INVESTIGATING THE EFFECTS OF BRING YOUR OWN DEVICE ON INFORMATION SECURITY WITHIN TREASURY

BY

Nomvula Zulu

Student Number: 216073092

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

of

Master of Business Administration

Graduate School Of Business and Leadership

College of Law and Management Studies

Supervisor:

Professor Muhammad Hoque

Year of submission

2018

DECLARATION

I **Nomvula Annerlice Zulu** declare that:

- The research reported in this thesis, except where otherwise indicated, is my original work.

- This thesis has not been submitted for any degree or examination at any other university.

- This thesis does not contain other persons' data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.

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

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

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

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

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

Signed: _____

Acknowledgements

To God almighty, this degree is evidence that you are true in your word, promises and doings. I thank you Lord, for being faithful, for giving me strength, courage and the will to soldier on. Ngiyakhuleka Thongo lami, ngiyathokoza ngokungibekezelela nokuhamba nami loluhambo, thokoza Dlozi. I am grateful to my parents for the vision, encouragement and believing in my dreams, your love and support keeps me humbled. To my children, my true source of joy, for allowing me to pursue my dream, for loving and supporting me, thank you. The one who holds my heart, for believing in my dream and walking with me, I am grateful. A special thanks to the following:

- My supervisor, Professor Muhammad Hoque, for your guidance throughout my research.
- To my brothers, 'esteemed members', Jama nawe Ngilozi, I am indebted to you for being there continuously encouraging and supporting me throughout this journey, I will forever cherish the moments we shared especially the Jakobe times.
- Mngani, my prayer warrior, thank you for inspiration, ngiswele imilomo eyizinkulungwane, Ndabezitha.
- Mntwana uMaqeda and my team Mthoks, Zee, Msi and Ndo, isandla sedlula ingalo.
- KwaZulu-Natal Provincial Treasury, for enabling this project.

Kubobonke abangesekile kuloluhambo, nime njalo nina beSilo.

Abstract

Treasury, is a government department within the KwaZulu- Natal provincial government. Information is a strategic resource that organisation derive among other competitive advantage and advance their position regardless of its medium. Organisations must endeavour to protect information from security threats and risks. Bring your own device (BYOD) refers to a strategy where employees are allowed to use their private mobile devices for work purposes. This study aims to investigate the effects of the BYOD phenomenon on information security within Treasury. The research problem was centred on the threats posed by the BYOD on the security of information within Treasury. The study adopted a positivist research paradigm and followed quantitative research methods. Data were collected using a questionnaire which was self-administered by the researcher to all participants, the population was the entire staff in Treasury, and the sample size was 167 staff members. The key findings were that, the majority of the participants often use their private mobile devices for work purposes at work as well as outside work premises. Interestingly, the smartphone was the most used device among participants. Participants not only used but stored work information on their private mobile devices which are exposed to a number of security threats through downloading of games and apps. Majority of the participants were not aware of the policy regarding the use of private mobile devices for work purposes and were not aware of the procedure to safeguard work information on the private mobile device. Participants pointed out a number of benefits since using their own device for work purposes such as an increase in their productivity, the ease of meeting deadlines as well as convenience. Given the findings of this study, it is recommended that an organisational culture of information security be developed and inculcated among users, clear BYOD strategy inclusive of the policy, detailing information that can be accessed using the BYO device, the type of device as well as requisite security features for the private mobile device. Training and raising awareness among users on threats and risks posed by the BYOD strategy, as well as their individual roles and responsibilities towards security of information was among recommendations.

Table of contents Page number

Chapter one: Introduction

1.1 Introduction

Technological advancements in South Africa and the rest of the world have led to the extinction of defined working and personal environments Ubene, Agim, and Umo-Odiong (2018). The pervasiveness of technologically advanced mobile devices and accessibility of the internet for some, means less reliability on enterprise network infrastructure for connectivity and fulfilling work commitments (Rice 2016). This study seeks to investigate the effects of the BYOD phenomenon on information security within the KwaZulu-Natal Provincial Treasury (Treasury). The succeeding paragraphs will provide a brief background of Treasury, as a study site.

Considering that the Bring Your Own Device (BYOD) phenomenon is an unfamiliar concept, the background which defines and explain the concept will be provided well as the definition of information security. The motivation, as well as the focus of the study, will be given followed by the statement of the problem. Thereafter, the objectives of the study and the research questions are be highlighted. The limitations of the study will be discussed and lastly, the chapter concludes with a summary.

1.2 What is BYOD

While the Bring Your Own Device (BYOD) began in other countries such as the United States of America as early as 2007, it is yet to take off within the South African government environment (Ubene et al., 2018). Consumerisation of Information Technology (CoIT) trend is one of the biggest enablers of the BYOD since CoIT blurs the traditional line between business and private technology as well as equipment, private technology and equipment can be used for business purposes as well (Rice, 2016). CoIT trend promotes the use of personal technology as well as devices for work purposes, among other things, due to user preference and perceived benefits of using own technology (Mphahlele, 2016). The CoIT trend reverses the traditional norm that companies introduce new technology then users follow. In CoIT, users identify and use new technology then introduce it to the company in the form of BYOD (Disterer and Kleiner, 2013).

Another related trend is known as the Choose Your Own Device (CYOD), where the employee is allowed to choose a device and, in some instances, the employer may carry the cost of the device (Almarhabi, Jambi1, Eassa1 and Batarfi1, 2017). The CYOD trend is common among organisations who prefer to own mobile devices that are used by employees, using this strategy organisations can drive the mobile device management, *inter alia*, to protect information stored on the device (Vorakulpipat, Sirapaisan, Rattanalerdnusorn and Savangsuk 2017). Proponents of this trend state that it minimises information security risks, unlike the BYOD trend it eliminates the confusion relating to ownership of information stored on the mobile device (Almarhabi et al., 2017).

On the other hand, Corporately Owned Personally Enabled (COPE), - allows the employee to choose their device from a pre-approved list provided by the company, the company pays for and own the device while the user (employee) has the freedom to use it (Vorakulpipat et al., 2017). In the COPE arrangement, the security features such as the Mobile Device Management software may come pre-installed on the device, the employee may have restrictions in downloading certain software that may pose a risk to the security of information on the device (Dhingra, 2016).

Further, the COPE environment may facilitate the adoption of the Software as a Service (SaaS) trend since employees are allowed to enable their devices (Agarwal and Agarwal, 2011). SaaS trend allows users (in this case employees) to download software, applications that they prefer over the internet such as Google Apps (Agarwal and Agarwal, 2011). However, SaaS like other trends carries a risk of exposing the organisational information to information security threats that are lurking in the cloud environment (Agarwal and Agarwal, 2011).

In the context of this study, the BYOD phenomenon is defined as the strategy adopted by organisations where employees are allowed to use their personal mobile devices to perform work functions partially or in full.

1.3 Background

Treasury is a government department responsible for the division of revenue, allocation of equitable share, auditing, forensic investigations as well as financial and fiscal management in the province. Treasury's mission asserts the value of employees in achieving its mandate, its core

values include professionalism, excellence and integrity, among other things. These are elements that the Treasury takes pride in, and represent the brand Treasury. In executing its mandate Treasury handles large quantities of sensitive information which must be protected against unauthorised access, maintain its integrity and avail information when called upon.

In the era of information age, mobile devices and wireless networks, employees want to stay connected with their work even outside working hours (Ubene et al., 2018). The ubiquitous nature of technology provides employees access to corporate networks and information at the click of a button provided there is an internet connection (Rainer et al., 2015). The Bring Your Own Device (BYOD) phenomenon refers to a trend where employees are permitted to use their own mobile devices to access organisational network and information (Anderson, and Kaul 2017).

A study conducted in Croatia found that 28% of employees were more productive as a result of unlimited access to their work, moreover, using their device of choice makes working a lot pleasing and it brings to life the old adage of work hard, play hard (Peraković, Husnjak, Mišić, Kuljanić and Mijo, 2016). Some proponents of the BYOD, posit that by implementing the BYOD, employers save costs on purchasing equipment and keeping up with the latest technology (Almarhabi et al., 2017).

The workforce demographics have changed and consist of mainly the techno-savvy generation (millennials and generation Z) which embraces technology faster than the older generations who often struggle to keep up (Steelman and Sabherwal, 2016). Organisations, government sector in particular, often struggles to keep up with the latest technology and equipment, among other things, due to the cost factor, as a result, employees are often burdened with obsolete equipment and outdated technology, this creates dissatisfaction and frustration among employees, the younger workforce in particular (Khakurel, Melkas and Porras, 2018).

Some of the studies conducted on the impact of the BYOD on productivity revealed, *inter alia,* that the BYOD strategy, allows employees to enjoy flexibility and satisfaction of performing their work when they most feel relaxed resulting in getting more work done (Seth, 2016). Proponents of the BYOD argue that mobility enables employees to get more work done even after normal working hours (Almarhabi et al., 2017). Whereas the BYOD has a number of benefits for the organisation, it also carries disadvantages, mainly that of information security risks and threats

(Bello Garba, Armarego and Murray, 2015). The BYOD presents in the era where cyber threats such as espionage, malware, denial of services to name a few are at the highest (Vorakulpipat et al., 2017).

Treasury offers mobile devices on a company scheme to qualifying employees, based on seniority and operational requirements which can be termed Corporately Owned Personally Enabled (COPE). However, apart from commercial security features, there are no defined or organisational security measures to protect information (Akadeo, 2016). In spite the policy provision that "*privately owned mobile device can only be used if the user agrees to the installation of security software, remote monitoring",* there is no monitoring of private devices.

In Treasury, a number of employees use their private mobile devices to access departmental information predominantly through email, calendar, contacts and/ or other forms. This practice is allowed since some of the employees work outside their offices for extended periods, some, the nature of their work requires them to have ongoing access to their emails for example even outside working hours and environment. The preceding reasoning for granting users access to some or all of the enterprise applications can be viewed to be in support the argument that convenience, productivity and cutting-edge technology are the main drivers of implementation of the BYOD in Treasury.

However, traditional methods of information security are limited to securing information within the domain of organisational IT department, for example, it does not extend to cloud and mobile (Almarhabi et al., 2017). These inadequacies leave proprietary information vulnerable to a third party's malicious intents due to lack of security measures and or negligence of the user, these will be discussed further in the following chapters.

In the implementation of the BYOD, organisations must be conscious to the competing priorities namely, employee convenience, productivity and preservation of Integrity, Confidentiality and Availability (CIA) of proprietary and personal information (Anderson et al., 2017). It is imperative that organisations define the security measures, level of access, mitigation strategies for an array of negative possibilities such as loss of the device, ownership of information stored in the personal device, among other things (Steelman and Sabherwal, 2016). Convenience and short term profits from increased production should not form sufficient ground to risk losing future competitive advantage (Peraković, et al. 2016).

The study investigates the effects of the BYOD on information security within Treasury. This chapter presents the background and rationale outlines the motivation and focus of the study. An overarching objective and sub-objectives of the study and research questions are highlighted followed an in-depth discussion of the problem statement. The literature review undertaken for the study is presented and the research design and methodology outlined.

1.3 Motivation of the study

The public sector (government departments) is unwittingly participating in the BYOD phenomenon, however, there are no clear guidelines, policies for the utilisation of the BYOD as well as management of the BYO devices (Dingwayo and Kabanda, 2017). There are no clear information security policies that detail the user's responsibilities regarding the safeguarding of information. The employer has no comprehension of how much and what information is stored in the users' private devices, as a result, has no control over it.

This study aims to benefit both the public and private sector by providing the policy framework for the implementation of the BYOD in the public sector. While the private sector, such as the academia has taken on the BYOD route, however, there is a lack of a framework for the utilisation of the BYOD as well as ownership of information. This is a first study conducted within the public sector in the KwaZulu-Natal Department of Treasury and it will form the basis for future research. It aims to start the discussion pertaining to the issues relating to information security within organisations and the need to protect such information regardless of where it is stored.

1.4 The focus of the study

The study focuses on information security management including policy framework, and risk aspects of the BYOD strategy on information security within an organisation. The technical aspects will not be dealt with.

1.5 Problem statement

The value of information generated and handled by government employees is huge, however, the inadequate attention towards the security of information in the public sector is appalling. The public sector can no longer shy away from the BYOD phenomenon, it has to decide to embrace or revoke it (Steelman and Sabherwal, 2016). The number of employees using their private devices to access organisational information whether for email or sharing documents is significant for it to be left uncontrolled (Ubene et al., 2018). The use of unsecured private mobile devices exposes the organisation to a plethora of security risks including information leakages, the proliferation of viruses and malware that could lead to serious cyber-attacks on the network such as denial of service (Muhammad, Ayesh, and Zadeh, 2017).

Information is a source of competitive advantage for most organisations including government sector, therefore, information must be protected against prevailing threats and emerging risks (Cho, 2016). The principles of information security which are confidentiality, integrity and availability (CIA) underpinning this study cannot be satisfied if users continue to access and store information in their unsecured private mobile devices without the employer's knowledge, this practice may have serious legal and reputational damage should the information be lost or accessed by unauthorised person (Dhingra, 2016). While some of the drivers of BYOD, include convenience, improving staff morale and satisfaction as well as an increase of production, these should not be achieved at the expense of confidentiality, integrity and availability of information (Steelman and Sabherwal, 2016). Mphahlele (2016) states that instead of pretending that BYOD does not occur, accepting the BYOD means organisations must have in place strategies and measures to mitigate, among other things, information security risks such as unauthorised access to the device and information. Similarly, a study by Musarurwa, Flowerday and Cilliers (2017) found that employees are aware of the BYOD trend and are keen to participate but the employer has not provided the policy framework for implementation.

The organisation must not renege of its responsibility to safeguard information even if it is stored in private devices, this could be achieved by detailing clear procedures for storage, security and access to information (Steelman and Sabherwal, 2016). Risks, such as loss of the device leave the employer without any recourse as far as proprietary information stored on the device is concerned since the employer does not know what information has been shared and stored in the users private

device to be able to gauge the extent of lost information and damage to the organisation (Li and Yang, 2017).

There are no basis to implement control measures due to the lack of decisive, comprehensive policy position and framework for implementation of the BYOD (Hemdi and Deters, 2016). The assurance that departmental information is kept along the principles of maintaining integrity, confidentiality and availability of information can no longer be provided (Krauss, 1980). The problem with failure to provide assurance regarding security of information leads to a lack of trust (Ubene et al., 2018). Having identified and elucidated briefly the problem with BYOD this study seeks to ascertain the effects of the BYOD on the security of information in Treasury.

1.6 Objectives

The general objective of this study is to ascertain the effects of the BYOD on information security within Treasury further, to ascertain specifically the following sub-objectives:

Objective one

- To identify the prevalence of the BYOD among employees within the Treasury.

Objective two

- To determine information security risks posed by the BYOD on the security of information at Treasury.

Objective three

- To investigate the management of the BYOD (mobile devices) within Treasury.

Objective four

- To ascertain the benefits of the use of the BYOD within Treasury.

1.7 Research questions

- To what extent is the BYOD practised within the KZN Treasury department?
- What are the risks posed by the BYOD on information security within the Treasury?

- How are the BYOD (mobile devices) managed within the Treasury?
- What are the benefits of the BYOD within the Treasury?

1.8 Methodology

The purpose of the study is to investigate the effects of the BYOD on information security, it follows the positivist paradigm (Creswell, 2014). Since the researcher seeks to determine the existence of and quantify the same, this study follows quantitative research methods (Saunders, 2011). The population of the study is all employees of Treasury. The rationale is that all employees in Treasury have an equal chance of participating in the BYOD. Further, all employees in Treasury bear the responsibility to safeguard information entrusted to them by the employer. Sekaran and Bougie (2016) provide a blueprint of an acceptable sample size to achieve an acceptable level of reliability and validity.

Given the foregoing assertion on the BYOD participation and information security responsibility, the random sampling method is preferred in this study. In this study, the total population is 450, therefore, a total number of 167 respondents is required to accomplish the desired level of reliability and validity (Sekaran and Bougie, 2016). Data collection will be undertaken using a self-developed questionnaire. While there are a number of available methods of administering the questionnaire, the researcher preferred to personally administer the questionnaire to employees (Sekaran and Bougie, 2016). Collected data will be cleaned and entered on an excel spreadsheet for further processing and analysis.

1.9 Chapter outline of the dissertation

This section provides an outline of the study, for convenience the outline is presented chronologically in chapters.

Chapter one: Introduction

Provides the background of Treasury, the focus of the study, the motivation for the study, problem statement, research objectives, research questions, an overview of the research methodology for the study and limitations.

Chapter two:Literature review

Introduces the theoretical framework and the review of the literature on the subject. The literature in this study is organised in line with the objectives of the study.

Chapter three: Research methodology

Elucidate on the research design and methodology preferred in this study, population, sampling strategies, data collection and analysis choices made in this study.

Chapter four: Presentation of results

Illustrate the results of the study through statistical analysis and interpretation. Meaningful inferences will be drawn from the collected, analysed and interpreted data.

Chapter five: Discussion

An in-depth discussion of the results of the study drawing comparisons with previous studies and the literature on the subject matter will be offered.

Chapter six: Conclusion and recommendations

The final chapter offers the conclusion of the study, implications and limitations of the research, and provide recommendations to solve the problem as well as areas for future research.

1.10 Summary

This study aims to echo the importance of information as a strategic resource for an organisation which must be protected commensurate to the ingenuity of prevailing threats and emerging risks. Further, the competing interests of employee's convenience, improved productivity versus the responsibility of securing information are highlighted. In this chapter, the background of the Treasury and some of the key functions the department performs was delineated. The BYOD phenomenon was discussed along with similar trends practices in various organisations.

Given the nature of functions performed at Treasury, the risk posed by the presence of proprietary and personal information on the BYO devices and without the requisite security module was discussed. The motivation of the study is anchored on the need to protect proprietary information

from unauthorised access, maintain its integrity and ensure its availability upon demand. The problem statement highlights the presence of sensitive proprietary and personal information and begs the question of information security in the era of the BYOD within the Treasury. Research objectives and questions were provided and an overview of the research methodology preferred for the study was presented. The following chapter introduces the theoretical framework underpinning the study as well as literature review.

2 Chapter two: Literature Review

2.1 Introduction

This chapter examines the existing body of knowledge relating to the prevalence of the BYOD trend, inherent information security risks posed by participation and or adoption of the BYOD trend, management of the BYO devices as well as benefits of implementing the BYOD in an organisation. In this chapter, a theoretical framework underpinning the study will be discussed and a critical review of literature relevant to the research objectives will be undertaken to expose gaps in literature where a further contribution can be made. The chapter concludes with a summary.

2.2 Theoretical framework

Saunders (2011), defines theory firstly as setting out the concepts of the study secondly, determining whether the cause and effect relationship between the variables exist or not and lastly explain the relationship or lack thereof between the variables. Information security theories were developed just as the internet became public and personal computers took off. The development of technology, equipment, and availability of the internet ushered in new risks on both technical and administrative use and management of information technology network within organisations (Parker, 2015). A number of theories are discussed below however, the CIA seems to be the one theory that most organisations use to inform their information security requirements (Nweke, 2017).

The realisation by organisations and government that information was indeed a source of competitive advantage dates back to the cold war era (Rainer et al., 2015). In the early developments, computer security saw the introduction of the checklists, the aim of the checklists was to audit the security proficiency of the computer systems, ascertain if the existing security measures are effective and efficient and well as recommending upgrades where necessary (Krauss, 1980). Later on, and with the development of technology and the concept of information security, some of the detractors of the checklist raised concerns that the checklists were merely an operating procedure rather than an information security tool (Parker, 2015).

Along came the confidentiality, integrity and availability the so-called (CIA triad), the CIA triad provided a clear basis for information security which is the preservation of confidentiality,

integrity and availability (Nweke, 2017). Confidentiality can be defined as the safeguarding of information from unauthorised disclosure through the application of security procedures including the use of passwords, network security and encryption of information stored on as well as securing communication and information sharing platforms (Agarwal and Agarwal, 2011).

According to Agarwal and Agarwal (2011) in the context of information security, integrity relates to assurance that the essence of the information stored and or transmitted is not altered while in transit whether electronically and or manually by implementing network protection procedures, intrusion detection software and suitable registry protocol in case of manual deliveries. Nweke (2017) asserts that availability is the guarantee that information will be available timely and uninterrupted on demand for both manual and electronic mediums by implementing sound registry procedures and in case of electronic information the use of cloud as an example.

While Nweke (2017) supports the CIA triad as the fundamental building blocks of an organisation's information security strategy, he offers the Authentication, Authorisation and Accounting (AAA) model which must be adhered to achieve or satisfy the CIA of information. Even though the AAA model brings in a crucial element of accountability, very little has been written about the AAA model as an enabler of CIA of information.

Arguably, most organisations base their information security policies and protocols on the CIA model (Nweke, 2017). Some scholars agree that the fundamental reason to protect information is to preserve its confidentiality, integrity and availability (Roy, 2012). However, like the checklists some scholars reject this theory as incomplete (Parker, 2015). Don, (2015) argues that the CIA triad does not capture practical implementation and the technological advancements of IT and information security.

Parker (2015), introduces what he terms the six information security elements, this framework includes availability, utility, integrity, authenticity, confidentiality and possession (CIA+UAP). While the theory submitted by Parker (2015) added other dimensions that must be observed in the protection of information, it did not gain much popularity within the information security management sphere. In this study, the CIA is the preferred underpinning theory.

2.3 Prevalence of BYOD

The Bring Your Own Device (BYOD) phenomenon refers to a trend where employees are permitted to use their own mobile devices to access organisational network and information (Anderson et al., 2017). According to (Bradley et al., 2012) the BYOD as a universal trend, where employees carry their own devices and use them to connect to the corporate network and or access certain functionalities such as emails, a calendar to name a few. Differently stated, the ubiquitous nature of mobile devices, technology and the internet mean employees no longer need to rely on corporate networks to fulfil their work obligations.

Mobile computing, globalisation, work pressures and other aspects contribute to the increasing need for employees to remain connected and able to continue performing their functions way after normal working hours (Vorakulpipat et al., 2017)**.** The BYOD phenomenon is propelled by the advancement of technology, the dematerialisation of a smartphone (Rainer et al., 2015). Dematerialisation of a smartphone refers to the ability of a single smartphone to perform functions traditionally performed by a number of devices, an example a smartphone has a built-in camera (Reiner et al 2015). Conversely, Bello Garba et al. (2015) argues *inter alia* that this contributes to employees preferring to use one device for both work and personal needs. The foregoing argument is further substantiated by (Rainer et al., 2015) in their assertion that proliferation and ease of access to wireless technologies, dematerialisation of Smartphone's and the influx of mobile devices creates a substantial case for the use of BYOD.

Olalere et al. (2015) point out that the influx and popularity of mobile devices specifically smartphones, the convenience of doing work anytime, anywhere makes the BYOD strategy attractive and as such organisations can no longer afford to ignore the BYOD reality in their ICT strategy. In support of the above argument regarding the influx of smartphones, (Alsaleh et al., 2017) found that in the United States of America more than 334 million smartphones were sold in less than 3 months in 2015, reveals a study which investigated, among other things the popularity of smartphones.

In some organisations, the BYOD strategy is implemented formally, meaning there is a policy framework that details the type of device, type of information that can be accessed and stored on the BYOD device and the acceptable level of security to ensure preservation of confidentiality, integrity and availability of proprietary information on the BYOD device (Dingwayo and Kabanda, 2017). However, Dingwayo and Kabanda (2017) warn that some organisations, government departments, in particular, have not formalised the adoption of the BYOD, the absence of formalisation may not be construed to mean that there is no participation by employees on the BYOD phenomenon. While BYOD has not been studied in depth in the context of the South African public sector, however, studies conducted found that 63% of South African employees are allowed to use their private devices on enterprise network, by contrast, the same study found that only 5 % of organisations had formally adopted the BYOD policies (Dingwayo and Kabanda, 2017).

Just like any new technology or trend, BYOD took off like a house on fire in the late 2000s, in 2013, Gartner predicted that in 2017 most organisations will have BYOD in place (Gartener, 2013). Further, Dhingra (2016) argues that the prevalence of the BYOD phenomenon may reach at least one billion active BYOD devices globally. The BYOD trend is not unique to established multinational companies but it also manifests in small and medium enterprises as well as in the public sector (Fani et al., 2016). However, in a study about BYOD adoption in the South African banking sector, Mphahlele (2016) found that in 2015 at least 38% of employees were participating in the BOYD phenomenon worldwide. In the same vein, (Ubene et al., 2018) point out that in the United Kingdom (UK) the survey conducted on the public sector employees found that 73% of organisations in the public sector domain have implemented the BYOD strategy.

On a similar note,(Fani et al., 2016) found that smaller companies (SMME sector) are more likely to fully adopt the BYOD strategy instead of the complex fixed network infrastructure preferred by large corporates, therefore, in view of the latter statistics in comparison with the earlier statistics provided above the BYOD trend is seemingly attractive and useful strategy however, organisations are not quick to adopting it as previously predicted earlier on in by Gartner. Whereas, a study by Musarurwa et al. (2017) found that employees are aware of the BYOD trend and are keen to participate but the employer has not provided the policy framework for implementation.

Bradley et al (2012) conducted a survey which found that the BYOD phenomenon is a universal trend, further, that at least 89% of the IT departments wholly or partly supports the BYOD strategy. As a result, Bradley et al (2012) refer to the phrase 'mobile workers', they describe these workers as those employees who continually rely on their mobile devices for both work and personal use, they argue further that these are born out of elimination of reliance on fixed corporate networks.

Arguably, most organisations underpin the adoption of BYOD on one or a combination of the following key drivers: improving productivity, employee satisfaction, saving on capital costs associated with purchasing equipment and boosting staff morale, among other things (Anderson et al., 2017). A notable increase of employee productivity makes a compelling case for the adoption of the BYOD in organisations. Conversely, (Ubene et al., 2018) asset that the rigid nature of most corporate policies and privacy issues, employees simple opt to use their own equipment for both work private use (Bradley et al., 2012).

Adoption and or prevalence of the BYOD in a workplace may be affected by a number of factors, among other things, the workforce demographics and agility of information security policies (Li and Yang, 2017, Peraković et al., 2016). Peraković et al., (2016), found in the study in Croatia that the workplace demographics further determines the acceptance and participation on the BYOD since new technology largely appeals to the generations of millennials. Li and Yang (2017), found that the mobility provided by the BYOD may be contributing to anxiety and burnout.

Fani et al. (2016), investigated the BYOD phenomenon in the Small and Medium Enterprises (SME) in South Africa, it was found, among other things, that there is a need for adoption of BYOD within the SMME sector and further outlined the requisite key success factors for the successful implementation within the sector.

Kebande et al. (2016) point out that while the BYOD may present benefits and opportunities for organisations, it also poses a plethora of risks particularly the information security risks, as well as the privacy of personal information as such organisations implementing the BYOD strategy, must have in place proper management tools to mitigate the risks. However, in the case of the South African public sector which is the focus of this study as well as private sector, studies have shown that challenges such as information security and privacy, among other things, have brought the early adoption of the BYOD to a doubtful start (Dingwayo and Kabanda, 2017).

2.4 Information security risks

Rainer et al. (2015), define information as any recorded or displayed data or knowledge or content of the communication, regardless of its format. From a government perspective, information is defined as any recording, knowledge, content stored or communicated (Agency, 1996). According to the proposed Protection of State Information Bill (POSIB (2016) information security is defined as the means of protecting information from the threat. On the other hand, information security, is defined as the methods, procedures, and processes necessary to the preserve confidentiality, integrity and ensure availability of information through prevention of unauthorised disclosure, modification, destruction and loss of proprietary information (Fani et al., 2016). Similarly, the Minimum Information Security Standard (MISS) defines information security as the 'conscious provision and application of security measures to protect information irrespective of its medium' (Agency, 1996). Since the focus of the study is on a government department the definition provided in the MISS stated above is adopted herein.

Ubene et al., (2018) submit that information is a source of competitive advantage for most organisations including government sector, therefore, information must be protected against prevailing threats and emerging risks further, the confidentiality, integrity and availability of information must be ensured. In agreement with Ubene et al (2018), Dhingra, (2016) asserts that the principles of information security which are confidentiality, integrity and availability underpinning this study cannot be satisfied if users continue to access and store information in their unsecured private mobile devices without the employer's knowledge, this practice may have serious legal and reputational damage should the information be lost or accessed by unauthorised person.

Gao and Zhong (2016), emphasises the value of information for an organisation and asserts that organisations should recognise the value of its information and be prepared to protect their competitive advantage and profits which are directly linked to the information it has. Further, that loss of information such as customer information may have disastrous consequences including loss of revenue and reputational damage (Gao and Zhong, 2016).

Of all risks associated with the BYOD strategy, security of information ranks high Gartner (2013) sharing a similar view Distere G (2013) who as early as 2013, coined the phrase "Bring Your Own

Danger" in reference to legal and security dangers potentially posed by implementation of the BYOD strategy in organisations. Dingra (2016) submits that security of information on the BYOD device ranked among the highest concerns for organisations in implementing the BYOD strategy, threats such as network intrusion and eavesdropping have steadily increased in the recent past, the ease of launching these attacks has also increased. Vorakulpipat et al. (2017), in a similar vein concur that these threats may be targeting the individual and or the organisation. Vorakulpipat et al. (2017) assert that in most cases, network intrusion has been easily facilitated through email links, malicious applications therefore by combining private and proprietary information on a single device, the probability of materialisation of the threat multiply.

Information security risks include loss, destruction, modification and unauthorised access to privileged information name a few (Arregui et al., 2016). Risks are inherent in organisations' corporate ICT system, the key is to identify these and implement countermeasures to mitigate the same (Anderson et al., 2017). Mobile devices including but not limited to laptops, smartphones tablets etc. are the most common devices used by employees in the BYOD environment (Hemdi and Deters, 2016). One of the most prevalent risks to proprietary information is a loss of mobile devices, which implies a loss of information stored within the devices (Vorakulpipat et al., 2017). The concern of lack of security measures to safeguard information aggravates the risk of unauthorised access to information. Organisations who have accepted BYOD must have policies in place that, among other things, guide the users on the security imperatives to be observed (Vorakulpipat et al., 2017).

The source of some organisational concerns regarding the implementation of BYOD is the threat it poses to confidentiality, integrity and availability of information since the organisation does not own or have full control over the BYOD devices used by employees for work purposes (Bello Garba et al., 2015). Bello Garba et al. (2015), argue that the presence of different mobile applications (Apps) may lead to exfiltration of data among apps which is further exacerbated by the lack of adequate security measures to protect proprietary information on the device (Bello Garba et al., 2015). Further, a threat of social engineering coupled with malware is a lethal combination, users can be deceived to downloading links which contain malware thereby exposing confidential information to unauthorised recipients (Bello Garba et al., 2015). Social engineering

is where a user can be tricked to believe the other party and begin to share information with them (Reiner et al. 2015).

Fani et al. (2017) submit that the information security and other risks associated with adoption of the BYOD are not insurmountable, organisations must develop and implement credible and well researched BYOD security framework that will govern the BYOD implementation and management of risks associated with the BYOD. Whereas Das and Khan (2016) submits that there is a conflict of priorities between the user and the organisation in that, that users are more concerned about the effects of malware and other threats on the privacy of their data however, concerns do not extend to possible targeted theft of proprietary information, on the other hand the organisation is more concerned about the security of proprietary information consequently, in the BYOD environment, this attitude further expose the organisation to information security risks.

Okere et al. (2012), introduce the information security culture construct within an organisation in an argument that security of information is dependent on what the organisational culture is in relation to information security. Okere et al. (2012) argue further that organisations must have an enabling culture underpinned by information security knowledge. Similarly, Carcary et al. (2016) point out that organisational culture and the attitude which users have towards information as a valuable asset and recognition of the need to protect the same determines the successful implementation of an information security programmes resulting in a notable reduction of information security breaches.

User behaviour, is another source of risk argues Wu and Wang, (2016), that the sense of comfort between the user and the recipient influences disclosure of proprietary information (Wu and Wang, 2016). In concurrence, Alsaleh et al. (2017) mentions, among other things, that lack of awareness by users of smartphones in particular that downloading malicious applications and software onto their device exposes the device to an array of security risks including hacking and malware these risks can easily transfer to the corporate network when connecting and or sharing documents and emails. The same view is shared by Carcerey (2016) that even if organisations can have in place technical tools to safeguard its information, the key to a successful information security programme is dependent on the level of security consciousness on the part of employees and or users

Likewise, Fani et al. (2017), emphasise the importance of continuous education of users on their role in the implementation of information security further, Dingra (2016) stresses that users must be educated about the possible consequences of their behaviour on the security of information, possible litigation and reputational damage to the organisation. Garba et al. (2015) warn that while information security attacks may emanate from outside the organisation, however, in some cases there is what they term "malicious insider action", this is where unauthorised disclosure of information is intentionally done by employees who have access to information.

Agarwal and Agarwal (2011) argue that trends such as the SaaS compounds the problem of information security since it allows users to store information not only on the device but also on the private cloud storage facility of their choice, on the other hand (Balozian and Leidner, 2017) found that device selection and customisation influence the choice of a device, users have the freedom to choose their BYO device and the choice of the device is often informed by the aesthetics and functionality, rarely is the choice based on level of information security and or privacy the device provides. A similar view was found in a study by (Peraković et al., 2016) that based on their needs and preferences, users grant application developers permissions to applications such as contacts, camera etc sensitive information on the devices without knowledge of the developers privacy policies and due consideration of security of information in the device.

Alsaleh et al. (2017) assert that smartphone vulnerability has grown up to 32 %, meaning that the smartphone is the device mostly susceptible to targeted and incidental attacks. These are attributed to the sheer lack of awareness and a false sense of security that users have that controlled app stores are secured. The security risks are further compounded by the fact that users grant free applications permissions to access their information such as location, contacts, camera and others, (Alsaleh et al. 2017).

A study on the behaviours of smartphone users found that 43% of the participants knew the smartphone security pin of a friend or family member Alsaleh et al., (2017), this observation reveals not only negligent behaviour but also a lack of security consciousness among smartphone users. The nature of a smartphone is that it's a multipurpose device, at least 13% of the users used the cloud services to back up data from their smartphones, and this brings forth the question of ownership of data kept on the mobile device (Alsaleh et al. 2017).

The use of independent cloud storage to store proprietary information remains a threat to the security of information since the security of the cloud may not be in line with organisational standards (Mvelase et al., 2014). Therefore, the security vulnerabilities of the cloud can be exploited to access, modify and or even remove information therein, the consequences being a failure to ensure that proprietary information is secured in line with the CIA principle (Mvelase et al., 2014). Loss of information and or premature exposure of information may have serious repercussions such as loss of the competitive edge, reputational damage to name a few (Vorakulpitat, et al. 2017).

Storage of information on mobile devices and public cloud services that organisations do not have control over places the security of information at risk of unauthorised access and possibly compromise the confidentiality, integrity and availability of information principle (Mvelase et al., 2014). Secure storage of information is critical as an enabler of the BYOD strategy in the public sector, in particular, Mvelase et al. (2014), propose a public cloud that will be enabled by government and possess the requisite security measures to safeguard the information.

Loss of a device is one of the information security risks highlighted by Vorakulpitat, et al. (2017), loss of a device containing proprietary information could lead to premature exposure of such information and loss of competitive edge, an overwhelming 37% of participants in the smartphone user's behaviour believed that their data could not be accessed if the lost phone was locked (Alsaleh et al. 2017). This finding confirms the submission by Garba, et al. (2016) that educating users on information security risks as well as their roles and responsibilities is critical in preserving the CIA principle.

Vorakulpitat et al. (2017) accentuate that the risk of mobile in particular BYOD devices connecting to the corporate network, given that the users download, among other things, free games and APPs which give access privileges to various device applications such as contacts, camera to name a few these could easily transfer viruses, malware onto the corporate network resulting in unavailability of information on demand. While, Alsaleh et al. (2017) highlight the behaviours of smartphone users in particular, as posing an information security risk, he maintains that by chatting, sharing photos and documents downloading free games and providing applications access to device applications results in a mobile device being vulnerable to information security breaches.

Widely accessible internet and the availability of commercial cloud that promises users protection of information has only increased the need for organisations to secure their information and information systems against the threat of malware, spyware and cyber-attacks to name a few (Balozian and Leidner, 2017). If organisational networks which enjoy sophisticated security applications is susceptible to security threats then the privately-owned mobile device and cloud service cannot be precluded from the same threats.

2.5 Management of BYOD

Fani et al. (2016) brand the BYOD strategy an institutionalised security risk, therefore, technical tools such as the network security, network access control, firewalls are an existing part of information security architecture, however, in a BYOD environment none of these sophisticated information security tools exists. Therefore, the argument that sharing and continuous education of users on information security roles and responsibilities hold true (Wu and Wang, 2016).

Fani et al. (2016) share, among other things, the tools that organisations considering BYOD implementation should have in place. Chief among these is the BYOD management policy that should guide the implementation of BYOD, define roles and responsibilities, deal with breaches and compliance monitoring thereof. According to Carcarey et al (2016), security awareness and training are critical for users to understand their roles and responsibilities in relation to security of information further, embedding an organisational culture of security awareness is just as important.

In addition to the BYOD implementation and management policy framework, Vorakulpitat et al. (2017), warn that the use of mobile devices heightens the risk information security breaches, this threat is further exacerbated by not keeping a record and registering BYOD devices that are allowed on the corporate network. The risk of an employee losing the device containing corporate information is omnipresent, therefore, a mechanism of tracking BYOD devices is critical in the management of BYOD in an organisation (Vorakulpitat et al. 2017)

Mobile device management (MDM) is a software that is commonly used by organisations to manage access to the corporate network by a mobile device, the employer may require the employee to install and adhere to the MDM protocol when participating in the BYOD (Dingwayo and Kabanda, 2017). However, the fact that MDM grants the employer the administrator rights including, among other things, remote access and control of the device leaves a bitter taste on

employees who tend to value their privacy over the security of proprietary information argues (Dhingra, 2016).

Proponents for the MDM expound that MDM presents the most practical device management tool to mitigate information security risks associated with BYOD and it is available for most operating systems including IOS and Android (Steelman and Sabherwal 2016). Small-scale organisations (SMME's) often find that the traditional IT networks are cumbersome to manage and expensive to install, therefore, innovations such as BYOD provides the technology needed at minimum cost (Bradley et al, 2012).

In order to mitigate security and privacy risks, organisations must have clear policies on the selection, management, security of information access to the BYOD device (Steelman and Sabherwal, 2016). In organisations where the policy requires an employer to install preapproved software or remote management of any sort to safeguard information thereon, such imposition may be viewed as an invasion of privacy (Dhingra, 2016). Similarly, organisations where there are no defined policies for the use of BYOD there is an ongoing confusion regarding the users as well as organisation's roles and responsibilities as far as information control, ownership and security are a concern submits (Dhingra, 2016). However, a survey by Gartner in 2015 found that only 30% of companies have approved BYOD policies, 50% of the companies do not stipulate the expected level of security for the device (Rice et al. 2016).

Mobile Application Management (MAM) is a component of MDM, MAM is responsible for vetting of mobile applications, where MAM is adopted the employer and employee agree on acceptable public applications that the user can install on the BYOD device, if an application is not within the agreed list it is not allowed (Li and Yang, 2017). MAM can be a useful tool in monitoring the use of various applications thereby ensuring that employees remain productive(Li and Yang, 2017).

On the other hand, Arregui, et al., (2016) proposed MAM in a form of an enterprise app store where users can download applications vetted applications in the main these are developed and driven by the organisation. While Steelman and Sabherwal, (2016), concedes that enterprise technology is rather slower than a commercial one, therefore, the enterprise app store may not

present users what they seek in the first place which is cutting edge latest technology and equipment.

Scholars such as Olalere et al. (2015) argue that deployment of MDM on the BYOD devices does not address the security challenges and risks posed by the BYOD further, argues that MDM is merely a governance tool and it does not prevent threats such as targeted attacks on the device. Olalere et al. (2015) warns that while the threat of a compromise of proprietary information is real, by implementing stringent control measures such as MDM which threatens the privacy of personal information, organisations threaten the adoption of the BYOD within the organisation.

Olalere et al. (2015) postulate that the organisational and individual interests and benefits, as well as concerns in the implementation of the BYOD strategy interest, differs. Users interests are largely based on convenience and their concerns are the privacy of their information whereas, the employer's benefit is an increase in the productivity levels and their concerns are that of information security risks that are inherent in the BYOD strategy Olalere et al. (2015). Downer and Bhattacharya (2015) warn that organisations must classify and implement restriction on information and the extent of access granted to the BYO device.

User behaviour, is another source of risk argue Wu and Wang (2016), that the sense of comfort between the user and the recipient influences unwitting disclosure of confidential information (Wu and Wang, 2016). In some organisations unauthorised disclosure of information is intentionally done by employees who have access to information, this phenomenon is termed malicious insider action (Bello Garba et al., 2015), in congruence, Downer and Bhattacharya (2015) cautions organisations to pay attention to users who are unreasonable against any form of device management and or restriction of access to the BYO device. Spoofing or interception of the network, these threats emanate from wireless networks such as Wi-Fi and the internet where a device can be tricked to connect on a cloned network or site (Bello Garba et al., 2015).

A study conducted in Croatia indicated that 44% of the respondents did not know if the company they work for has a BYOD policy while only 8% agreed to be aware and knowledgeable about their company's BYOD policy. Human element, is one important element that determines the success and or failure of any system, therefore, creating a workforce that is aware of information security risks, individual roles and responsibilities, policies governing the use of the BYOD and

sheer value of information requires organisations to embark on a comprehensive awareness and training programme (Peraković et al., 2016).

While the storage of proprietary information on private devices is inherent to the BYOD phenomenon, organisations adopting the BYOD strategy must have policies in place to mitigate information security risks Fani et al. (2016). Technical and management tools to mitigate some of the risks presented by the BYOD may be provided and implemented, however, as Choooi et al. (2016) assert a key component is whether employees themselves understand what is at stake, and what their role in the mitigation of risks is.

Kebande et al. (2016), hold the view that if security risks posed by BYOD are not adequately addressed, organisations face, among other things, loss of information. Cho (2016) argues that the advancements of technology carry equal advances and robust information security risks, with the BYOD phenomenon in place these risks could only be exacerbated, for that reason, organisations must design information security strategies that are relevant to the prevailing and consider the emerging threat.

2.6 Benefits of BYOD

BYOD is intended to help both the organisation and the employee achieve organisational goals, organisations derive benefit from an employee using the latest technology without any capital investment (Garba et al. 2015). The spread of the internet of things (IoT) meant that people, appliances and applications are able to store and share information when connected to the internet (Rainer et al., 2015). According to Vorakulpitat et al. (2016) the ability to share work information at the fingertips means much quicker decision making and a reduced reliance on corporate equipment and networks. Some scholars in favour of the BYOD states that organisations benefit from saving on capital expenditure on equipment because of employees simple use their own devices (Arregui et al., 2016). As early as 2013 the benefit of capital cost savings was recognised as one of the benefits of implementing the BYOD in an organisation (Disterer, et al. 2013). However, there seems to be a lack of studies where the organisations actually saved costs by adopting the BYOD.

On the one hand globalisation promotes the ability of businesses to connect and operate in a competitive space, therefore, ease of doing business, flexible operational hours, quicker decision making, faster commercialisation of ideas and implementation is essential for success and profitability of an organisation (Kotler et.al 2015). On the other hand, open sharing of information lays the basis for potential risks such as reputational damage, lack of trust and legal issues (Anderson et al., 2017). Human capital is one of the organisations valuable resource, the BYOD affords employees the freedom to perform their work using their own device as such this leads to an increase in staff morale (Dhingra, 2016).

Some of the most benefits of BYOD can be seen in how mobility, access to the internet propels the growth of small enterprises, small enterprises save costs on purchasing, installation and maintenance of IT network infrastructure by simply allowing employees to use their mobile device for work purposes. In this case, the organisation is wholly dependent on the BYOD strategy of IT (Bradley et al, 2012). By contrast, these small enterprises open themselves to the risk of losing their future earnings from possible exposure of proprietary information to competitors.

By using their private devices for work purposes employees open themselves to a possible invasion of privacy (Anderson et al. 2017). In organisations where the policy requires an employer to install preapproved software to safeguard information thereon, such imposition may be viewed as an invasion of privacy (Dhingra, 2016). Advanced applications and capability as well as personalisation of the smartphones, for example, users feel comfortable using newer technology and are keen to continue their work anywhere and anytime instead of the confines of the corporate network and office.

Often when new systems or technology is introduced there is a downtime due to the need to train staff on the system, the BYOD eliminated this drawback since users own, customise and understand their devices, therefore, they can continue functioning (Arregui et al., 2016). While Arregui, et al (2016) argue that there is no need for training on the use of the new device Anderson et al. (2017) argues that there is dire need to train and create awareness among users of the risks posed by the BYOD, organisational responsibilities, the limitation of their privacy as well as their role in the successful implementation and use of the technical tools provided for the preservation of proprietary information in personal devices.

A study conducted in Nairobi Equity Bank found that employee's convenience and improved production are the biggest drivers of the BOYD strategy in the organisation in the banking sector, Seth (2017) this finding correlates with the literature which also places convenience and productivity as key benefits of adopting the BYOD further, employees were also found to be more engaged, and motivated, this could be attributed to the ease of doing work and the removed pressure to be office-bound Vorakulpitat et al. (2017) also share the view that in organisations who have implemented the BYOD strategy the content levels of employees were higher.

In the era of globalisation, flexibility is essential therefore, the BYOD can be a catalyst for organisations to maximise on opportunities that come with globalisation (Vorakulpitat et al. (2017). Mobile devices can be flexible to different time zones and ability to use the same application to share or develop a document can increase productivity and efficiency as well as eliminate delays Vorakulpitat et al. (2017). In organisations where the BYOD strategy is implemented, employees' state that the work processes were much more efficient and flexible (Ubene et al.2018).

A study by Fani et al (2016) which focused on the governance of the BYOD in the small medium and micro enterprises (SMME's) found that the simplicity of IT infrastructure brought by implementation of the BYOD strategy may be of strategic value or benefit to the sectors who often do have large IT budgets and lack the requisite IT management skills.

Kebande (2017) concurs with other scholars that the BYOD strategy can result in cost-effectiveness for organisations by saving costs on software licencing and hardware maintenance, however, he cautions that the cost saving should be viewed in the light of organisational information risks as well.

The significant increase in the need for connectivity and use of IT within organisations places an enormous pressure on the traditional infrastructure, implementation of the BYOD strategy may be a solution to ease the pressures on the network (Kebande, 2017). Ubene (2018) found that the employees in the UK public sector averred that the BYOD strategy increased the job satisfaction levels.

2.7 Summary

Investigating the effects of the BYOD trend on information security within the Treasury is the aim of this study. The literature in this study sought to provide an in-depth analysis of the BYOD trend and show the link with information security through evaluating the existing body of knowledge on the subject. The literature review discussed the prevalence of the BYOD trend in Europe, America and South Africa. The enablers of the BYOD trend as well as business that are have taken on the trend wholly or partially were identified. Equally, some of the critical risk posed by the BYOD trend which is the security of information was discussed.

The most common threats posed by the BYOD trend, such as user behaviour and consequences thereof were dealt with at length. Management of the BYOD trend was highlighted including the available options of device management including software such as MDM. The importance of user awareness and training was also elaborated upon. This chapter also delved into the motivation for the adoption and participating in the BYOD trend is the benefits thereof. A number of benefits supported by studies conducted in different countries and scholarly articles. The following chapter details the research design preferred for the study along with research methods and data collection.

3 Chapter three: Research methodology

3.1 Introduction

The aim of the study was to ascertain the effects of BYOD on information security within Treasury. It looked at other possible factors that contribute to and or affect information security. This study took place in Treasury which is a government department in KwaZulu-Natal. The overall question of the study looked at the presence of the BYOD phenomenon within Treasury, whether there is a link between the BYOD and information security. This chapter considered the research design, location of the study and the research paradigms. Further, the population, sample, and the sampling strategy for the study were discussed. The data collection methods, data collection instrument design, the various methods of administering the data collection instrument and data analysis. Discussion on validity and reliability, ethical considerations, was be included and lastly, a summary will be provided.

3.2 Research design / strategy

Collis and Hussey (2003) define research design as the science and art of planning procedures for conducting research studies so as to get the most valid outcome. The end product of research design is a plan or blueprint for conducting the intended research (Babbie & Mouton, 2009). According to Wiid and Diggnes (2010), such a blueprint or plan for the intended research study is used to guide data collection and analysis. In essence, the research design focuses on the kind of study being planned, kind of results being aimed at, and the evidence required in adequately addressing the research questions.

The choice of research design appropriate for a study is based on the fundamental objective or purpose of the research, as well as the intended use of the research findings and recommendations (Kolb, 2008). There are various research designs that can be adopted in a study and these research designs can be classified into three main categories: exploratory, descriptive and causal (Collis & Hussey, 2003; Babbie & Mouton, 2009; Kolb, 2008; Wiid & Diggines, 2010). Exploratory studies aim to acquire insight and develop understanding than to collect accurate, replicable data (Wiid & Diggines, 2010).

Descriptive research goes further in examining a problem than exploratory research since descriptive research is undertaken to ascertain and describe the characteristics of the pertinent issues (Collis & Hussey, 2003). Causal studies are done mainly with the purpose to reveal cause and effect between the dependent and independent variables. In essence, exploratory research attaches meaning to variables; descriptive research often reveals possible links between particular variables; while causal research confirms and describes the relationship between variables or shows such relationship to be false (Wiid & Diggines, 2010). Differently stated, the exploratory research proposes new theories; descriptive research tests theories; while causal research reinforces theories.

This study adopted an exploratory research approach considering that the study was conducted to gain new insights, discover new ideas and increase knowledge of the phenomenon referred to as BYOD, a relatively new research area in South Africa. Unlike descriptive and causal research approaches, the exploratory research looks for patterns, ideas or hypothesis, rather than testing or confirming a hypothesis (Wiid and Diggines, 2010). This characteristic of exploratory research would be effective in achieving the envisaged outcome of this research, which was to identify and propose effective ways of implementation of the BYOD approach within the public sector in particular. Considering that the BYOD approach, is not yet well researched in South Africa, exploratory research was found to be the most suitable approach of three approaches considered. Barbie and Mouton (2009) assert that exploratory research is best suitable when a research examines a new interest or the subject of study itself is relatively new.

3.3 Research philosophy

Sekaran and Bougie (2016) mention various research philosophies discussed below. The research must have an underpinning theory. Positivist worldview, supports the view that the truth is absolute, depends on existing tools to support the search for the truth and relies on observations and conclusive views supported by science (Creswell, 2014). Constructivist perspective, that the truth is relative to one's feelings, knowledge as such it is about how people understand and make sense of a phenomenon under investigation (Sekaran and Bourgie 2016). Constructivist viewpoint, takes a qualitative research methodology, aimed at developing the body of knowledge on the

subject matter (Sekaran and Bourgie, 2016). On the other hand, critical realism posits that one can only get closer to the truth about a certain phenomenon, it acknowledges that the truth has the capacity of changing, it is not absolute and is influenced by many factors such as feelings, knowledge, etc (Damak 2015).

The positivist worldview was the approach preferred in this study. Considering the fluidity of information on the subject of information security, the frequent technological changes and new knowledge on the subject that is developed ever so frequently it is also important to quantify the extent of adoption of the trend within Treasury. This approach assisted the researcher to contribute to the body of knowledge on the subject at hand and quantitatively determine the effects of BYOD on information security within Treasury.

3.4 Research methods

According to Creswell (2014) there are three broad research methodologies that a study can follow namely, quantitative, qualitative and mixed method. The quantitative research method is often applied where the researcher seeks to identify the existence of the relationship between variables and or measure the effects of an independent variable on a dependent variable. This method is linked to the positivist worldview which holds that the truth is absolute, depends on existing proven tools to support the search for the truth and relies on observations and conclusive views backed by science (Creswell, 2014).

In contrast, qualitative research method holds the view that facts, observations can be given a specific meaning at a time through interpretation (Sekaran and Bourgie 2016). The main aim of qualitative methods is to develop knowledge on the subject while quantitative aims to prove existence of facts. Qualitative research relies on participants views and knowledge of the subject these can be given meaning though interpretation. This method is closely linked with the constructivist worldview. While, mixed method is the combination of the qualitative and quantitative research methods. Often, the combination manifests in the data collection and analysis phase of the research project. In this method, researcher adopts either a quantitative study with the element of qualitative such as incorporating interviews in the data collection or qualitative study

with the elements of quantitative by incorporating numerical data in the (Sekaran and Bourgie 2016).

In this study, quantitative research method was preferred, given that the study investigates the existence of a relationship between information security and the BYOD phenomenon as well as measure the effects thereof. It was found fitting to rely on quantifiable numerical data to establish the same.

3.5 Study site

Sekaran and Bourgie (2016) define a study or research site as the preferred location of the study where data will be collected. This study aimed at investigating the effects of BYOD on information within Treasury, as such the study site is Treasury. Treasury is a strategic department which, among other things, is entrusted with allocating and monitoring financial resources of the state as well as an audit function for the entire provincial government. Therefore, this study aimed to assist the department and the entire public sector in the development of best practices in relation to the BYOD participation and information security.

3.6 Target population

Saunders (2014) defines the target population as an entire unit that has an equal chance of being selected to participate in the study through a sampling technique. In this study the target population is the entire staff establishment of department which consist of 450 filled positions. Included in the target population were the different business units, senior, middle and junior management. All employees were targeted because of they have access to the shared network *albeit* at different levels however, a compromise at one point can have a ripple effect on the entire network thereby, compromising security of information.

3.7 Sampling strategy

According to Creswell (2014) there are two broad sampling designs namely: probability and non-probability sampling. Sekaran and Bourgie (2016) assert that probability sampling is used when the elements of the population have an equal chance of being chosen to participate in the study. Some of the mentioned sampling strategies below belong to the probability sampling family, simple random sampling where random selection from the sampling frame is done, systematic sampling where systematically and consistently the sample is selected from the sampling frame, stratified random sampling the sample is selected according to predetermined characteristics such as occupation lastly, cluster sampling where the sample is selected according to predetermined attributes such as geographical location (Sekaran and Bourgie, 2016). Saunders (2014) states that probability sampling is useful where the sample size is more than one hundred, further that this technique is used when every member of the population stands an equal chance of being selected to participate in the study (Sekaran and Bourgie, 2016).

Non probability sampling strategies include quota sampling where the quota is specified from the sampling frame,-purposive sampling is preferred where the specific information can be obtained from a participant based on their knowledge and or involvement on the subject, volunteer strategy is where participants volunteer to participate without being selected by the researcher and haphazard sampling where there is no specific criteria for selection except availability (Saunders 2014).

Consequently, the probability sampling particularly the random sampling strategy as the most suitable given that adoption of the BYOD is not limited to a few but rather all employees at Treasury have the potential to and or may be participating in the BYOD phenomenon. A single stage sampling procedure was applied since participants in this study are Treasury employees and the researcher has access to them. Sekaran and Bourgie (2016), provides a possible sample size based on the number of the total population. Based on the provided guideline the total population is 450 which consist of senior, middle managers and staff. Therefore, the participation of 167 staff members was envisaged in order to yield a confidence level of 95% with a 5% margin for error (Sekaran and Bourgie 2016).

3.8 Research instrument

Sekaran and Bourgie (2016), define a questionnaire as a set of predetermined questions used to collect necessary information on the subject at hand. Saunders (2011), states that questionnaires allow for the collection of standardised data from large sample sizes. Therefore, a questionnaire will be used in this study. Thirty two (32) closed questions were prepared in the questionnaire because the researcher sought to establish the existence and effects of the BYOD within Treasury.

The research instrument was made up of three sections, the first section had four questions which deal with the participant's demographical information, work experience and the position within the department. The second section dealt with issues relating to the objectives of the study. In relation to objective one, there were six questions which sought to find out if the participant took part in the BYOD phenomenon, frequency thereof as well as the device of choice. There were eight questions relating to objective two, these sought to ascertain the participant's behaviour, whether the participant's stored information on the private mobile device or not, loss of device as well as the security of the mobile device. The third objective was assessed using seven questions which sought to ascertain the management of the private mobile device and policy provisions relating to the BYOD. There were six questions assessing the fourth objective, these concerned the benefits of the BYOD for both the employer and the employee. The third section investigated whether the participant viewed the BYOD as a threat or an opportunity for the department.

3.9 Data collection

Data were collected over a two-week period from the 15th to the 29th of October 2018. The questionnaire had fifteen (15) yes or no questions as well as an option to answer only section A and C if the person did not participate in the BYOD. Sekaran and Bourgie (2016) state that the questionnaire should not be unnecessarily long because the responded my lose interest. The questionnaire for this study was designed to take ten minutes or less in the case of non -BYOD participants to fill.

There are a number of methods to administer the questionnaire to the participants, Sekaran and Bourgie (2016) mentioned three most used methods namely mail delivery, electronic delivery and

personally administered by the researcher. An online delivery method through email allows for the instrument to be delivered to all participants and ensures minimal interference with their daily work routines (Sekaran and Bourgie 2016). However, online delivery also carries a risk of questionnaires being forgotten by recipients.

The mail delivery method involves cost, takes longer to reach the participant and generally the response rate is low (Sekaran and Bourgie, 2016). Sekaran and Bourgie (2016) state that the personally administered questionnaire can be filled and collected quicker that mailed and or online questionnaires. In order to increase the response rate given the time constraints, the questionnaire for this study was personally administered by the researcher. This method was preferred because it is quicker and inexpensive while data was collected immediately. Choosing this method allowed for the informed consent letter to be incorporated as part of the introduction letter. In the introductory letter, participants were requested to indicate their voluntary participation in the study by signing.

3.10 Data analysis

Data were collected using manual methods, participants had to manually fill in their responses, therefore, upon receipt of filled questionnaires, the information was uploaded on an excel spreadsheet for further processing. Some of the received questionnaires were incomplete these were removed to ensure that data which will be analysed is complete. The Microsoft excel function was used to further clean up collected data. Descriptive statistics function on the SPSS programme version 25 was used to analyse the data. The researcher also made use of the cross tabulation, chi-square tests and the symmetric measures to further analyse the collected data.

3.11 Reliability and Validity

Saunders 2011, defines reliability as the ability of the repetition of previous research and still obtain similar results. Reliability can be categorised into internal and external reliability. Reliability of collected data can be influenced by one or more of the following: participant error, which can be influenced by any factor, for example, time of the day. Participant bias occurs when,

a participant provides untruthful answers, researcher bias occurs when the researcher loses objectivity (Saunders 2011).

Validity is defined as accuracy of the research results and the ability of generalisation, Saunders (2011), points out that three types of validity namely measurement validity, concerned with validity between data and construct, internal validity, relates to precise articulation of the causal relationship between the variables, and external validity, which is concerned with generalisability of the study findings.

To ensure validity, data was collected from employees in the department some of whom participate in the BYOD phenomenon while others do not. The collected data sought to answer the research questions such as the prevalence of the BYOD, management of the BYOD and information security issues around the BYOD as well as benefits for those participating. To eliminate the risk of false information being provided, the respondents to the questionnaire were given an option to only answer section A and C if they are not participating in the BYOD phenomenon.

3.12 Bias

Saunders (2011) states several areas where bias can manifest in a study. Chiefly, bias can either arise from a researcher or participant. Among others, (Saunders 2011) mentions the following types of errors that are common in research projects, the participant error, participant bias, researcher error and researcher bias.

3.12.1 Researcher bias

According to Sekaran and Bourgie (2016), a researcher's experience, knowledge and involvement in the subject being studied may influence and manipulate the outcomes of the study. In that case, the researcher may be tempted to influence the research project towards his preconceived outcomes. This can be done, among other things, by manipulating the data and or the sampling process. Saunders (2011), lists researcher error as an error on the interpretation of data to alter the essence of the participant's answer. Researcher bias occurs when the researcher is negligent in the recording of responses, this can be further exacerbated by the researcher's own experience and

knowledge on the subject. In this study, the researcher is passionate about security and information security in particular.

The researcher holds the view that information security within the Treasury and the public sector, in general, can be improved by implementing policies and obtaining management buy-in. To eliminate the researcher's biasness in this project, the sample size was the entire population, this limits the chances of only selecting the desired participants in the sample.

3.12.2 Participant bias

Participant bias can occur in two ways namely, participant error and participant bias assert (Saunders 2011). In a case of participant bias, a participant deliberately provides untruthful answers to the research questions. Participant error, can be influenced by any external factor, for example, time of the day the questionnaire was answered, the participant's state of mind at the time. To eliminate the above form of bias, the questionnaire provided for participants who do not participate in the BYOD trend only to answer section A and C, thereby reducing the chances of false reporting.

Since the questionnaire was personally administered those who were uncomfortable to participate declined the appointment and opted not to complete the questionnaire. In spite of the efforts to eliminate participant bias, participants were influenced by the researcher's position in the department and saw the survey as an investigation even though the informed consent letter was included with the questionnaire. As a result, a number of participants opted not to give their names and remained anonymous.

3.13 Ethical considerations

Ethical behaviour and secure handling of collected data as well as the information relating to respondents is critical to the researcher and the success of this study. The gate keeper's letter was obtained for the Treasury department authorising the researched to conduct research on the subject in the department attached hereto. An application for ethical clearance was submitted to the University of KwaZulu-Natal's (University) Ethics Committee and approval was granted attached

hereto. The informed consent letter was incorporated in the introduction letter informing respondents of the voluntary participation in this study. The researcher undertook to handle collected data with integrity in line with the University protocols.

3.14 Limitations of the study

The researcher opted for single data collection method whereas an interview with select employees for example within the IT department would have given an in-depth understanding of the information security risks, prevalence and management of BYOD in Treasury. Viewed as a limitation was the respondent's willingness to respond to the questionnaires where an informed consent letter required the name, respondents preferred to remain anonymous. The position held by the researcher in Treasury influenced and or intimidated potential participants from participating.

3.15 Summary

The overarching objective of this study was to investigate the effects of the BYOD phenomenon on information security within Treasury. In this chapter, a detailed discussion of the research design, the research paradigm was provided. The chapter also delved into issues of the population for the study, sample and the preferred sampling strategy. Data collection, data collection instrument of choice which is a questionnaire, instrument design was discussed, together with methods of administering the instrument to respondents and an overview of data analysis was given. Ethical considerations, as well as study limitations, were provided. The succeeding chapter dealt with the presentation of the findings and data analysis.

4. Chapter four: Presentation of results

4.1 Introduction

In this chapter, the data collected from employees in Treasury through the questionnaires are presented and discussed. The discussion makes use of descriptive statistics including graphs and

tables. The chapter presents an overall statistics report relating to participation in the survey. The demographical information is followed by an analysis and discussion of the data as it relates to the research objectives. The presentation and discussion is organised according to the research objectives. The features of the sample and the responses to the questions relating to the objectives were determined using Descriptive Statistics in the form of frequencies and percentages. Descriptive statistics are vital in assisting one to understand the characteristics, variables in the study (Sekaran and Bourgie, 2016).

4.1.1 Research Objectives

The general objective of this study is to ascertain the effects of the BYOD on information security within Treasury further, to ascertain specifically the following sub-objectives:

- To identify the prevalence of the BYOD among employees within the Treasury.
- To determine information security risks posed by the BYOD on the security of information at Treasury.
- To investigate the management of the BYOD (mobile devices) within Treasury.
- To ascertain the benefits of the use of the BYOD within Treasury.

4.1 Data analysis

Saunders (2011), describes data analysis as a systematic process of giving structure and meaning to collected data. In this process, the researchers may apply inductive and or deductive reasoning to the research project. An inference is drawn out of the collected responses. Data is presented visually in the form of tables and or charts to enable easy reference and understanding. Each table presents numerical scores as well as percentages in line with the questionnaire.

The descriptive statistical procedure entails analysis and interpretation of data using numbers and percentages (Creswell, 2011). In addition, data analysis software may be used to further interpret and analyse collected data in order to draw inferences arrive at conclusive findings. This being a quantitative study with an aim to measure the effects of the BYOD on information security the

SPSS software version 25 was used to as analyse the data. Specifically, the researcher made use of cross-tabulation and frequencies in the analysis.

The results are presented in the same order as in the questionnaire, first the demographical information about the respondents contained in Section A, this information is important for the researcher to understand the sample of the study. In this study demographical information was limited to only gender, age, number of years at work and the position at work. This information was sufficient to provide a clear profile of the respondent. Secondly, the presentation of data in the order of the research objectives as per Section B of the questionnaire and lastly Section C.

4.2. Response rate

A total of 214 questionnaires were prepared for distribution, completion and collection. The questionnaires were personally administered by the researcher to the participants. The response rate was 77%. The target was to obtain 196 completed questionnaires, however, only 166 were usable. The sample size was 450 which is the entire population in Treasury therefore with 166 usable responses there was a shortfall of 30 participants. The table below provides a numerical summary of the research project participation.

4.2 Section A: participation in the research project by demographics

The participants were asked to indicate their age group, gender, work experience and work position. The study findings are illustrated below: The command used was Frequencies.

4.3.1 Frequency: age group variable

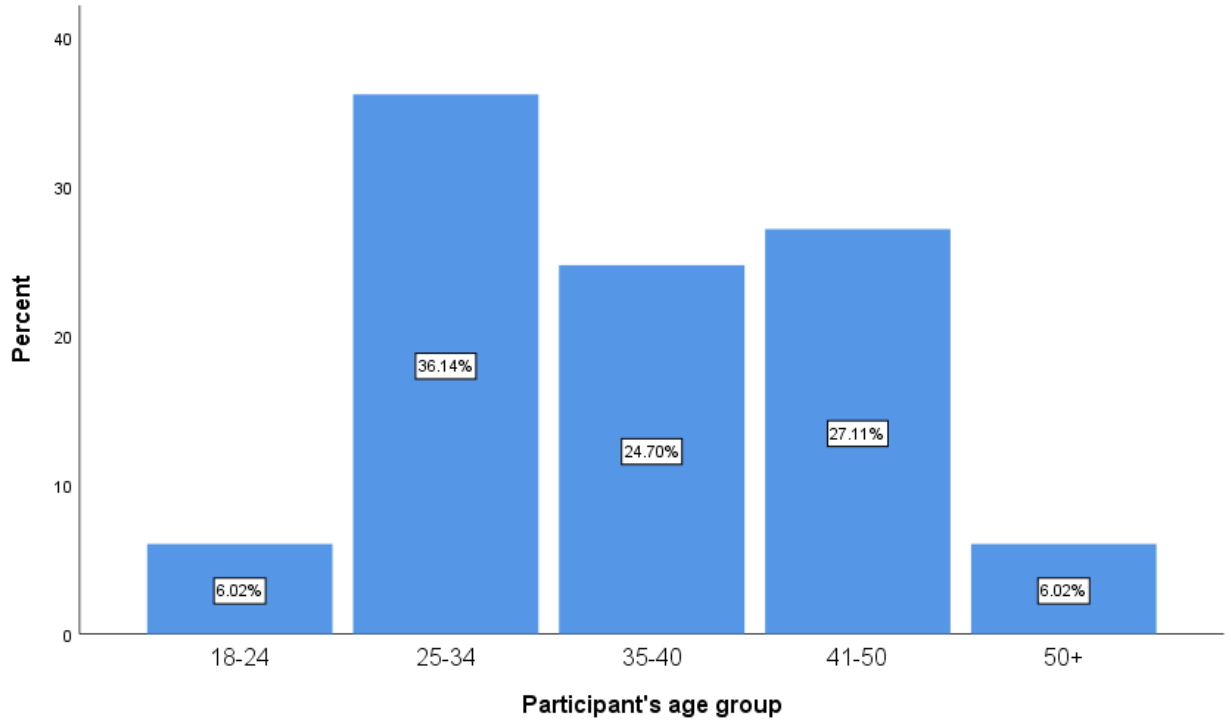

Figure 4-1 Age distribution

The above graph illustrates that the majority of participants who responded most to the questionnaires were within the 25-34 age group at (**36.1 %**). In addition, the least number of participants were in the category of 50 and above age group at (**6 %**). This finding was largely influenced by the employment statistics at Treasury.

4.3.2 Frequency: variable two gender

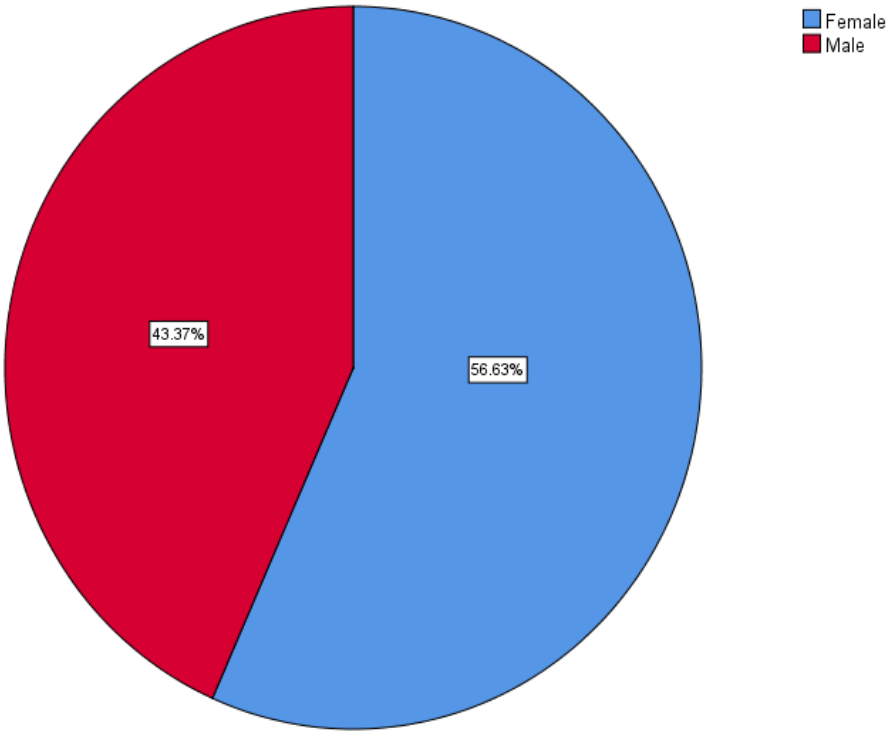

Figure 4-2 Gender Distribution

The above graph illustrates the responses to the second question which asked the participants to state their gender. According to collected data, most respondents were females at 94(**57%**) and males at 72(**43%**). This finding is largely influenced by the employment statistics at Treasury.

4.3.3 Frequency: variable three work experience

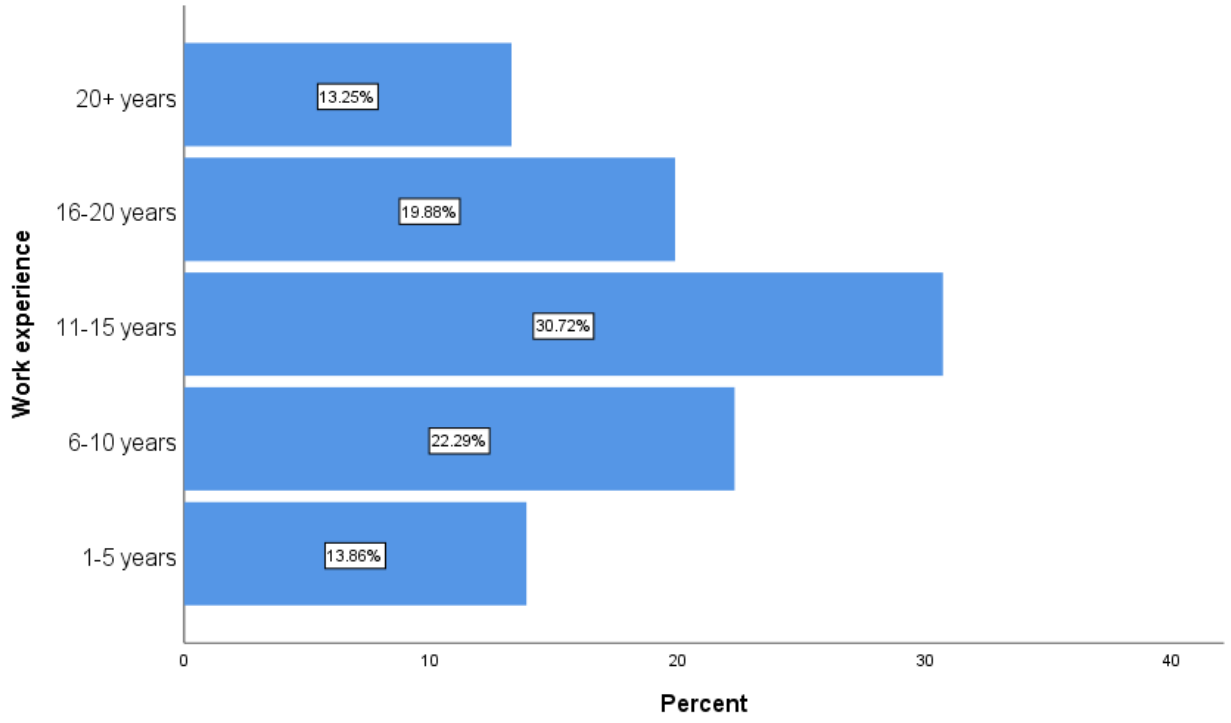

Figure 4-3 Participants according to the work experience

Figure 4.3 above, indicates that the majority of respondents 51(**31%**) have between 11 and 15 years of work experience, while the minority 22(**13%**) were between 20 years and above of work experience. An interesting outcome since the employees with longer work experience may have been exposed to both the traditional ways of corporate network reliance as well as alternatives such as the BYOD.

4.3.4 Frequency: variable four position at work

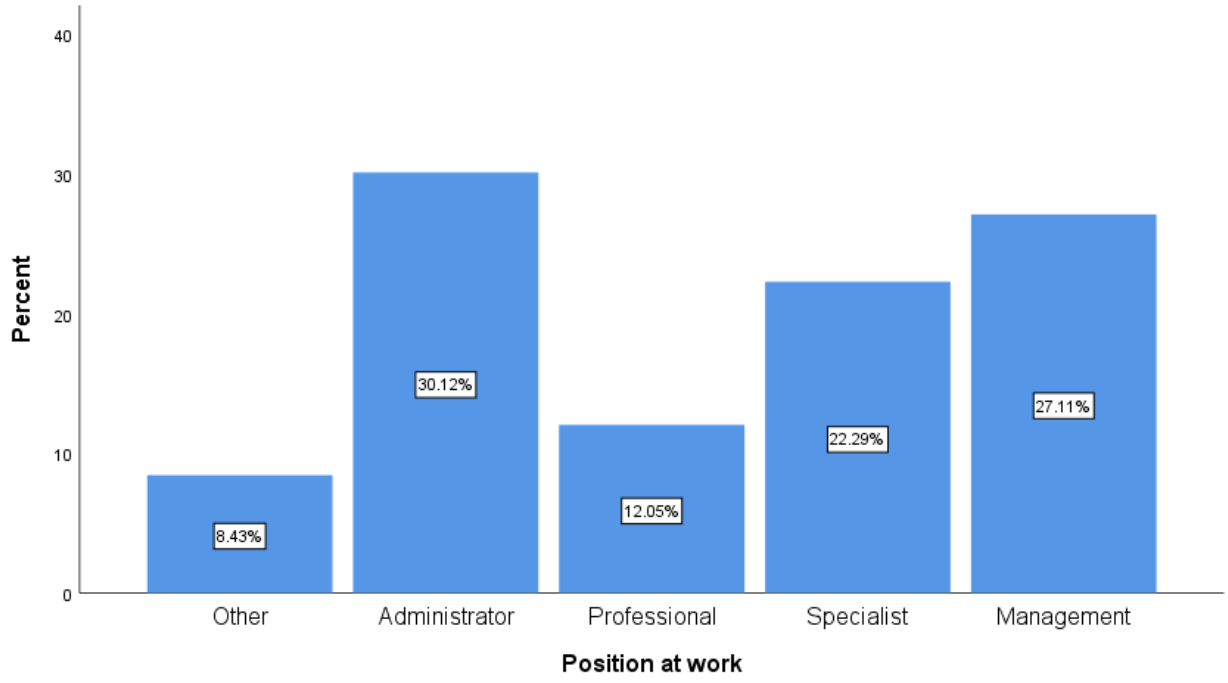

Figure 4-4Participants according to the position at work

The above graph depicts the participant's position at work, the positions are grouped and do not necessarily reflect the organisational structure but rather a function. Majority of the respondents were administrators at 50 (**30%**) and closely followed by those in the management positions at 45 (**27%**) the least were other at 14 (**8%**). The position held at work is largely associated with responsibilities and tight deadlines, how this disposition relates to the benefits of the BOYD will be fascinating.

4.4 Section B: responses according to the research objectives

The responses captured below relate to and are organised according to the objectives of the study. The tables and graphs shown below are followed by a narrative interpretation of statistical data.

4.4.1 Objective 1: prevalence of the BYOD

4.4.1.1 Frequency: Do you use your private mobile device for work purposes?

	Frequency	Percent
No	108	65.1
Yes	58	34.9
Total	166	100.0

Table 4.1 BYOD participation rate

This question sought to determine the extent of the BYOD participation in Treasury. There were 166 responses collected and a significant number of **(35%)** stated that they use their private mobile device for work purposes. The remaining 108**(65%)** were excluded from the rest of Section B since they do not participate in the BYOD.

4.4.1.2 Crosstabulation: Do you use your private mobile device for work purposes?

		No	Yes	Total
Participant's age group	18-24	10	0	10
	25-34	36	24	60
	35-40	22	19	41
	41-50	35	10	45
	50+	5	5	10

Total	108	58	166

Table 4-2 participation in the BYOD by age group

The above table depicts shows that the BYOD participation is prevalent among the age group below 40 years old at 74%.

4.4.1.3 Crosstabulation: Do you use your private mobile device for work purposes?

		No	Yes	Total
Work experience	1-5 years	21	2	23
	6-10 years	20	17	37
	11-15 years	38	13	51
	16-20 years	16	17	33
	20+ years	13	9	22
Total		108	58	166

Table 4-1participation in the BYOD by work experience

The above table depicts that the BYOD is mostly prevalent among those with work experience between 6 and 15 years at 81%.

4.4.1.4 Crosstabulation: Do you use your private mobile device for work purposes?

		No	Yes	Total
Gender	Female	63	31	94
	Male	45	27	72
Total		108	58	166

Table 4-2participation in the BYOD by gender

Gender participation in the BYOD was found to be mostly among females at 53%.

4.4.1.5 Crosstabulation: Do you use your private mobile device for work purposes?

		No	Yes	Total
Position at work	Other	11	3	14
	Administrator	42	8	50
	Professional	18	2	20
	Specialist	26	11	37
	Management	11	34	45
Total		108	58	166

Table 4-3 participation in the BYOD by the position at work

The management and specialist positions held the most participation in the BYOD at 77%.

4.4.1.2 Crosstabulation: Which mobile device do you use? (tick as many)

		Smartphone and another device	Smartphone	
Position at work	Other	1	2	3
	Administrator	1	7	8
	Professional	1	1	2
	Specialist	1	10	11
	Management	3	31	34
Total		7	51	58

Table 4 -4 choice of the mobile device per position at work

The above table reflects the results of crosstabulation analysis using **position at work** and the type of private mobile device used for work purposes as variables. The findings were that an overwhelming **31%** who are in management position use the **smartphone**. It was found that the **smartphone** is the most preferred device which is used by participants at 51(**88 %**) and there were 7(**12 %**) participants who used a **smartphone and another device**.

4.4.1.3 Crosstabulation: Which mobile device do you use? (tick as many)

		Smartphone and another device	Smartphone	Total
Participant's age group	25-34	3	21	24
	35-40	1	18	19
	41-50	3	7	10
	50+	0	5	5
Total		7	51	58

Table 4-5choice of mobile device per age group

Prevalence of the BYOD participation was observed among the age group 25 and 34 which were 21(**41%**) and participants aged 35 and 40 were 18(**35%**) depicted in the table above which is consistent with the literature. The participants aged 50 and above with smartphone usage of 5(**10%**) on the other hand were not prominently participating in the BYOD. The literature largely states that the generation Z and millennials are most likely to use technology more than other generations.

4.4.1.4 Chi- square: which mobile do you use?

			Smartphone and another device	Smartphone	Total	Chi-squared value	P-value
Position at work	Other	Count	1[a]	2[a]	3	4.421	0.352
		% within Which mobile device do you use? (tick as many)	14.3%	3.9%	5.2%		
	Administrator	Count	1[a]	7[a]	8		
		% within Which mobile device do you use? (tick as many)	14.3%	13.7%	13.8%		
	Professional	Count	1[a]	1[a]	2		

		% within Which mobile device do you use? (tick as many)	14.3%	2.0%	3.4%		
	Specialist	Count	1_a	10_a	11		
		% within Which mobile device do you use? (tick as many)	14.3%	19.6%	19.0%		
	Management	Count	3_a	31_a	34		
		% within Which mobile device do you use? (tick as many)	42.9%	60.8%	58.6%		
Total		Count	7	51	58		
		% within Which mobile device do you use? (tick as many)	100.0%	100.0%	100.0%		

Table 4 -**Error! No text of specified style in document.**-6Which mobile do you use per position at work

A chi-square analysis was done for the question which mobile device do you use using the variable position at work and the findings were that each subscript letter denotes a subset of Which mobile device do you use? (tick as many) categories whose column proportions do not differ significantly from each other at the .05 level.

4.4.2 Objective 2: information security risks posed by BYOD

4.4.2.1 Crosstabulation and chi square test: Have you ever lost a private mobile device?

			No	Yes	Total	Chi-squared value	P-value
Participant's age group	25-34	Count	17_a	7_a	24	20.582a	.000
		% within Have you ever lost a private mobile device?	45.9%	33.3%	41.4%		
	35-40	Count	5_a	14_b	19		
		% within Have you ever lost a private mobile device?	13.5%	66.7%	32.8%		

	41-50	Count	10_a	0_b	10		
		% within Have you ever lost a private mobile device?	27.0%	0.0%	17.2%		
	50+	Count	5_a	0_a	5		
		% within Have you ever lost a private mobile device?	13.5%	0.0%	8.6%		
Total		Count	37	21	58		
		% within Have you ever lost a private mobile device?	100.0%	100.0%	100.0%		

Table 4-7 have you ever lost a mobile device per age group

The above table presents a chi- square analysis of have you ever lost a mobile device using age group variable and found that each subscript letter denotes a subset of the question have you ever lost a private mobile device categories whose column proportions do not differ significantly from each other at the .05 level.

4.4.2.2 Crosstabulation and chi- square test have you ever lost a private mobile device?

			No	Yes	Total	Chi-squared value	P-value
Gender	Female	Count	20_a	11_a	31	.015	.902
		% within Have you ever lost a private mobile device?	54.1%	52.4%	53.4%		
	Male	Count	17_a	10_a	27		

		% within Have you ever lost a private mobile device?	45.9%	47.6%	46.6%		
Total		Count	37	21	58		
		% within Have you ever lost a private mobile device?	100.0%	100.0%	100.0%		

Table 4- 8 gender distribution have you ever lost a private mobile device

The above table presents a chi- square analysis of have you ever lost a mobile device using age group variable and found that each subscript letter denotes a subset of have you ever lost a private mobile device categories whose column proportions do not differ significantly from each other at the .05 level.

4.4.2.3 Crosstabulation and chi-square: Have you ever lost a private mobile device?

			No	Yes	Total	Chi squared test	P value
Position at work	Other	Count	0_a	3_b	3	17.738	.001
		% within Have you ever lost a private mobile device?	0.0%	14.3%	5.2%		
	Administrator	Count	8_a	0_b	8		
		% within Have you ever lost a private mobile device?	21.6%	0.0%	13.8%		
	Professional	Count	1_a	1_a	2		
		% within Have you ever lost a private mobile device?	2.7%	4.8%	3.4%		
	Specialist	Count	3_a	8_b	11		
		% within Have you ever lost a private mobile device?	8.1%	38.1%	19.0%		
	Management	Count	25_a	9_a	34		
		% within Have you ever lost a private mobile device?	67.6%	42.9%	58.6%		
Total		Count	37	21	58		
		% within Have you ever lost a private mobile device?	100.0%	100.0%	100.0%		

Table 4-9 have you ever lost your mobile device per position at work

The above table presents a chi- square analysis of have you ever lost a mobile device using age group variable and found that, each subscript letter denotes a subset of have you ever lost a private mobile device categories whose column proportions do not differ significantly from each other at the .05 level.

4.4.2.4 Crosstabulation and chi square test have you ever lost a mobile device?

			No	Yes	Total	Chi-squared value	P-value
Work experience	1-5 years	Count	1_a	1_a	2	20.582	.000
		% within Have you ever lost a private mobile device?	2.7%	4.8%	3.4%		
	6-10 years	Count	11_a	6_a	17		
		% within Have you ever lost a private mobile device?	29.7%	28.6%	29.3%		
	11-15 years	Count	7_a	6_a	13		
		% within Have you ever lost a private mobile device?	18.9%	28.6%	22.4%		
	16-20 years	Count	9_a	8_a	17		
		% within Have you ever lost a private mobile device?	24.3%	38.1%	29.3%		
	20+ years	Count	9_a	0_b	9		
		% within Have you ever lost a private mobile device?	24.3%	0.0%	15.5%		
Total		Count	37	21	58		
		% within Have you ever lost a private mobile device?	100.0%	100.0%	100.0%		

Table 4-12 work experience have ever lost a mobile device

The above table presents a chi- square analysis of have you ever lost a mobile device using age group variable and found that Each subscript letter denotes a subset of have you ever lost a private

mobile device? categories whose column proportions do not differ significantly from each other at the .05 level.

4.4.2.5 Crosstabulation: Were you advised by the IT department how to protect data on your BYOD device?

		No	Yes	Total
Gender	Female	27	4	31
	Male	25	2	27
Total		52	6	58

Table 4 -10 Knowledge of data protection per gender

The crosstabulation analysis above recorded the responses of the participants participated in the study, the majority participants 52(**90%**) were not aware of how to protect their data on their BYOD devices compared to 6(**10%**) who were aware. This finding is concerning given that literature states that both users and the employer have the responsibility to protect and preserve the CIA of information.

4.4.2.6 Crosstabulation: Were you advised by IT department how to protect data on your BYOD device?

		No	Yes	Total
Participant's age group	25-34	23	1	24
	35-40	14	5	19
	41-50	10	0	10
	50+	5	0	5
Total		52	6	58

Table 4-11 Advice on data protection by age group

Crosstabulation of the data to the question were you advised by IT department how to protect data on your BYOD device, showing that only 10% was advised.

4.4.2.7 Crosstabulation: I store work information on my private mobile device.

		Always	Often	Sometimes	Rarely	
Gender	Female	7	10	7	7	31
	Male	8	8	3	8	27
Total		(26%)15	(31%) 18	(17%)10	(26%)15	(100%) 58

Table 4 -12: Storage of data on the device per gender

The crosstabulation recorded the responses of the participants and the findings were that there were 15 (**26%**) who always use their mobile devices to store work information followed closely by 18 (**31%**) who often use their devices to store work information. These are significant numbers which show that Treasury information may be exposed to information security risks due to the user's lack of knowledge on how to secure information.

4.4.2.8 Crosstabulation: Do you update your operating system and install new patches?

		Always	When available	Never	Auto update	
Gender	Female	4	19	2	6	31
	Male	7	15	0	5	27
Total		11	34	2	11	58

Table 4-13: Updating of operating system per gender

34(**59%**) mentioned that they only update their operating system when available and 11(19%) always and auto-update their operating systems and conscious of updating their security system compared to 2(**3%**), a large number of participants 34(**59%**) assumed that their devices are updated when available the security module.

4.4.2.9 Crosstabulation: Security module on my private BYO device was approved by IT department.

		No	Yes	
Gender	Female	23	8	31
	Male	12	15	27
Total		35	23	58

Table 4-14: IT's approval of the security module per gender

Participants who used BYOD devices 35(**60%**) were not conscious about the security of their device or information while 33(**57%**) stated that they always and often store work information on their devices.

4.4.2.10 Crosstabulation: How often do you use your private mobile device for work purposes? I store work information on my private mobile device. Do you download Applications and or games onto your private mobile device that you use for work purposes?

Do you download Applications and or games onto your private mobile device that you use for work purposes?		I store work information on my private mobile device.				Total
		Always	Often	Sometimes	Rarely	
How often do you use your private mobile device for work purposes?	Rarely	0	0	0	1	1
	Sometimes	1	8	3	6	18
	Often	7	9	7	4	27
	Always	5	1	0	2	8
Total		13	18	10	13	54
How often do you use your private mobile device for work purposes?	Often	1				1
	Always	1				1
Total		2				2
	Rarely	0	0	0	1	1
	Sometimes	1	8	3	6	18

How often do you use your private mobile device for work purposes?	Often	8	9	7	4	28
	Always	6	1	0	2	9
Total		15	18	10	13	56

Table 4-15 Pivot table how often do you use your private mobile device

The table depicts that most users use their mobile devices often and often store work information on their devices also download mobile apps and games often.

4.4.3 Objective 3: management of the BYOD within Treasury

4.4.3.1 Crosstabulation: Are you aware of the departmental policy regarding the use of private mobile devices for work purposes?

		No	Yes	
Gender	Female	30	1	31
	Male	21	6	27
Total		51	7	58

Table 4 -16: Awareness of policy provisions per gender

The crosstabulation above recorded the responses by the participants, 51 (**88%**) participants mentioned that they were not aware of the departmental policy regarding the use of private mobile devices for work policies compared to 7(**12%**) who are knowledgeable about the policy.

4.4.3.2 Crosstabulation: Were you advised by IT department how to protect data on your BYOD device?

		No	Yes	
Gender	Female	27	4	31
	Male	25	2	27
Total		52	6	58

Table 4-17: Advice on data protection by IT department

The crosstabulation above indicated that the majority of participants 52 (**90%**) were not advice by IT on the security module in their device compared to the 6 (**10%**) who were advised.

4.4.3.3 Crosstabulation: Do you download applications (Apps) and or games onto your private mobile device that you use for work purposes?

		Yes	2	
Gender	Female	28	1	29
	Male	26	1	27
Total		54	2	56

Table 4 -18: Downloading of applications and games per gender

The crosstabulation above showed that the majority of participants 54(**94%**) downloads applications and games on their mobile devices that they use for work purposes.

4.4.3.4 Crosstabulation: If answered yes to question 11 above, how often do you download Applications and or games?

		Always	Occasionally	Rarely	Never	Total
Gender	Female	6	22	1	2	31
	Male	4	17	3	3	27
Total		10	39	4	5	58

Table 4-19: Frequency of downloading apps and games

The majority of participants 39(**67%**) occasionally downloads applications and/or games using their private mobile. 10(**17%**) always downloads applications and/or games and 5(**9%**) never use private mobile devices to downloads applications and/or games.

4.4.4 Objective 4: Benefits of BYOD

4.4.4.1 Crosstabulation: Since using your private mobile device for work purposes, have your productivity improved?

		Strongly disagree	Agree	Strongly agree	
Gender	Female	7	8	16	31
	Male	1	11	15	27
Total		8	19	31	58

Table 4-20: Productivity since using own mobile device by gender

An increase in productivity measured per gender found that 53% strongly agreed that their productivity has increased since using their own devices for work purposes.

4.4.4.2 Crosstabulation: Since using your private mobile device for work purposes, have your productivity improved?

		Strongly disagree	Agree	Strongly agree	
Position at work	Other	0	0	3	3
	Administrator	3	0	5	8
	Professional	0	2	0	2
	Specialist	0	7	4	11
	Management	5	10	19	34
Total		8	19	31	58

Table 4-21 Productivity since using own mobile device by position at work

Those in management position strongly agreed that their productivity has increased since using their own devices for work purposes

4.4.4.3 Crosstabulation: Keeping up with deadlines is a lot easier when I use my private device

		Strongly disagree	Disagree	Agree	Strongly agree	
Gender	Female	4	0	19	8	31
	Male	6	10	1	10	27
Total		10	10	20	18	58

Table 4-23 Keeping up with deadlines since using own mobile device

Those who used private mobile devices 50(**86%**) often stated that they see much improvement in their production, 38(**66%**) also agreed that by using private mobile devices are keeping up with deadlines.

4.4.4.4 Chi-Square test: Since using your private mobile device has your production increased?

	Value	Df	Asymptotic Significance (2-sided)
Pearson Chi-Square	4.753[a]	2	.093
Likelihood Ratio	5.294	2	.071
Linear-by-Linear Association	2.419	1	.120
N of Valid Cases	58		

a. 2 cells (33.3%) have expected count less than 5. The minimum expected count is 3.72.

Table 4-24 increase in productivity since using own private device

The chi-square test measures the discrepancy between the observed cell counts and what you would expect if the rows and columns were unrelated. The two-sided asymptotic significance of the chi-square statistic is greater than **0.10**, so it's safe to say that the differences are due to chance variation, which implies that more participants who often used mobile devices see much improvement in their production.

4.4.4.5 Symmetric Measures

		Value	Approximate Significance
Nominal by Nominal	Phi	.286	.093
	Cramer's V	.286	.093
N of Valid Cases		58	

Table 4-22 Symmetric Measures

The significance values of all two measures are **.286** for Phi and Cramer's V, indicating a statistically significant relationship. However, the values of all the two measures are under **0.3**, so although the relationship is not due to chance, it is also not very strong.

4.5 Presentation of section C of the questionnaire

In the era of the fourth industrial revolution, participants were asked if they considered BYOD a threat or an opportunity for the organisation.

4.5.1 Crosstabulation: Is BYOD a threat to information security?

		No	Yes	Total
Gender	Female	10	21	31
	Male	5	23	28
Total		15	44	59

Table 4-23 Gender distribution: Is the BYOD a threat to information security?

An overwhelming 44(**75%**) of participants considered the BYOD to be a threat compared to the 15 (**25 %**) who considered it not to be a threat.

4.5.2 Crosstabulation: Does BYOD provide an opportunity for innovativeness at work?

		No	Yes	Total
Gender	Female	7	87	94
	Male	6	66	72
Total		13	153	166

Table 4-24: Gender distribution: Does BYOD provide an opportunity for innovativeness at work?

Equally an overwhelming (**92%**) of participants considered the BYOD an opportunity for innovativeness at work.

4.6 Summary

The data shown above only captures the responses to section A of the questionnaire, which is the biographical data. This data is critical in the analysis of the responses relating to the user's participation in the BYOD phenomenon. A number of variables will be looked at when analysing the data such as how age, position, influence the adoption of the BYOD. The choice of device used as well as how often these are used for work purposes will assist in determining the existence of mobile workers. A discussion of the findings in relation to the literature will be presented in the succeeding chapter.

5 Chapter five: Discussion of the results

5.1 Introduction

This chapter provides a discussion of the research findings. The findings reflected in chapter four are discussed. The discussion hinges on the research objectives, research questions and findings of the study as presented in the previous chapter. Relevant literature inclusive of studies captured in chapter two of the study inclusive of the theory underpinning the study will be used to compare the research findings and draw significant inferences and conclusion. Further, determine whether the research questions were answered or not. The research objectives are captured in the chapter below which is followed the discussion of findings. The discussion is organised in the order of the research objectives.

5.2 Presentation of demographical findings

The demographical data collected included the gender, age, position at work and work experience. Majority of the participants were at 57%. The finding confirms, among other things, the employment statistic at Treasury. By age distribution, it was found that most respondents were in the age group under 40 years at 67% and the remainder were above 40 years of age. Using the variable work experience, it was found that 66% of the respondents had between 1 and 15 years of work experience. The last variable in this section was position at work, the findings were that the majority of the respondents were in the Administrator position at 30% followed closely by those in a Management position at 27%.

5.3 Research objectives

The purpose of this study is to investigate the effects of the BYOD phenomenon on information security within Treasury. In order to address the purpose, the following research objectives were designed:

- To identify the prevalence of the BYOD among employees within Treasury.
- To determine information security risks posed by the BYOD on the security of information at Treasury.
- To investigate the management of the BYOD (mobile devices) within Treasury.
- To ascertain the benefits of the use of the BYOD within Treasury

5.3.1 Prevalence of the BYOD among employees

This objective was designed to answer the question relating to the extent of the BYOD participation in Treasury. A significant number of participants stated that they use their private mobile device for work purposes. Interestingly, the BYOD phenomenon was found to be prevalent specifically among the age group below 40 years old. Khakurel et al. (2018), found that older users were not keen on new technology and exploring new work strategies, similarly, this study found that an overwhelming majority of those who participate in the BYOD were below the 40-year age grouping.

Various studies reviewed in this project supports the view that the BYOD phenomenon is prevalent in organisations. The findings of this study are consistent with the literature, Dingwayo and Kabande (2017), also found that majority of South African employees participate in the BYOD even though only 5% of organisations had formally adopted the BYOD, Treasury was no exception. Use of private mobile devices was found mostly among participants who are below 40 years of age was also in line with the argument that the younger generation embraces technology (Steelman and Sabhewal, 2016). The variable position at work was tested to ascertain prevalence of the BYOD, an overwhelming number of those in management level followed closely by the specialists often participates in the BYOD. These findings are congruent with the study by Mphahlele (2016) as well as Ubene et. al, (2018), these studies found, among other things, that the younger workforce and those in management position often participate in the BYOD because of

the interest in the newer technology and the managers are interested in keeping and meeting their deadlines.

Das and Khan (2016) found that most BYOD participants preferred using the smartphone in the completion of their work tasks and other applications. Whereas the study by Mphahlele (2016) found that employees mostly used the tablet in the BYOD participation. In this study, it was found that most users at management level preferred to use the smartphone that most users prefer the smartphone over other devices. This may be a result of the dematerialisation of the smartphone (Rainer et al.2015). Users prefer to carry and use one mobile device for most applications.

5.3.2 Information security risks posed by the BYOD

This objective was designed to answer the question what are the risks posed by the BYOD phenomenon on information security. Kebande (2017) points out that while BYOD may present benefits and opportunities for organisations, it also poses a plethora of risks particularly the information security risks as well and privacy of personal information. Therefore, organisations implementing the BYOD strategy must have proper management tools in place to mitigate the risks. On the one hand, Vorakulpipat et al. (2017) list the loss of mobile devices, outdated operating software, security of mobile devices susceptibility of mobile devices to viruses and malware as well as the security of information stored on the device as leading information security risks related to the implementation of the BYOD. On the other hand, organisations, as well as the users, have the responsibility to preserve confidentiality, integrity and availability of information.

The BYOD participants admitted to storing work information on their mobile device often. In concurrence with Vorakulpipat et al (2017), a significant number of participants who participated in the BYOD have lost their mobile devices, differently stated there is a 22% chance of unauthorised access, theft and modification of information stored on the lost private mobile device. Further, it can be inferred that Treasury may not be fulfilling the confidentiality, integrity and availability requirements in relation to security of information. Whereas there is no formal implementation of the BYOD and policies guiding sharing and storage of proprietary information in Treasury, at least a third of participants in this study stored work information on their private

mobile device often. Consequently, information stored on the private mobile device is at risk of unauthorised access, theft and destruction to name a few (Steelman and Sabhewal,2016).

Bello Garba et al. (2015), argue that the presence of different application (Apps) may lead to exfiltration of data among apps which is further exacerbated by the lack of adequate security measures to protect proprietary information on the device. In view of the foregoing submission, participants were asked if the download apps onto their BYO devices and an overwhelming 96% answered yes to the question. The fact that participants downloaded free apps and games that may harbour malware and viruses presents a threat to the CIA of information (Parker 2015).

In congruence with Bello Garba (2015), Dingra (2016) submits that security of information on the BYOD device ranked among the highest concerns for organisations in implementing the BYOD strategy since threats such as network intrusion and eavesdropping have steadily increased in the recent past. Downloading of apps and or games often requires the user to accept terms and conditions of the developer or administrator, these terms are only accessible via a given website whether or not users actually read and understand these terms in relation to access to information and storage protocols was not tested. However, it is common cause that certain apps require access to the device's location, camera microphone to name a few, as such users may not be aware of who and when and what was accessed using the installed apps and or games. Vorakulpipat et.al (2017) further emphasise that these (apps and games) are areas of information security risks since the user does not control how the app administrator uses the permissions granted. This renders the mobile device vulnerable to risks such as unauthorised access to information and use of uses information for commercial use to name a few.

User behaviour is another critical element in the security of information, (Carcaray et al. 2016) this was measured by asking the participants if they update the operating system on their BYOD devices, 58% said they updated only when the updates were available. As pointed out by Bello Garba (2015), the lax attitude towards securing the devices as well as information therein exposes Treasury to information security risks such as viruses. Only a marginal percentage of participants made a concerted effort to ensure that their devices operating system is updated.

5.3.3 Management of the BYOD in Treasury

This objective was designed to answer the question how is the BYOD (mobile devices) managed in Treasury? Fani et al. (2016) brand the BYOD strategy as an institutionalised information security risk. At the time of the study only 13 % of the participants had knowledge of the policy relating to the use of private mobile devices, by contrast a large number agreed to using their private mobile devices for work and storing work information. Therefore, the risk of Treasury's information being compromised is high. Clear policies on the selection, management, security of information and access to the BYOD device are critical in mitigating the risks posed by the BYOD (Steelman and Sabherwal, 2016). Further, there is an ongoing confusion regarding the users as well as organisation's roles and responsibilities as far as information control, ownership and security are a concern submits (Dhingra, 2016).

However, a survey by Gartner in 2015 found that only 30% of companies have approved BYOD policies, 50% of the companies do not stipulate the expected level of security for the device (Rice et al. 2016). Management of the BYOD includes both technical and administrative tools. The literature recommends, among other things, the Mobile Device Management software which is installed on the private device and allow the employer to remotely access the device. There are a number of concerns relating the MDM primarily, being privacy. However, in order to achieve information security and the convenience of using one's own device an agreement must be reached (Dingra (2016).

5.3.4 Benefits of the BYOD

This objective was designed to answer the question what are the benefits of the BYOD phenomenon within Treasury? The literature relating to the benefits of the BYOD is vast, some of the organisational benefits include savings on capital infrastructure expenditure (Disterer, et al. 2013). Participants agreed that it's a lot easier to do work even outside the office, as well as keeping up with deadlines when using their personal mobile device. These findings supported the argument by proponents of the BYOD that it allowed the employee to be independent and better manage their workload and this, in turn, has a positive outcome for the employer. In congruence, (Arregui et al., 2016) argue in favour of the BYOD that organisations benefit from saving on capital expenditure on equipment because employees simple use their own devices. However, the benefits

must be viewed in the light of information security risks associated with the implementation of the BYOD. Similarly, various studies have found that employee benefits include convenience, motivation and innovativeness to name a few (Seth, 2017).

An improvement in production levels since using the BYOD was tested and an overwhelming majority 86% agreed that since using their own devices productivity levels have increased. Similarly, Seth (2017) found that implementation of the BYOD strategy resulted in an increase in productivity. Participants were asked if their participation in the BYOD was for convenience or not, a resounding 68% agreed with the statement. The literature states that one of the reasons for users to prefer using their own devices is convenience, in this study an overwhelming 68% agreed with the literature. This finding was an indication that there exist a need for implementation of the BYOD in Treasury, such implementation holds benefits for both users and Treasury (Mphahlele, 2016).

5.4 Is the BYOD a threat or an opportunity for Treasury?

In addition to the objective related questions, all participants were asked whether the BYOD is a threat or an opportunity for the department. 86% stated that the BYOD is a threat to information security interestingly, the age group below 34 were the highest. This finding supports the view by that the BYOD is an institutional risk that ought to be managed *inter alia* through clearly defined policies (Fani et al. 2016). The BYOD was found to be presenting an opportunity for innovativeness since almost all respondents agreed with the statement. This finding is synonymous with the submission by Mphahlele (2016) that users can be a lot more creative when using their own devices with the technology and applications they are familiar with compared to the highly regulated and monitored corporate equipment. The BYOD strategy is not compulsory but enabler in view of benefits that he organisation may derive from its implementation.

5.5 Summary

It is common cause that the BYOD presents both threats and opportunities for organisations, however, the findings in this study indicate the need for implementation of the BYOD. It is also important to balance both the interests of the organisation mainly the CIA of information and the

wellbeing of staff as well as those of the users mainly, convenience. In this chapter, the findings in the preceding chapter were discussed. A synthesis of the findings with the studies and the literature was presented. The research questions were answered as well a discussion in relation to the theory underpinning the study was offered. The following chapter presents the conclusion and recommendations

6 Chapter six: Conclusions and recommendation

6.1 Introduction

This is the final chapter of the dissertation, where the conclusions, implications of the study are discussed and the limitations encountered during this project are also elaborated upon. This project was set out to study a problem that relates to the use of the BYOD and its implication on information security, as such, the recommendations to solve the research problem are provided and discussed. A number of other areas that were not covered in this study, therefore, suggestions of areas for future research are provided in order to enhance the knowledge on the subject.

6.2 Conclusions

The focus of the study was the KwaZulu-Natal Provincial Treasury department. The overarching objective of the study was to ascertain the effects of the BYOD phenomenon on information security within Treasury. Sub-objectives were formulated as follows: to identify the prevalence of the BYOD among employees within Treasury, to determine information security risks posed by the BYOD on the security of information at Treasury, to investigate the management of the BYOD (mobile devices) within Treasury and to ascertain the benefits of the use of the BYOD within Treasury.

The research problem was centred on the threats posed by the BYOD on the security of information within Treasury. The study adopted a positivist research paradigm and followed quantitative research methods. Data were collected using a questionnaire which was self-administered by the researcher to all participants, the population was the entire staff in Treasury, and the sample size was 167 staff members. The research conclusions are organised in line with the research objectives.

In relation to the prevalence of the BYOD, this objective aimed to measure the prevalence of the BYOD in Treasury. Given the risks associated with the BYOD and the responsibility to maintain confidentiality, integrity and availability (CIA) of information, Treasury has a task of balancing the maintenance of the CIA as well as the rapid adoption of the BYOD. It is without a doubt that the BYOD phenomenon is prevalent in Treasury, even though at the time of this study the BYOD was not formally adopted, however, a total of **74%** of employees who participated admitted to

participating in the BYOD phenomenon. This finding only makes a strong case for a formal adoption and implementation of the BYOD in Treasury to enable employees to enjoy the full benefits of the BYOD participation. It was found that most participants in the study are younger than 40 years of age, according to various studies the younger workforce preferred using their devices for work purposes.

Concerning objective two which was to determine information security risks posed by the BYOD on the security of information at Treasury. Information relates to all information including emails and photos. A number of information security risks posed by the BYOD were identified. Majority of the participants admitted to storing work information on their private mobile device. The CIA of information can be compromised through loss of the device which was found to be at 22%, downloading of apps and games which was at 96% and the laxity relating to updating operating software was at 62%. Loss of information and unauthorised access to information are among information security risks that were highlighted in the literature review. Even though the actual loss of information and or attempted hacking of the corporate network were not tested, the above numbers mean that Treasury's information on the BYO devices has a 33% chance of being stored in unsecured devices.

BYOD management is largely done through the implementation of policies, raising awareness about employee's responsibilities and roles as far as information security is concerned. Majority of the participants admitted that they do not know the policy provision that relates to safeguarding information. This lack of knowledge could be attributed to inadequate communication of policy or that there is no specific policy that provides guidance on the implementation of the BYOD.

It was important to ascertain the benefits of the BYOD usage within Treasury. It was found that those who use their own devices for work purposes have realised an increase in productivity at 86%, ease of meeting deadlines was found to be at 66% and convenience was found to be at 68%. Even though there are indications that there was an improvement in the productivity of those who participate in the BYOD, actual benefits derived by Treasury from the BYOD participation were not measured in this study.

6.3 Implications of this research

This study contributed to an understanding of the BYOD phenomenon, the information security risks that come with it and the possible benefits of the BYOD. The motivation of the study was to contribute to the development of a policy framework for the implementation of the BYOD within the public sector in particular. This study contributed to the body of knowledge by providing a public sector perspective on the BYOD phenomenon. Treasury benefitted by gaining an in-depth understanding of the phenomenon and its risks to the security of information and possible benefits. This insight is crucial for the development of a policy framework and implementation strategy. Recommendations provided in the succeeding paragraph are practical and the implementation thereof will result in a successful BYOD strategy for Treasury.

6.4 Limitations of study

The number of participants the study targeted 196 participants, however, only 166 participated and the responses were useful to the study. The limitation may be attributed to the researcher's position at Treasury. Potential participants were uncertain if the study was a purely academic exercise or a compliance inspection on their information security behaviours. To overcome this limitation the researcher provided documentation relating to the academic research and ethical clearance, most respondents agreed to participate in the study.

The minimum understanding of the BYOD concept, some participants had a very limited understanding of the BYOD concept. This resulted in delays where the researcher had to explain the concept first before the participant can answer the questions. The fact that the questionnaires were personally administered assisted the researches to explain the concept and minimise errors in the answering thereof.

The timeframe of questionnaire administration, the researcher only had three weeks administer the questionnaire and collect the required data. This challenge was a result of the late receipt of approval from the University Ethics Office. The researcher used meeting platforms and approached participants even during lunch breaks to collect the data.

At the time the research was conducted, Treasury had not officially or formally implemented the BYOD. This may have contributed to the lack of understanding of the concept. The researcher took the time to explain the concept to ensure that participants understood before answering the questions.

6.5 Recommendations to solve the problem

Data collected from Treasury indicated that the BYOD phenomenon exists, users are benefitting from its use and therefore, the department must decide to take control of the manifestation of the BYOD or risk chasing after it and doing damage control. Given the findings in this study, elements of mobility can be incorporated while still maintaining a clear responsibility and ownership of information contained therein, mitigation of information security risks through implementation of both technical and administrative tools. Recommendations are organised into administrative and technical

6.5.1 Administrative recommendations

- The fact that employees are able to store work information without any knowledge on how to safeguard the same is indicative of a lack of information security culture at an organisational level. The culture of understanding that information is a strategic resource that requires protection from threats and risks, must be developed and inculcated among Treasury staff. Developing and inculcating an organisational culture requires top management's will, supported by organisational policies.

- The BYOD strategy inclusive of guiding policies, implementation and management plans, as well as monitoring and evaluation, are key to a successful BYOD programme. This requires, *inter alia,* development of a policy setting out clear roles and responsibilities, information that can be accessed and stored on the private device, management of the private mobile device and protocol in case of loss of the device.

- User behaviour determines whether the BYOD strategy is a success or a failure. Training and creating awareness on threats and risks as well as individual role and responsibilities of information security. Employees ought to understand the values of organisational information and their role in its protection.

6.5.2 Technical recommendation

Implementation of technical measures aimed at securing organisational information irrespective of its medium. In the implementation of the BYOD software such as MDM and MAM provide the necessary governance of the devices even though they do not prevent the manifestation of threats. Implementation of intrusion detection software, anti-virus and other security software is essential to safeguard the organisational network as well as information against attacks. However, Treasury must guard against the temptation of overprotection which may result in poor adoption of the BYOD.

6.6 Recommendations for Future Studies

A number of limitations were encountered in this study which future studies can address. Recommendations are listed hereunder.

- Sample size, the current study only targeted 196 participants in one department, future researchers can increase the sample and the study site to include other departments in order to provide a provincial government perspective.
- In this study, only quantitative methods were used, however, given that the BYOD is not well understood elements of qualitative methods such as interviews with IT managers will add value.
- Actual benefits to the company were not ascertained this study only offers benefits enjoyed by users. In the future, it will be important to actually determine if the implementation of the BYOD yields any benefit for the organisation.
- Actual cases of compromised information were not measured. Future researches may need to ascertain if there are actual cases of loss of information of compromise to the corporate network that can be attributed to the BYOD.

6.7 Summary

It is without a doubt that the public sector, in particular, can no longer afford to turn a blind eye on the proliferation of mobile devices, the fast pace at which technology and cloud computing is growing. The researchers aim was to ascertain the effects of the BYOD on information security within Treasury. It was found that the BYOD has an effect of the security of information at Treasury.

6.8 References

AGARWAL, A. & AGARWAL, A. 2011. The security risks associated with cloud computing. *International Journal of Computer Applications in Engineering Sciences,* 1**,** 257-259.

AGENCY, N. I. 1996. Minimum Information Security Standards.Government Information systems, Pretoria.

ALMARHABI, K., JAMBI1, K., EASSA1, F. & BATARFI1, A. O. 2017. Survey on Access Control and Management Issues in Cloud and BYOD Environments. *International Journal of Computer Science and Mobile Computing,* 6**,** 44-54.

ALSALEH, M., ALOMAR, N. & ALARIFI, A. 2017. Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods. *PloS one,* 12**,** e0173284.

ANDERSON, C., BASKERVILLE, R. L. & KAUL, M. 2017. Information Security Control Theory: Achieving a Sustainable Reconciliation Between Sharing and Protecting the Privacy of Information. *Journal of Management Information Systems,* 34**,** 1082-1112.

ARREGUI, D. A., MAYNARD, S. B. & AND ATIF, A. 2016. Mitigating BYOD Information Security Risks. Woolongong. University of Melbourne.

BABBIE, E. & MOUTON, J. 2009. *The practice of social science,* South Africa, Oxford University Press.

BALOZIAN, P. & LEIDNER, D. 2017. The Assumptions and Profiles Behind IT Security Behavior. Hawaii. CC-BY-NC-ND.

BELLO GARBA, A., ARMAREGO, J. & MURRAY, D. 2015. Bring your own device organizational information security and privacy. *ARPN Journal of Engineering and Applied Sciences,* 10**,** 1279-1287.

BRADLEY, J., LOUCKS, J., MACAULAY, J., MEDCALF, R. & BUCKALEW, L. 2012. BYOD: A global perspective, harnessing employee-led innovation. *Cisco.“http://www. cisco. com/c/dam/en_us/about/ac79/docs/re/BYOD_Horizons-Global. pdf*.

CARCARY, M., RENAUD, K., MCLAUGHLIN, S. & O'BRIEN, C. 2016. A Framework for Information Security Governance and Management. *IT Professional,* 18**,** 22-30.

CHO, D.-J. 2016. A Study on Prospect and Security Technology of Big Data. *International Information Institute (Tokyo). Information,* 19**,** 605-614.

CRESWELL, J. W. 2014. *A concise introduction to mixed methods research*, Sage Publications.

DAS, A. & KHAN, H. U. 2016. Security behaviors of smartphone users. *Information & Computer Security,* 24**,** 116-134.

DHINGRA, M. 2016. Legal Issues in Secure Implementation of Bring Your Own Device (BYOD). *Procedia Computer Science***,** 179-184.

DINGWAYO, M. & KABANDA, S. 2017. Bring Your Own Device (Byod) And Information Privacy Compliance In South African Organizations.

DISTERER, G. & KLEINER, C. 2013. BYOD bring your own device. *Procedia Technology,* 9**,** 43-53.

FANI, N., VON SOLMS, R. & GERBER, M. A . 2016. Framework towards governing "Bring Your Own Device in SMMEs". Information Security for South Africa (ISSA), IEEE, 1-8.

GAO, X. & ZHONG, W. 2016. A differential game approach to security investment and information sharing in a competitive environment. *IIE Transactions,* 48**,** 511-526.

GARTENER. 2013 . STAMFORD.

HEMDI, M. & DETERS, R. 2016. Data Management in Mobile Enterprise Applications. *Procedia Computer Science,* 94**,** 418-423.

KEBANDE, V. R., KARIE, N. M. & VENTER, H. A . 2016. Generic Digital Forensic Readiness model for BYOD using honeypot technology. IST-Africa Week Conference, IEEE, 1-12.

KRAUSS, L. 1980. *Security Audit and Field Evaluationfor Computer Facilities and Information Systems,* New York, Amacom.

LI, P. & YANG, L. 2017. Management strategies of Bring Your Own Device. MATEC Web of Conferences,EDP Sciences, 02007.

MVELASE, P., DLAMINI, Z., MACLEOD, D., DLODLO, N. & SITHOLE, H. A .2014. Business model for a South African government public cloud platform. IST-Africa Conference Proceedings, 2014, IEEE, 1-10.

NWEKE, L. O. 2017. Using the CIA and AAA Models to Explain Cybersecurity Activities.

OLALERE, M., ABDULLAH, M. T., MAHMOD, R. & ABDULLAH, A. 2015. A review of bring your own device on security issues. *Sage Open,* 5**,** 2158244015580372.

PARKER, B. D. 2015. *Computer Security Handbook*, John Wiley & Sons, Inc.

PERAKOVIĆ, D., HUSNJAK, S., MIŠIĆ, V. & KULJANIĆ, T., MIJO. 2016. Employee's awareness on security aspects of use bring your own device paradigm in Republic of Croatia. Croatia. RCITD.

RAINER, R. K., PRINCE, B. & WATSON, H. J. 2015. *Management Information Systems,* Canada, Wiley.

RICE, A. L. 2016. Best Practices for Secure BYOD Implementations.

ROY, A. A. K., A. 2012. MANAGEMENT OF INFORMATION SECURITY IN SUPPLY CHAINS - A PROCESS FRAMEWORK. CApe Town. CIE & SAIIE.

SAUNDERS, M. N. 2011. *Research methods for business students, 5/e*, Pearson Education India.

SEKARAN, U. & BOUGIE, R. 2016. *Research methods for business: A skill building approach*, John Wiley & Sons.

STEELMAN, Z. R. & SABHERWAL, M. L. A. R. 2016. Charting Your Organization's Bring-YourOwn-Device Voyage. | *MIS Quarterly Executive 85,* 15**,** 85-104.

UBENE, O.-I. E., AGIM, U. R. & UMO-ODIONG, A. 2018. The Impact Of Bring Your Own Device (Byod) On Information Technology (It) Security And Infrastructure In The Nigerian Insurance Sector. *American Journal of Engineering Research,* 7**,** 237-246.

VORAKULPIPAT, C., SIRAPAISAN, S., RATTANALERDNUSORN, E. & SAVANGSUK, V. 2017. A policy-based framework for preserving confidentiality in BYOD environments: A review of information security perspectives. *Security and Communication Networks,* 2017.

WIID, J. & DIGGINES, C. 2010. *Marketing Research,* Cape Town, Juta Academic.

WU, H. & WANG, X. 2016. ISBP: Understanding the Security Rule of Users' Information-Sharing Behaviors in Partnership. *PloS one,* 11**,** e0151002.