g. a BYOD policy to protect the enterprise data.

BYOD security awareness levels among mobile device users as presented in chapter 4, section 4.2.2. BYOD security gaps were observed hence the recommendation to develop the BYOD-SAM to enhance mobile device user's awareness level

6.3 Reflection

This section outlines the study reflection against the 3 types of reflection namely: scientific, substantive, and methodological. Reflection is a DSR process conducted before concluding a research study (Vaishnavi & Kuechler, 2004). Scientific reflection entails the generalisation of the research contributions made; substantive reflection defines the scope of the study whereas methodological reflection defines the research process followed to develop the model.

6.3.1 Scientific reflection

BYOD offers tremendous benefits that can maximise enterprises outputs. Despite the benefits offered by BYOD, it also comes with some security threats. The study revealed that the BYOD security threats can be mitigated by implementing the security measures for example policies, awareness program and technical controls. The study proposed a BYOD security awareness model that will help enterprises to create BYOD security awareness among the mobile device users within their enterprises. The proposed models will contribute to enterprises security capacity building and act as a guideline for the formulation, implementation, and enforcement of the security controls within their enterprises.

6.3.2 Substantive reflection

To create awareness among mobile users, the researcher proposed BYOD-SAM which is necessary to the enterprises in creating BYOD security awareness among their mobile device users with the aim to safeguard the organisational data. To do this the researcher identified the BYOD security awareness model components. To ensure validity of the BYOD-SAM was evaluated by expert reviewers as described in chapter 5 section 5.3.5.1.2.

6.3.3 Methodological reflection

When conducting any research study, the researcher must be neutral and unbiased. The study used the qualitative case study research paradigm and the DSR paradigm to design the BYOD security awareness model. The DSR process reflects the different phases that lead to the development of the BYOD-SAM.

Questionnaires, interviews were used as the data collection tools and the proposed model was evaluated by experts through expert reviews. The research methods and tools used for this research are best suited for the study objectives. The methods used for this research were best suited for the objectives of this study.

6.4 Lessons Learnt

The researcher learnt the following from this study:

- Without any doubt, most enterprises have already implemented BYOD within their organisations. The reality is some enterprises implemented the BYOD concept without knowing and without security controls in place which may leave the enterprise data prone to BYOD security threats. The researcher learned that BYOD security threats can be mitigated by having the right security controls in place.
- COVID19 pandemic has changed the way businesses operate hence the need to strengthen BYOD security.
- New strategies are needed as BYOD keeps evolving and available strategies and approaches need to constantly improve as there is no universal solution for securing BYOD environments.
- The study revealed that BYOD security is strongly influenced by technical and operational measures, both considered in the design of the proposed BYOD security awareness model.

6.5 Research Limitations

It is normal that every research will have some limitations; however, it is important to try to reduce the range of scope of limitations throughout the study. The main limitation of this study was the time constraint as it was not easy to get the responses from the participants within the set timeframe. The researcher had to constantly engage the Senior IT Manager to encourage the staff to complete the questionnaires and interviews. Research participants were also conveniently chosen depending on their availability, which might have affected the quality of data gathered.

6.6 Future Considerations

Some areas of interest for future work are:

- Future work could incorporate different enterprises for the findings to be generalised to other Namibian enterprises as this will bring a new dimension.

- Behaviour analysis tools could also be incorporated into the model to detect mobile user activities and notify the technical team if anything diverts from the norm.
- Additionally, it is also recommended for the proposed BYOD security awareness model to be constantly revised to cater for any future technological advancements.
- Testing of the BYOD-SAM to assess if the mobile user's security awareness posture has improved.
- Designing of universal technical controls that Namibian organisations will need.
- Developing of universal user training awareness material and programs

6.7 Concluding Remarks

The main aim of the study was to create a BYOD security awareness model aimed at creating BYOD security awareness among the mobile device users with the Namibian enterprises. The findings of the study showed that BYOD offers several benefits for instance cost reduction, flexibility, improved service delivery and the Namibian enterprises are benefiting too as shown in chapter 2, section 2.2.1, and in chapter 4, section 4.2.2. However, the concept can also pose major security threats. Mobile device users were identified as the weakest link thus there was a need to create BYOD security awareness among the users. To do this, the BYOD security awareness model was developed which was the main objective for this study. Table 6.1 summaries the major work carried out in this research study.

Research question	**Answer**	**Evidence**
How do Namibian enterprises address BYOD relate cyber threats?	Based on BYOD-SAM evaluation, it was observed that the enterprise currently does not have anything in place to administer BYOD.	Chapter 4 Section 4.2.3 and 4.4.5 None of the research respondents are aware of the existing BYOD policy, as they all indicated that they do not know the content of that policy. Since the concept is not yet fully implemented,

		the respondents highlighted that the enterprise does not have anything in place to administer BYOD. The enterprise does not have a BYOD management strategy nor a policy in place to govern this. Based on the responses from the respondents, it came out that there are several gaps or loopholes that needs to be addressed one of them being mobile user awareness as this is the weakest link to BYOD security threats.
How effective are the existing BYOD security awareness models?	The existing models offers important guideline for BYOD security management. They can be used to conduct periodic checks on the state of the enterprise's security posture. The models have practical applications to organizations. The models are suitable to enterprises of any size. Some security loopholes observed.	Chapter 2 section 2.2.6.1 Chapter 5 section 5.3.5.2.1 Three (3) existing BYOD security awareness models were reviewed. With all the models that were reviewed, the users BYOD security awareness gap remains a concern, which motivated the development of the BYOD-SAM.

How effective is the proposed BYOD security awareness model?	Increased BYOD security awareness among mobile users.	Chapter 5 section 2 The BYOD-SAM development was guided by literature review and primary data collected through interviews conducted within Namibia Motor Vehicle Accident Fund (MVA) and a questionnaire distributed within the said enterprise. The proposed model will be instrumental towards creating BYOD security awareness among employees within the enterprise.

Table 6.1: Research questions, answers and evidence

The research objectives were addressed, and the proposed BYOD-SAM model will aid in improving the security posture within Namibian enterprises.

REFERENCES

Al-Katib, A. (2020). *A Look at BYOD Environments and the Role They Play During the COVID-19 Pandemic.* https://www.missioncriticalmagazine.com/articles/92898-a-look-at-byod-environments-and-the-role-they-play-during-the-covid-19-pandemic.

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2017). A survey of cyber-security awareness in Saudi Arabia. *In 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST*), pp. 154-158.

Amoud, M., & Roudies, O. (2017). *Experiences in Secure Integration of BYOD.* http://delivery.acm.org/10.1145/3140000/3134394/p127Amoud.pdf?ip=196.216.165.246&id=3134394&acc=ACTIVE%20SERVICE&key=ECA2E7626D86F333%2EDD46891288A5B34F%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&__acm__=1521562850_3987317593e9cf9ea4ab7571b2ef6d59.

Aspers, P., & Corte, U. (2019). What is Qualitative in Qualitative Research? *Qual Sociol, 42, 139–160.* https://doi.org/10.1007/s11133-019-9413-7.

Bambulas, N. (2020). *How Often Should You Do Cybersecurity Awareness Training?.* http: https://www.gflesch.com/elevity-it-blog/how-often-should-you-do-cybersecurity-awareness-training.

Bapat, S. (2018). *Simplifying Building Management With Future - Focussed Technologies.* https://next-gen-technology.ciotechoutlook.com/cxoinsight/simplifying-building-management-with-future-focussed-technologies-nid-4258-cid-159.html.

Bhasin, H. (2020). *What are Ethical Considerations in Research?.* https://www.marketing91.com/ethical-considerations/.

Britt,B. (2017). *Cyber security breaches survey 2017.* https:// /attachment_data/file/609187/Cyber_Security_Breaches_Survey_2017_infographic_general_business_findings.pdf.

Brocke, Jan., Hevner, A., & Maedche, A. (2020). Accumulation and Evolution of Design Knowledge in Design Science Research - A Journey Through Time and Space*. Journal of the Association for Information Systems.* 21. 520-544. 10.17705/1jais.00611.

Brook, C. (2020). *The Ultimate Guide to BYOD Security: Overcoming Challenges, Creating Effective Policies, and Mitigating Risks to Maximize Benefits.* https://digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating.

Campagna,R., Iyer, S., Krishnan, A., & Bauhaus, B. (2016). *Opportunities and challenges for MNO s in the mobile cloud.* https://docplayer.net/2008598-Opportunities-and-challenges-for-mno-s-in-the-mobile-cloud-uwe-herzog-eurescom-herzog-eurescom-eu.html

Cheatham, M. (2019). *8 Steps for Successfully Implementing a BYOD Policy*. https://www.devicemagic.com/blog/8-steps-successful-byod-policy/.

Chetty, P. (2016). *Importance of research approach in research.* https://www.projectguru.in/publications/selecting-research-approach-business-studies/.

Crossman, A. (2019). *An Overview of Qualitative Research Methods.* https://www.thoughtco.com/qualitative-research-methods-3026555.

Damjanovic, B., Korać, D., & Simić, D. (2020). *Information Security in M-learning Systems: Challenges and Threats of Using Cookies*. 10.1109/INFOTEH48170.2020.9066344.

Daniel, J. (2020). Education and the COVID-19 Pandemic*. PROSPECTS, 49, 91-96.*

Deloitte. (2016). *Global Mobile Consumer Survey: US Edition.* https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-global-mobile-consumer-survey-2016-executive-summary.pdf.

Dunham, L. (2018). *Our privacy policy*. http://www.leedunhamracing.com/privacy-policy.

Ferrill, P., & McAllister, N. (2023). *The Best Mobile Device Management (MDM) Solutions.* https://www.pcmag.com/picks/the-best-mobile-device-management-mdm-solutions.

Flores, D., Qazi, F., & Jhumka, A. (2016). *Bring Your Own Disclosure: Analysing. BYOD Threats to Corporate Information.* 2016 IEEE TrustCom-BigDataSE-ISPA, 1008 – 1015. https://www.doi:10.1109.

Fogden, T. (2019). *Best Phones of 2019*. https://tech.co/news/best-phones-2019-12.

Francis, R. (2017). *The top 5 mobile security threats.* https://www.computerworld.com/article/3199371/mobile-wireless/the-top-5-mobile-security-threats.html.

Gebel, G. (2018). *Why you need both authorization and authentication.* https://www.csoonline.com/article/3269302/why-you-need-both-authorization-and-authentication.html.

Gibson, K. (2016). Mixed methods research in sport and exercise: Integrating qualitative research. In Routledge handbook of qualitative research in sport and exercise pp. 404-418.

Gökçe, K., & Dogerlioglu, O. (2019). Bring your own device policies: Perspectives of both employees and organizations. *Knowledge Management & E-Learning, 11*(2), 233–246.

Gustafsson, J. (2017). *Single case studies vs. multiple case studies: A comparative study.* http://www.diva-portal.org/smash/get/diva2:1064378/fulltext01.pdf

Harrison, H., Birk. M., Franklin. R., & Mills, J. (2017). Case Study Research: Foundations and Methodological Orientations. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research, 18*(1).

Hoenich. J. (2019). *Security Awareness Practitioner.* https://www.marmaladebox.com/awareness/security-awareness-practitioner-qa-with-jason-hoenich/.

Howard, C. (2019). *Advantages and Disadvantages of Online Surveys.* https://www.cvent.com/en/blog/events/advantages-disadvantages-online-surveys.

Infoguard Cybersecurity. (2017). *Reduce the risk of becoming a cyber ransom victim*. https://www.infoguardsecurity.com/wp-content/uploads/Infoguard-Cyber-Security-Newsletter-V2.0.pdf.

Johar, L. (2017). *Do you know what Mobile Device Security or BYOD (Bring Your Own Device) Security Best Practices is?.* https://www.linkedin.com/pulse/do-you-know-what-mobile-device-security-want-answers-please-luv-johar/?trk=portfolio_article-card_title.

Kelly, K. (2023). *What is Data Analysis? Methods, Process and Types Explained.* https://www.simplilearn.com/data-analysis-methods-process-types-article#what_is_data_analysis\.

Linneberg, S., & Korsgaard, S. (2019). Coding qualitative data: a synthesis guiding the novice. *Qualitative Research Journal, 19(3*), 259-270. https://doi.org/10.1108/QRJ-12-2018-0012*.*

Liebermann, H., Schuler, J., Strager, M., Hentz, A., & Maxwell, A. (2018). Using Unmanned Aerial Systems for Deriving Forest Stand Characteristics in Mixed Hardwoods of West Virginia. *Journal of Geospatial Applications in Natural Resources: 2(1).* https://scholarworks.sfasu.edu/j_of_geospatial_applications_in_natural_resources/vol2/ iss1/2.

Loew, L. (2018). Competencies for the future workforce. The talent management handbook, New York, McGraw-Hill, 3rd ed, pp. 71-86.

Lord, N. (2020). *The ultimate guide to BYOD security: overcoming challenges, creating effective policies, and mitigating risks to maximize benefits.* https//www.digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating.

Lucas, S. (2020).*The Pros and Cons of a Bring Your Own Device (BYOD) to Work Policy.* https://www.thebalancecareers.com/bring-your-own-device-byod-job-policy-4139870.

N-able. (2019). *N-central Integration Guide.* https://www.watchguard.com/help/docs/help-center/en-US/Content/Integration-Guides/General/N-central.html

Mahoney, R. (2016). *Preventing cybercrime*. *Business NH Magazine, 33(5)*, 20-22. http://web.a.ebscohost.com.eresources.nust.na/ehost/pdfviewer/pdfviewer?vid=1&sid=d4997de994e24183818dbb1471a91666%40sessionmgr4008.

Makanyeza, C., Kudzai, B., & Ngorora-Madzimure, G. (2022). Factors influencing small and medium enterprises' innovativeness: *Evidence from manufacturing companies in Harare, Zimbabwe, Global Business and Organizational Excellence*, *42*(3), 10-23. https://doi.10.1002/joe.22180.

Palanisamy, R., & Wu, Y. (2021). Users' attitude on perceived security of enterprise systems mobility: an empirical study. *Information and Computer Security, 29*(1), 159-186. https://doi.org/10.1108/ICS-05-2020-0069.

Pries-Heje, J., Baskerville, R., & Venable, J. (2008). Strategies for Design Science Research Evaluation. *ECIS 2008 Proceedings (87).* http://aisel.aisnet.org/ecis2008/87.

Prasanthi, L & Ishwarya, T. (2015). Cyber Crime: Prevention & Detection. *International Journal of Advanced Research in Computer and Communication Engineering,* 4(3). https://ieeexplore.ieee.org.eresources.nust.na/stamp/stamp.jsp?tp=&arnumber=7522358.

Privacy Rights Clearinghouse. (2018). *Online Harassment & Cyberstalking.* https://privacyrights.org/consumer-guides/online-harassment-cyberstalking.

Ratchford, M. (2020). BYOD-Insure: A Security Assessment Model for Enterprise BYOD. Masters Theses & Doctoral Dissertations, (354). https://scholar.dsu.edu/theses/354.

Resnik, D., Rasmussen, L., & Kissling, G. (2015). An international study of research misconduct policies. *Accountability in research*, 22(5), 249–266. https://doi.org/10.1080/08989621.2014.958218

Rice, A. (2016). *Best Practices for Secure BYOD Implementations.* https://scholarsbank.uoregon.edu/xmlui/bitstream/handle/1794/22340/Rice%20Week%207%20FINAL.pdf?sequence=1.

Ronwyn, A. (2016). *Bring Your Own Devices Vulnerability.* https://www.cimcor.com/blog/ Bring Your Own Devices Vulnerability.

Rouse, S. (2016). Of teacups and t-tests: Best practices in contemporary null hypothesis significance testing [Editorial]. *Psi Chi Journal of Psychological Research, 21*, pp 127-133.

Ruxwana, N., Msibi, M., & Mahlangu, T. (2018). Bring Your Own Device Adoption Readiness in a South African University. *South African Review of Sociology*, *49*(3-4), 78-95, www.DOI:10.1080/21528586.2019.1580218.

Savage, S. (2018). *Security update deployment information.* https://support.microsoft.com/en-us/topic/security-update-deployment-information-may-08-2018-170ad717-9155-af98-27e0-84b60b078e0b.

Seelman, K. Lewinson, T., Engleman, L., Maley, O., & Allen, A. (2017). Coping strategies used by LGB older adults in facing and anticipating health challenges: A narrative analysis. *Journal of Gay & Lesbian Social Services, 29(3*), 300-318.

Sheldon, R. (2019). *Advantages and disadvantages of mobile devices in business.* https://www.techtarget.com/searchmobilecomputing/feature/Discover-the-benefits-of-mobile-devices-in-the-enterprise.

Sonnenberg, C., & Brocke, J. (2012). *Evaluation Patterns for Design Science Research Artefacts. Communications in Computer and Information Science.* http:// 10.1007/978-3-642-33681-2_7.

Tory, M., & Moller, T. (2005). Evaluating visualizations: do expert reviews work. *IEEE computer graphics and applications*, *25*(5), pp. 8–11.

Vaishnavi, V., & Kuechler, B. (2004). Design Science Research in Information Systems Overview of Design Science Research. Ais, p.45.

Vekua, U. (2021). *What is Authentication?. A Complete Guide.* https://www.veriff.com/blog/what-is-authentication.

Veljkovic, I., & Budree, A. (2019). Development of Bring-Your-Own-Device Risk Management Model: Case Study from a South African Organisation. *The Electronic Journal Information Systems Evaluation*, 22(1), pp. 1-14.

Vrhovec, S. (2016). Challenges of mobile device use in healthcare. *39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO*), Opatija, Croatia, pp. 1393-1396.

Wlosinski, L. (2016). Mobile Computing Device Threats, Vulnerabilities and Risk Factors Are Ubiquitous*. ISACA journal, 4(1)*. https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/mobile-computing-device-threats-vulnerabilities-and-risk-are-ubiquitous.

Yin, R. (2014). *The case study methodology.* Thousand Oaks, CA: Sage Publishing.

Žukauskas, P., Vveinhardt, J., & Andriukaitienė, R. (2018). *Philosophy and Paradigm of Scientific Research.* https://www.intechopen.com/books/management-culture-and-corporate-social-responsibility/philosophy-and-paradigm-of-scientific-research.

APPENDICES

APPENDIX A: ETHICAL CLEARANCE LETTER

NAMIBIA UNIVERSITY OF SCIENCE AND TECHNOLOGY

FACULTY RESEARCH ETHICS COMMITTEE (F-REC)

DECISION/FEEDBACK ON RESEARCH PROPOSAL

Dear Ms Ester Alumbungu

Research Topic: Designing a real time BYOD security awareness model for mobile device users in Namibian enterprises

Supervisor (if applicable): **Dr F. Bhunu Shava**

Qualification registered for (if applicable): **Master of Computer Science**

(Reference number of application: FACULTY RESEARCH ETHICS COMMITTEE REGISTRATION NUMBER: 13/2018)

Re: Ethical screening application No: F-REC-13/2018

The **Faculty of Computing and Informatics** (FCI) Ethics Screening Committee of the Namibia University of Science and Technology reviewed your application for the above-mentioned research. The research as set out in the application has been:

Approved	X

We would like to point out that you, as researcher, are obliged to maintain the ethical integrity of your research, adhere to the ethical guidelines of NUST, and remain within the scope of your research proposal and supporting evidence as submitted to the F-REC. Should any aspect of your research change from the information as presented to the F-REC, which could have an effect on the possibility of harm to any research subject, you are under the obligation to report it immediately to your supervisor or F-REC as applicable in writing. Should there be any uncertainty in this regard, you have to consult with the F-REC.

We wish you success with your research, and trust that it will make a positive contribution to the quest for knowledge at NUST.

Recommendation: The application is approved: Recommendations of FCI/F-REC were addressed to the satisfaction of the Chairperson.

Sincerely,

Prof. Hippolyte N. MUYINGI
Acting Chair: Faculty Ethics Screening Committee
Tel: +264-61-207-2888

CC: Co-supervisor: Mercy Chitauro

NAMIBIA UNIVERSITY OF SCIENCE AND TECHNOLOGY
P/Bag 13388 Windhoek NAMIBIA
2019 -02- 14
OFFICE OF THE DEAN
FACULTY OF COMPUTING & INFORMATICS

FACULTY OF COMPUTING & INFORMATICS

APPENDIX B: QUESTIONNAIRE

Dear Respondent

I, Ester Shihepo, a Master student at Namibia University of Science and Technology in the Faculty of Computing and Informatics invites you to participate in a research study entitled:

DESIGNING A BRING YOUR OWN DEVICE SECURITY AWARENESS MODEL FOR MOBILE DEVICE USERS IN NAMIBIAN ENTERPRISES

This study is aimed at evaluating how Namibian enterprises address Bring Your Own Device related cyber threats prevalent in their space. I value your honest responses and please be assured that the information that you will provide will be treated as confidential. Please note that there will be no monetary gain for participating in this study and you are free to withdraw at any time. The questionnaire should take approximately 15 minutes to complete.

If you have any questions or concerns regarding this study, please contact me: ealumbungu@yahoo.com, cellphone number 081 3757078 or my supervisors at fbshava@nust.na, office number +264 61 207 2510 or mchitauro@nust.na, office number +264 61 207 2039.

1. Do you have a mobile device(s)?
   _____

2. What type of mobile device(s) do you have? Please select what is relevant.
   ☐ Iphone ☐ Samsung ☐ Huwaei ☐ Hisense

   ☐ Other (specify): _____

3. Are you allowed to use your personal mobile device(s) to access, store or transfer the enterprise/company confidential data?
   _____

4. What work do you do on your personal device?

   _____
   _____
   _____

5. How often do you take information from work to work on it home using your mobile device?

   _____

6. Are you aware of Bring Your Own Device (BYOD)?

   _____

7. Does your company have a security team?

   _____

8. Do you think you are secure from mobile threats? _____-

   _____

9. Is your mobile device(s) security configured to update automatically?

   _____

10. Can you tell if your mobile device(s) is/are infected or hacked? Please explain.

    ☐ Yes ☐ No

    _____
    _____
    _____
    _____
    _____

11. Who do you contact when your mobile device(s) is/are infected or hacked?

    _____
    _____

12. Do you think your mobile device(s) has/have value to mobile attackers? Why?

    _____
    _____
    _____
    _____

13. Is there a BYOD policy in the enterprise?

    _____

14. Do you know the content of this BYOD policy?

_____

15. If you delete a file from your mobile device, will that information be recovered or not?

    _____
    _____

16. How often do you receive training on BYOD security to raise awareness on the negative effect using BYOD? _____

17. How do you keep the files on your mobile device(s) protected?

    _____

18. Select all the tips the enterprise has implemented to reduce BYOD threats.

Tip	**Tick all applicable**
Use password protected access controls	
Control application access and permissions	
Control wireless network and service connectivity	
Keep OS, firmware, software, and applications up-to-date	
Back up device data	
Enrol in “Find my Device” and remote wipe services	
Never store personal financial data on a device	
Run mobile antivirus software or scanning tools	
Beware of free apps	

19. In your opinion, what is the weakest link for BYOD security threats in the organisation? Please explain.

    _____
    _____
    _____
    _____
    _____

APPENDIX C: INTERVIEW GUIDE

This semi-structured interview guide will be used to conduct personal interviews to assess Bring Your Own Device security awareness from enterprises mobile device users. This approach will offer an opportunity for the researcher to interact with research participants and immediately get the responses. Furthermore, will also stimulate the research participants to provide more information and will offer the researcher a platform to ask follow-up questions where more clarity is required. This interview guide is designed to last for approximately half an hour, but interview length can vary based on the respondent's responses.

1. Does the enterprise allow employees to use their personal mobile device (s) in the workplace?

   _____
   _____
   _____

2. What is your understanding with regards to the BYOD concept?

   _____
   _____
   _____

3. Has the enterprise implemented BYOD and how successful is its implementation?

   _____
   _____
   _____

4. What is the employee's expectation of BYOD adoption in the organisation?

   _____
   _____
   _____

5. What advantages can BYOD bring to the organisation?

   _____
   _____
   _____

6. Does your organisation have a BYOD adoption policy in place?

   _____
   _____
   _____
   _____

7. How responsive is your policy to employee and organisation BYOD expectations?

_____
_____
_____
_____

8. Is there a restriction/limit to the type and number of devices that can be used as a BYOD technology within the organisation?

_____
_____
_____
_____
_____

9. BYOD implementation comes with challenges. What are some of the challenges you foresee that are linked to BYOD implementation in your enterprise?

_____
_____
_____
_____
_____

10. What are some of the BYOD related cyber threats are you aware of?

_____
_____
_____
_____
_____

11. Has the enterprise ever experienced a BYOD related cyber threat?

_____
_____
_____
_____

12. How is the enterprise prepared in case of BYOD security crisis?

_____
_____
_____
_____

13. Is the organisation considering Mobile Device Management strategies?

_____
_____
_____
_____

14. Does the organisation have the necessary resources to secure and manage BYOD mobile infrastructure?

_____
_____
_____
_____

15. To what extent are the following security controls?

Control	**Most important**	**Important**	**Neutral**	**Less important**	**Not important**
Authentication					
Authorisation					
Availability					
Confidentiality					
Non-repudiation					

16. Which of the BYOD related security threats below are you aware of?

Physically-based threats	**Application-based threats**	**Network-based threats**	**Web-based threats**
Device loss/theft	Malware attacks	Network spoofing attacks	Web browser exploits
Attacks on devices intended for recycling	Inadvertent disclosure of information	Network exploits	Automatically downloaded applications
	Surveillance attacks		

APPENDIX D: EVALUATION TOOL

DESIGNING A BRING YOUR OWN DEVICE SECURITY AWARENESS MODEL FOR MOBILE DEVICE USERS IN NAMIBIAN ENTERPRISES

Dear participant

My name is Ester Shihepo, under the supervision of Prof Fungai Bhunu Shava and Dr Mercy Chitauro from the Namibia University of Science and Technology. This questionnaire serves as an evaluation tool for the BYOD security awareness model for mobile device users within Namibian enterprises. The aim is to evaluate the usability, understandability, security and applicability of the proposed BYOD security awareness model. Based on your inputs, a final model will be designed. The resulting model will contribute to the guidelines on how enterprises can create BYOD security awareness among their users to improve their security posture as well as that of the nation. Your responses are very important in informing improvements to the designed model.

I value your honest responses and please be assured that the information that you will provide will be treated as confidential. All data collected will be used solely for the purpose of this study. The questionnaire will take approximately 10 - 15 minutes to complete. If you have any questions or concerns regarding this study, please contact me on 0813757078 or ealumbungu@yahoo.com.

BYOD Security Awareness Model (BYOD SAM) Summary

BYOD SAM is depicted in Figure 0-1. In summary IT Administration, who are the technical users will evaluate the security awareness levels of the mobile device users (non-technical users) within the enterprise against existing policies and technical controls. If there are no existing policies and technical controls, IT Administration will have to develop them and assess the user's security awareness levels. Based on the outcome of their assessment, a BYOD security awareness program will be developed and implemented within the enterprise. The technical users will then continue to monitor the non-technical user (mobile device users) awareness levels and communicate the progress made. If need be, based on their assessments, they will have to revise their strategies, processes, policies and technical controls.

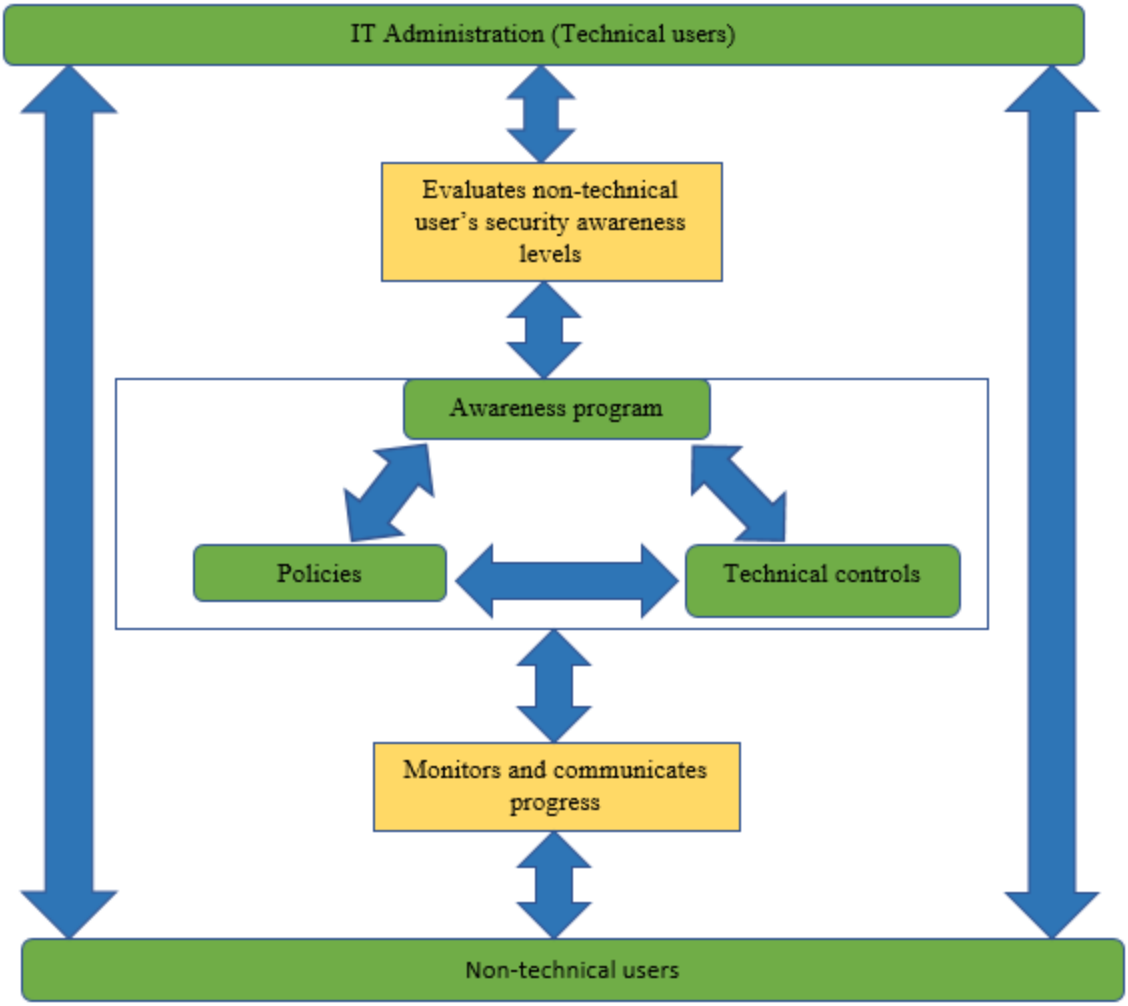


Figure 0-1: BYOD security awareness model (BYOD – SAM)

1. Biographical Information

This section is meant to collect biographical information of the selected stakeholders.

a. Highest IT/Computing academic qualification

☐ First Degree ☐ Honours Degree

☐ Master's Degree ☐ PhD

☐ Other (specify): _____

b. Professional Certifications (Tick all applicable)

☐ CISSP ☐ CISM

☐ CISA ☐ CEH

☐ CompTIA Security+ ☐ Other (specify): _____

c. Position

☐ Head of Information Security ☐ Security Analyst

☐ Security Specialist ☐ Information Security Engineer

☐ Other (specify): _____

d. Years of experience in information security

☐ 0 - 5 ☐ 6 - 10

☐ 11 - 20+ ☐ Others ……

2. <u>Model evaluation</u>

2.1 SECURITY

Does the proposed BYOD – SAM provide any technical aspect of BYOD security that will aid enterprises in reducing the BYOD related security threats within Namibian enterprises?

◯ Yes ◯

Please explain your answer:

……

……

……..

2.2 RELEVANCE

a) How relevant are the following security controls in creating BYOD security awareness among mobile device users within an enterprise?

Components	Much irrelevant	Irrelevant	Neutral	Relevant	Much relevant
IT Administration (Technical users)	◯	◯	◯	◯	◯
Policies	◯	◯	◯	◯	◯

Technical controls (Access control, software update, authentication, firewall and antivirus)	◯	◯	◯	◯	◯
Awareness program	◯	◯	◯	◯	◯

b) Is it necessary for IT Administration to constantly evaluate the non-technical user's security awareness level?

◯ Yes ◯

Please explain your answer:

……

……

2.3 USABILITY

To what extent do you agree that the listed properties about the BYOD - SAM model will influence the usage of the proposed model?

Properties	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
Detailed	◯	◯	◯	◯	◯
Learnability	◯	◯	◯	◯	◯
Consistent	◯	◯	◯	◯	◯
Offers good security	◯	◯	◯	◯	◯

Comments:

……

……

2.4 APPLICABILITY

To what extent do you agree that the implementation of the following within an enterprise will boost mobile user's BYOD security awareness levels?

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

Awareness program	◯	◯	◯	◯	◯
Policies	◯	◯	◯	◯	◯
Technical controls	◯	◯	◯	◯	◯

Comments:

……

……

2.5 UNDERSTANDABILITY

Please rate the proposed BYOD – SAM models using the aspects:

Aspects	**Strongly disagree**	**Disagree**	**Neither agree nor disagree**	**Agree**	**Strongly agree**
Comphrehensive	◯	◯	◯	◯	◯
Reasonable	◯	◯	◯	◯	◯
Concise	◯	◯	◯	◯	◯
Complete	◯	◯	◯	◯	◯

Comments:

……

……

2.6 OVERALL MODEL EVALUATION

a) How important is BYOD security awareness among mobile device users in Namibian enterprises.

Unimportant	**Slightly important**	**Moderately important**	**Important**	**Very important**
◯	◯	◯	◯	◯

Comments:

……

……

b) Please evaluate the model above using the measures below.

Overall, the model is:	**Strongly disagree**	**Disagree**	**Neither agree nor disagree**	**Agree**	**Strongly agree**
Useful	⬭	⬭	⬭	⬭	⬭
Relevant and needed	⬭	⬭	⬭	⬭	⬭
Understable	⬭	⬭	⬭	⬭	⬭
Applicable	⬭	⬭	⬭	⬭	⬭
Usable	⬭	⬭	⬭	⬭	⬭
Requires improvement	⬭	⬭	⬭	⬭	⬭

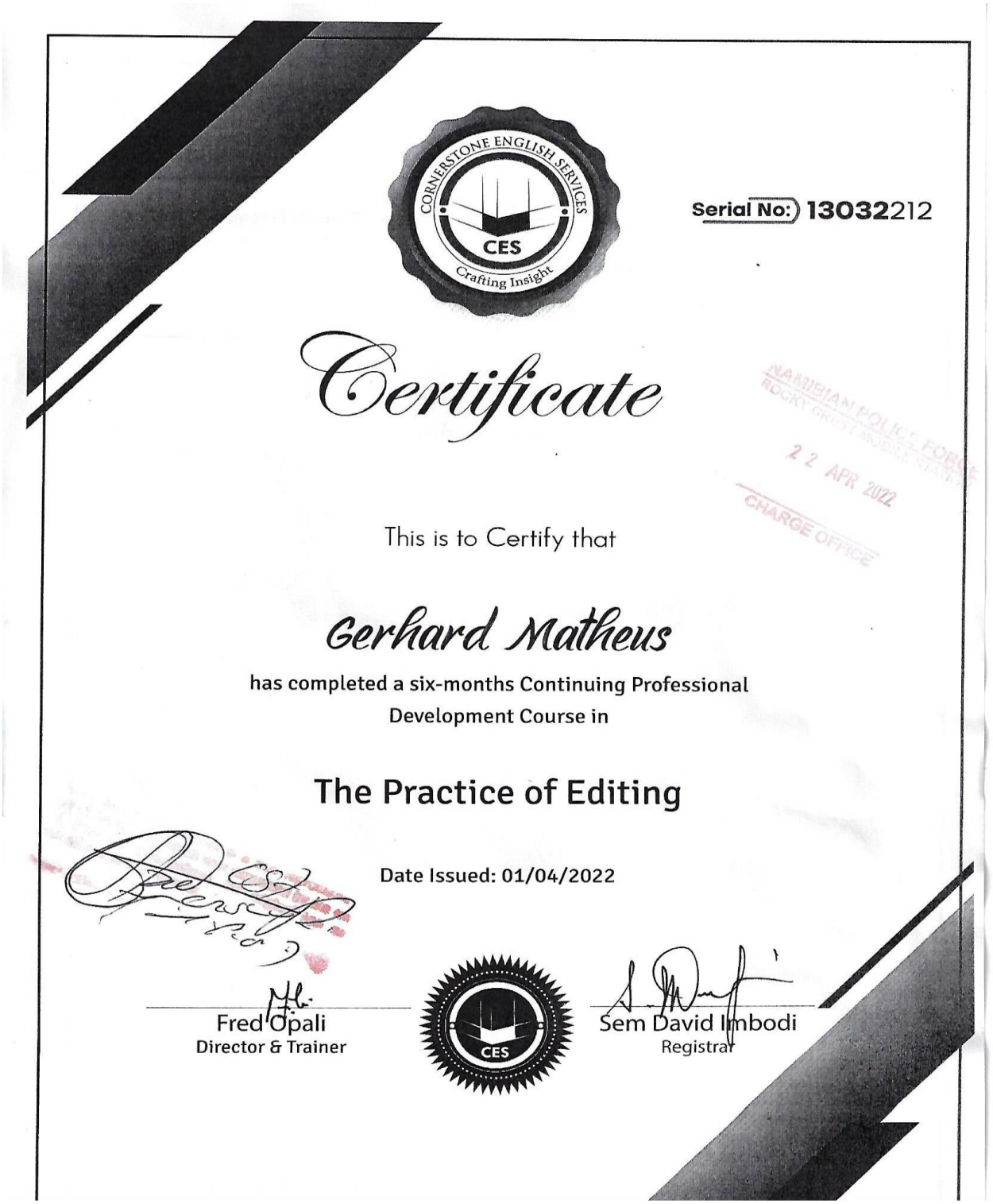
c) Please state any component that you think is missing and explain why it is important.

_____
_____
_____

Any other comments:

_____
_____
_____
_____

APPENDIX E: LANGUAGE EDITOR'S CERTIFICATE



CORNERSTONE ENGLISH SERVICES
CES
Crafting Insight

Serial No: 13032212

Certificate

NAMIBIAN POLICE FORCE
ROCKY CREST ROBBERY STATION
22 APR 2022
CHARGE OFFICE

This is to Certify that

Gerhard Matheus

has completed a six-months Continuing Professional Development Course in

The Practice of Editing

Date Issued: 01/04/2022

Fred Opali
Director & Trainer

CES

Sem David Imbodi
Registrar

APPENDIX F: LANGUAGE EDITOR'S LETTER

Gerhard Matheus

P.O. Box 25188

Windhoek 26 May 2023

To whom it may concern

LANGUAGE EDITING – Ester Shihepo

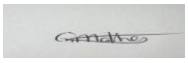
This letter serves to confirm that a **Master's in Computer Science** research project titled "**DESIGNING A BRING YOUR OWN DEVICE SECURITY AWARENESS MODEL FOR MOBILE DEVICE USERS IN NAMIBIAN ENTERPRISES"** by **ESTER SHIHEPO** was submitted to me for language editing.

The thesis was professionally edited, and track changes and suggestions were made in the document. The research content or the author's intentions were not altered during the editing process and the author has the authority to accept or reject my suggestions.

For any enquiries regarding this paper, I may be contacted on the provided phone number, or via email.

Yours faithfully

Ms Gerhard Matheus



Master of Arts (English Studies) Profgee12@gmail.com/ +264817296696