Business Priorities Driving BYOD and the Resulting Consequences: A South African Case Study

A dissertation presented to the

Department of Information Systems

University of Cape Town

By

Steve Gavin Miller

(MLLSTE028)

in partial fulfilment of the requirements for

Master of Commerce in Information Systems degree

INF5005W

Declaration

1. I know that plagiarism is wrong. Plagiarism is to use another's work and pretend that it is one's own.

2. I have used the APA convention for citation and referencing. Each contribution to, and quotation in, this essay "Business Priorities Driving BYOD and the Resulting Consequences: A South African Case Study" from the work(s) of other people has been attributed, and has been cited and referenced.

3. This essay is my own work.

4. I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as his or her own work.

5. I acknowledge that copying someone else's assignment or essay, or part of it, is wrong, and declare that this is my own work.

Signed by candidate

Signature Removed

Steve Gavin Miller Date: 04 March 2016

MLLSTE028

Dedication

This dissertation is dedicated to my loving wife Liezel Miller.

Acknowledgements

I would like to thank everyone who supported me during my studies but I would particularly like to thank the following people, without their support the completion of this thesis would not be possible:

I firstly would like to thank God for giving me the strength and ability to complete this study. Nothing is possible without his grace.

Secondly I would like to thank my supervisor Dr Jacques Ophoff for all his advice, guidance, support and patience throughout this whole process. You have made this experience very enriching. Thank you for allowing me the opportunity to work with you.

Thereafter I am thankful to the organisation that granted me permission to conduct this study in their environment.

I wish to express my gratitude to all the participants of this study that gave their valuable time during the interviews. I appreciate your input.

Furthermore I wish to thank my parents Gavin and Cheryl Miller for their belief in me and their continuous encouragement and pushing me to complete this thesis. Dad your positive attitude and determination is an example to us all.

To my sister Shannen Miller thanks for your loving support. Your work ethic is infectious.

Finally thanks goes to my wife Liezel Miller. Your constant support, motivation and patience is greatly appreciated. When I needed the nudge to keep going I could always count on you.

Abstract

The consumerisation of information technology (IT) introduced the bring your own device (BYOD) phenomenon into the enterprise environment. As mobile and Internet technologies improve employees are opting to use their personal devices to access organisational systems in order to perform their work tasks. Such devices include smart phones, tablets and laptop computers. BYOD provides opportunities for both the organisation and employees, but the adoption of BYOD also introduces risks to the organisation. Mobility and management of BYOD and CYOD (choose your own device) has consistently been a top concern for business management and Chief Information Officers (CIO's) globally.

In the current, challenging economic environment organisations need to use all their resources, including technology, effectively. Organisations that develop an effective BYOD program can use this to assist in achieving their organisational objectives. This study uses a case study approach to investigate how business priorities drive the adoption of BYOD and how BYOD benefits and risks are realised by the organisation. Primary empirical data was collected using semi-structured interviews with employees from a large financial services organisation. Policy documents from the organisation was analysed as secondary data. Thematic analysis of the data revealed six major themes: improving employee mobility; improving client service and experience; creating a competitive industry advantage; improving business processes; information security risks; and management best practises. The themes were combined into a conceptual model, showing the decision process in adopting a BYOD program.

This research contributes to the body of knowledge in this area, focusing on the South African context. The conceptual model can serve as an example for organisations currently making BYOD adoption decisions or organisations that are not achieving the full benefits of their BYOD program. The conceptual model reveals that organisations can use BYOD to achieve benefits including having a mobile workforce which results in an increase in productivity. However, mobility introduces risk to the organisation where information security risks is the top concern. This study recommends using a combination

of technical and human controls to manage the risks. The technical controls include the use of an enterprise mobility management system and password controls. The human controls include the creation of effective BYOD and information security policies that the employees understand and follow. Providing employees with information security awareness and training is essential.

List of acronyms

BYOD	Bring Your Own Device
CAQDAS	Computer Assisted/Aided Qualitative Data Analysis Software
CYOD	Choose Your Own Device
EMM	Enterprise Mobility Management
ERP	Enterprise Resource Planning
ISC	Information Security Culture
IT	Information Technology
MAM	Mobile Application Management
MDM	Mobile Device Management
MIM	Mobile Information Management
POPI	Protection of Personal Information
SLA	Service Level Agreement
SMS	Short Message Service

Table of Contents

1. Introduction

In recent years sales of smart phones and tablets have increased exponentially and sales of desktop computers have diminished as consumers have been opting for mobile devices (Gartner, 2013). One of the reasons for this increase in mobile device adoption is the ability these devices have for connecting the consumer to their information networks and the accessibility to the user's data irrespective of the location. 3G and 4G data services are enabling consumers to communicate with their networks and process data for business needs from any location. One phenomenon that emerged with the advent of smart phones and tablets is Bring Your Own Device (BYOD) which enables users to use their own mobile device in the business as well as the personal environment. Zielinski (2012) described BYOD as the concept where individuals were not reliant on company sponsored devices but chose to purchase and use their own mobile devices to connect and process organisational information. Gartner (2013a) defined BYOD as "the strategy that allows employees, business partners and other users to use a personally selected and purchased client device to execute enterprise applications and access data" (para. 3). BYOD was spurred on by the consumerisation of IT where consumer devices made their way into the corporate world (Gartner, 2012b).

The reasons mobile devices have become popular are the connectivity options now available which include cellular and wireless networks. Many organisations allow their employees' to connect to their wireless networks to access resources and stay connected in meetings and presentations etc. (Gartner, 2013). The variety of applications for business and personal use allows the mobile device owner to use the device for multiple functions. The advancement of these multifunctional mobile devices include increased processing power that allows users to complete functions they previously were only able to undertake on their desktop computers (Couture, 2010).

Although there are many benefits associated with BYOD there are also risks that need to be mitigated. In a global survey by Forrest Research, which included 10,000 professionals from 17 countries, more than half of those information workers use their

personal mobile devices in the organisational environment (King, 2012). Takesue (2007) and Ernst and Young (2011) both agree that BYOD devices are used by employees within the enterprise without understanding the risks that these devices introduce to the businesses information and infrastructure. Chen and Nath (2011) highlighted the risks that personal mobile devices introduce to the corporate network. If these devices are lost, stolen or the organisation does not have the appropriate security controls in place the sensitive business data stored on the device will put the business at risk. These compromised devices could be used to gain unauthorised entry into the organisations network through exploitation of a direct connection. Loss of sensitive data leaves businesses vulnerable to financial losses, reputational damage and losing their competitive advantage (The Ponemon Institute, 2012).

1.1 Research Problem

In the current global economic climate businesses are faced with recession, globalization, uncertainty of consumer behaviour and market trends therefore businesses need to utilize every possible advantage to remain competitive and maximize revenue for their stakeholders. Businesses have been using technology as one of the key strategic components to improve productivity, internal communication, marketing of their goods and services and customer service (Couldwell, 2011). Technology has also provided businesses with the systems to create innovative solutions for their clients (Weiß & Leimeister, 2012). Businesses have come to realise that BYOD provides benefits that include increased employee productivity, work flexibility and the cost reduction for IT (Wood, 2012).

In the past corporate information was stored within the organisational perimeter secured by firewalls and at a fixed location. In the digital age that businesses now operate in information is processed and sent to staff members and clients globally. This sensitive information is processed and resides on personally owned mobile devices of employees that have chosen to have more flexible working tools (i.e. BYOD). The risk is that

organisations have little control over BYOD in terms of where these devices move and the potential loss of the data stored on them.

Rich research and data is available on the many risks that BYOD introduce for organisations from a security perspective. Cisco IBSG (2013) stated that findings from the study of 2,400 mobile users across 18 countries in various industries reported that security was still their businesses main concern. Although the literature provides details of security management controls to address these concerns limited research has been conducted on the effectiveness and usability of the available solutions.

Organisations that do not understand the business objectives that drive BYOD adoption will not be able to effectively identify the appropriate requirements to build the BYOD program. These organisations will not be able to clearly justify the costs associated with the implementation of the BYOD program as well as the changes to business processes. Therefore organisations that invest in understanding the BYOD objectives would be in a better position to realise the organisations goals. Proper planning and management of the BYOD program would lead to limiting not only the costs of implementation, but also the security risks associated with the utilisation of this facility.

1.2 Research Objective and Questions

The objective of this research is to understand and examine the adoption of BYOD within a South African context. To achieve this objective the study is guided by the following primary research question: *How do business priorities drive the adoption of BYOD in the organisation?*

To answer the primary question the following secondary question is posed: *How are the benefits, risks and costs of implementing and managing a BYOD program realised by the organisation?*

This will assist organisations that are considering adopting a BYOD strategy and the organisations that already have a BYOD program in place but are not achieving optimal results.

1.3 Importance of this Study

As the popularity of BYOD increased so has the number of research publications on this topic (Brodin, Rose & Ahlfeldt, 2015). Although BYOD is not a new research area it is still relevant to the academic and business worlds. The challenges that BYOD introduces is currently a major concern for businesses and has consistently appeared as a top business priority over the past few years (Gartner, 2015).

The majority of the BYOD research covered strategic analysis which comprised of the expectations of BYOD and its capabilities (Brodin, 2015). A smaller portion of prior research covered strategy design, while very little is found in the area of implementation and evaluation of BYOD (Brodin, Rose & Ahlfeldt, 2015). A focus on North America and Europe dominates the number of studies and articles published and much less were found for Africa, especially in the South African context. This research will compare the results of BYOD studies in northern hemisphere to understand if similar benefits and dangers are experienced in South Africa especially within the financial industry at the Insurance organisation where the researcher is employed. This research filled the existing gap in literature on BYOD with the current situation within an organisation.

Another gap that exists in the research was that the majority of the studies conducted were based on security although BYOD introduces some other important concerns for organisations. Pieterse (2014) states that the other issues business are facing in regards to BYOD are compatibility, complexity and support issues. Investigating these issues further and providing solutions to how organisations are dealing with these problems can benefit other organisations with their BYOD implementation of management.

The findings of this study can provide practitioners who are in the process of deciding whether to implement a BYOD program at their organisation with valuable information. This study also assists organisations that have already implemented their BYOD program but are not gaining the full benefit thereof by providing guidance on how to limit the risks.

1.4 Structure of Dissertation

This remainder of this dissertation is structured as follows. Chapter 2 provides a literature review as theoretical basis for enterprise mobility and the BYOD concept. It highlights the importance of the trend and how it can benefit organisations as well as employees. The risks and operational concerns of BYOD are then identified and the controls to effectively deal with BYOD risks are covered. In Chapter 3 the research methodology is discussed including the researcher's philosophical assumptions, how the data will be collection and analysed. Ethical considerations and other aspects of the research is also covered in this chapter. The findings are presented, analysed and discussed in Chapter 4. Lastly conclusions are drawn in Chapter 5, along with the limitations of the study and future research opportunities.

2 Literature Review

This chapter begins by looking at the consumerization of IT and how this has influenced the corporate environment. Next, the importance of enterprise mobility in the modern organisation is emphasized. BYOD is defined and an overview of the key concepts are presented. Thereafter, the benefits and risks associated with BYOD are presented. The management of BYOD is discussed next and finally a summary of the literature review is provided.

2.1 Consumerization of IT

A concept closely related to BYOD, that is usually used in the mobile arena is, consumerization of IT. This concept refers to consumer devices, which are privately owned but also used for business functions (Gartner, 2012a). Harley (2013) defined consumerization of IT "as the use of technology that is supplied by non tech individuals" (para. 3). Even though this concept has been discussed over the past years it is still very relevant today, especially as a practice. This is highlighted by Gartner (2012b) that lists consumerization of IT within the top five major trends in information systems.

Moschella, Neal, Opperman, and Taylor (2004) viewed consumerization of IT as redefining the relationship between the employee and the organisation. Employees often feel frustrated with issues related to traditional infrastructure in the organisation. However with consumerization of IT employees can experience IT in an enjoyable and efficient manner by also selecting a device with hardware and software specifications that meets their criteria (Baskerville, 2011; Weiß & Leimeister, 2012). This is in contrast to the traditional infrastructure called Choose Your Own Device (CYOD) where employees had to accept the desktop computers and laptop provided by the company. The differences between CYOD and BYOD are shown in Table 1 below. These differences include ownership, user satisfaction, integration into business systems, etc. The two models have

their pros and cons and the suitability of the chosen model depends on the user or the organisations requirements. The table highlights that CYOD is owned and managed by the organisation making these devices easy to control. BYOD on the other hand, has the employees owning their devices, this means that the organisation has reduced control of the device and hence there is increased risk for the organisation.

Table 1. Difference between BYOD and CYOD

	BYOD	**CYOD**
Ownership	Individual	Organisation
User satisfaction	Very good – chosen by owner	Limited
Mobile data plan	Usually for users account	Sponsored by organisation
Integration into business systems	Due to complexity of different devices integration is limited	Systems often built with certain mobile platforms in mind.
Support	Complex due to different brands	Controlled and easier maintenance.
Device types	Any device	Devices chosen from preapproved list.
Applications	User's choice	User needs to follow organisation's policy.
Remediation for lost or stolen devices	Depends on agreement with user. Normally only business data is wiped	All data on mobile device is wiped.
Management of device	Difficult	Easier

In the next section enterprise mobility is defined and its importance is discussed.

2.2 Enterprise mobility

Ghoda (2009) has defined enterprise mobility as the ability for organisations to operate in both the traditional business sense based on fixed location and the new virtualized business where the location is irrelevant. Enterprise mobility allows employees to access organisational information, collaborate on projects with different teams and process information via wireless networks, broadband and satellite connections and services. Disabato (2015) has stated that enterprise mobility does not only relate to the technology within the organisation but how technology is incorporated into the business strategy and business processes. According to Disabato (2015), enterprise mobility must be used to generate new business opportunities, improve client relationships and extend business processes to cater for mobile functionality.

Basole (2007) has stated that enterprise mobility is the product of consumerization of mobile device technology within the organisation and will change how business is conducted. Configuring the mobile technology within an organisation does not mean that it is a mobile organisation but determines how the organisation operates.

The Gartner 2012 CIO survey has revealed that organisational mobile work became one of the CIO's main focus areas and that they planned to invest in mobile technologies within the coming year (Gartner, 2012a). According to a later survey of 2800 CIO's, mobile was listed in the top five investment priorities for 2015 (Gartner, 2015). Research by Forrester (2012) has confirmed that mobile was the "new face of engagement". Mobile applications using mobile devices and corporate networks are creating new opportunities for businesses. Accenture predicts organisations will develop mobile applications for general business activities and enterprise applications that interact and provide data from internal information systems. The availability of information from mobile devices leads reduced dependence on working from permanent locations for users, and allows them to operate freely wherever they are. Typical mobile activities include accessing business emails and calendars, managing documentation and accessing customer relationship management (CRM) systems and accessing intranet portals. Mobility cannot be achieved by infrastructure alone but organisations have to establish strategies to provide for access

to the various internal systems that will allow employees to complete their daily tasks (Unhelkar & Murugesan, 2010).

Current studies confirm that information and communication technology (ICT) advancements in the mobile space have opened new possibilities that can improve business processes and deliver more business value (Kornak, Teutloff, & Welin-Berger, 2004). Even though the benefits of mobile ICT are available not all organisations have adopted this strategy due to the risks that include security, privacy and other technology issues. To minimize the risks and maximize the benefits of mobile ICT for an organisation that wants to transform into a mobile enterprise, an evaluation of the organisations readiness must be completed (Hartman & Sifonis, 2000; Ward & Peppard, 2002). In order to illustrate the key issues Basole and Rouse (2007) have proposed the dimensions of the mobile enterprise illustrated in Figure 1. They have proposed that mobile enterprises demonstrate greater levels of adaptability, access and interaction than those traditional enterprises that have not adopted mobile strategy and business practices. Typically traditional businesses are operating in the inner circle in the diagram but mobile enterprise are represented in the outer circle.

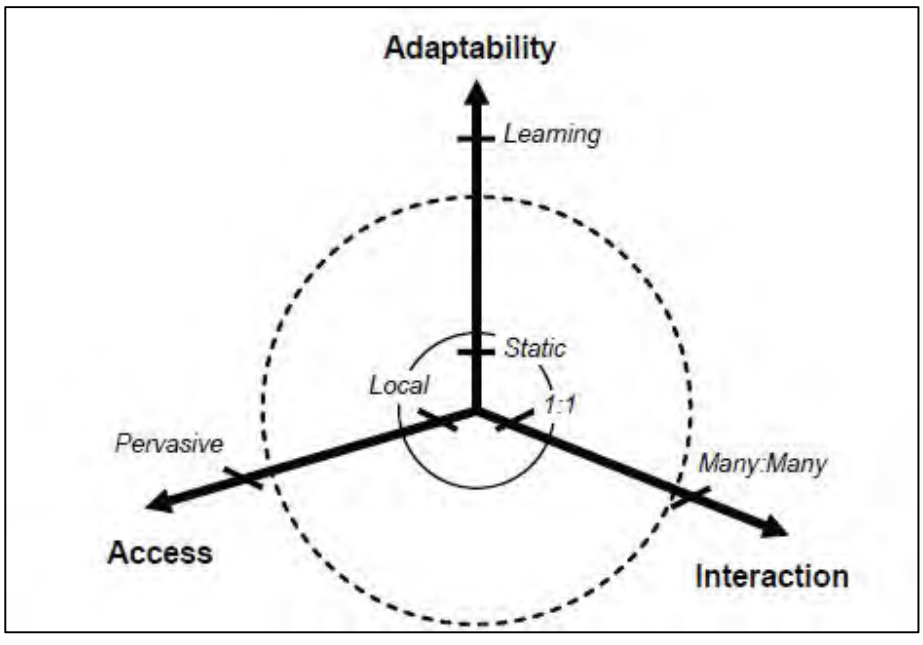

Figure 1. The Dimensions of the mobile enterprise (Basole & Rouse, 2007)

Basole and Rouse (2007) have recommended that an organisation that wants to convert their business into a mobile enterprise can follow the transformation stages below:

1. Mobilization – includes mobilization of information and software systems to enable mobile workers to access this information via their mobile devices irrespective of time and place of the mobile worker.
2. Enhancement – this stage involves creating new business processes more suited to mobile strategy.
3. Reshapement – while transitioning to this stage mobile ICT starts reforming organisation processes and strategies. The new business processes enabled by mobility provide the organisation with a means of competitive advantage.
4. Redefinition – this is the final stage of the transformation process where the benefits of Mobile ICT are realised.

The new organisation competencies and strategies which are built around mobility can pave the way for the organisation to access different markets and industries.

2.3 Benefits of BYOD

Many organisations adopt a BYOD strategy for the perceived benefits that this will bring the organisation and its employees. Liljander and Strandvik (1992) have defined Perceived Benefits as the benefits the consumers perceive they will receive. In the context of BYOD, perceived benefits reflect the overall benefits employees and organisations expect this technology will provide. Lee (2008) states that the two types of perceived benefits are direct and indirect benefits. With BYOD programs direct benefits are tangible and immediately available. BYOD's direct benefits include cost savings to the organisations and increased productivity (Calder, 2013). Indirect benefits are less tangible and include employee satisfaction and using BYOD programs to attract new employees (Dell and Intel, 2011). The benefits associated with BYOD are discussed in more detail below.

2.3.1 Employee Satisfaction

In market research that has been conducted among the stake holders of organisations, nearly 60% of the respondents indicated that job satisfaction among their staff was a factor in adopting the BYOD strategy (Citrix, 2011). A study by Dell and Intel (2011) has highlighted that for every ten employees surveyed six reported they enjoyed their working experience more if they were using the technology of their choice. This was found to be particularly true for the younger generation of employees who have grown up with technology and are generally more tech savvy than their older colleagues. The motivation of the organisations employees is strongly linked to the success of the business, since high employee morale results in improved productivity. The study has noted that organisations that have a BYOD policy are more attractive to potential new employees, who are tech-savvy, than those that do not (Dell and Intel, 2011).

2.3.2 Employee productivity and accessibility of data

One of the benefits that the BYOD concept provides to a business is that it allows corporate data to be readily available, via laptops, smartphones and tablets, to those employees who are travelling outside of the office. The accessibility of the corporate data by the employees allows businesses to provide better services to their clients (Calder, 2013). Research by Forrester (2011) claims that 80% of respondents stated that BYOD had translated into an increase in the productivity of the business employees. This claim has been backed up by an earlier study of IT users that use laptop computers, which discovered that these users were, on average, 50 minutes more productive, on a usual day, than those users that had desktop computers (Calder, 2013). Employees have indicated that being able to select their own mobile device and the technology that suits their individual requirements has enabled them to be more efficient. The increase in productivity has been due to the device, the operating system installed on it together with other mobile applications, and cloud services available on this device.

A global study by Cisco IBSG (2013) has found that respondents accomplish increased productivity on their own mobile devices and that employees are willing to spend their own income to obtain these mobile devices. On average each employee spent $900 on the device of their choice. Secondary costs of operating these mobile devices are data and voice costs, on which each employee, on average, spent $700. The prices of the mobile usage plans vary between countries and go as high as $1200 in the United States of America compared to some plans of as little as $400 in India.

The figure 2 below indicates the reasons for BYOD device choice of respondents of the Cisco IBSG (2013). The BYOD device types most frequently used by the respondents were smartphones. The study has confirmed that employee's that use BYOD are more comfortable using their own devices than those provided by their employer, and that this situation improves the accomplishment of their works tasks. They use their devices for both personal and business purposes.

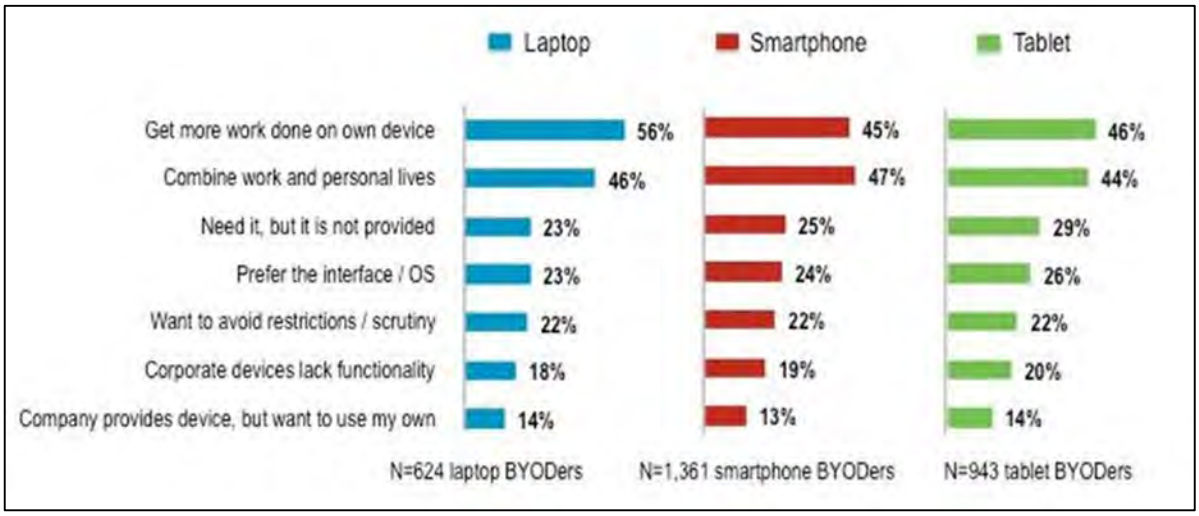

Figure 2. Mobile device preferences (Cisco IBSG, 2013)

2.3.3 Cost Savings for the organisation

In a business that decides to follow the BYOD trend the employee purchases the mobile device themselves which translates into significant savings for the organisation in regards to procurement and training (Wood, 2012). Wood (2012) states that many organisations

list cost savings as their number one reason for adopting a BYOD strategy. The annual cost of upgrading existing technology and purchasing new equipment for an organisation is significant, and saving costs is vital for businesses to operate in this global economy. When employees provide their own tools, these costs are for their own account. Having paid for a device themselves employees are more likely to take better care of these devices than the company issued assets. Support costs that would be borne by businesses are further reduced when employees support their own devices. Rains (2012) has highlighted a research study conducted by the HDI Research Corner that examined 844 organisations in 35 industries. This study has reported that 40% of these organisations required employees that had their own devices to contact the vendors themselves to resolve support issues with their devices. 30% of organisations in the study reported having the business supply internal support for BYOD devices at the cost of the business. Some BYOD decision makers in organisations in the US and Europe disagreed with this cost savings benefit as noted in a survey conducted by Forrester Consulting. The results of the survey have shown that even though organisations saved on the costs of the devices and support thereof, costs of security and compliance for BYOD increased (SC Magazine, 2012).

The risks associated with mobile devices are increasing, therefore organisations need to ensure that their data, as well as the privacy of their employee's data, are well secured. In the next section the importance of information security will be discussed.

2.4 Risks associated with BYOD

In the current information age organisations rely heavily on their information systems to operate successfully. Organisations need to manage the risks that accompany these connected systems and networks. A risk can be defined as the possibility that a threat could exploit a vulnerability and thus cause damage to the organisation (Whitman & Mattord, 2004). Many organisations globally have rated information security as one of the highest management priorities (Lohmeyer, McCrory, & Pogreb, 2002; Ransbotham &

Mitra, 2009). Information Security is the process of protecting information and ensuring that only authorized users (confidentiality) have access to accurate and complete information (integrity) when needed (availability) (ISACA, 2008). The three components are often referred to as the CIA triad (Whitman & Mattord, 2004). Confidentiality ensures that only the authorised users have access to the information. Integrity is the characteristic that is accurate, trustworthy information that has not been tampered with or modified unknowingly. Availability is having the information ready for the authorised users when required. Information security is vital when employees use their personal mobile devices to connect to their organisation's network infrastructure that contains confidential corporate information. All three components of the CIA Triad are immensely important in regards to the BYOD concept and mobility. Organisations' that have, or are considering implementing, a BYOD strategy need to have a solid information security program in place. This program must be geared to combat internal and external threats. The mobile devices that are owned by employees often have sensitive business information stored on them which is a risk to the organisation.

With the use of BYOD there also comes a certain level of risk. Bauer (1967) has introduced perceived risk in the perceived risk theory which analysed how individuals consider the risks associated with their actions and the consequences thereof. Cunningham (1967) stated that the theory assumes the perceptions of risks have a bearing on an individual's intention to complete an action. Stone and Gronhaug (1993, p.42) define perceived risk as a "subjective expectation of a possible loss". Perceived Risk Theory could be used as a basis to explain the consumer behaviour in adopting BYOD and their actions using the mobile devices when faced with decisions that could impact the privacy of their data and the security of the organisations systems, network and data. Perceived risk has been a major factor in how users intended to use IT systems (Featherman & Pavlou, 2003; Liu, Yang, Li, 2012)

Six types of perceived risks have been noted: financial, privacy, performance, social, physical and time-loss (Jacoby & Kaplan, 1972; Kaplan, Szybille ,George, Jacoby, 1974; Roselius, 1971). Featherman and Palvou (2003) state that the dimensions of perceived

risk may differ for product or service. Several risks that the BYOD concept has introduced into organisations are discussed next.

2.4.1 Data Loss

Calder (2012) states that one of the main risks of BYOD is the loss of confidential data that has been stored on the mobile devices. The results of the Cisco IBSG (2013) study that surveyed more than two and a half thousand mobile users across six countries also supported this finding. Cisco IBSG (2013) results show that security is the biggest challenge for business and employees. The loss of the mobile device presents a criminal with an opportunity to exploit the organisation's confidential information. This situation creates a severe security risk for the organisation. When devices are not configured with the basic security measures, such as locking the device with a strong pin, requiring a password to enter the device, encryption of the sensitive data, then it is easy for the criminal to gain access to this information. Gartner (2013b) reports that in 2013 almost 2.4 billion tablets and smartphones were sold, making these devices attractive to thieves because of the size and value of these items. For improved mobility and ease of use, the size of these devices is usually compact, making them prone to be lost or stolen.

Mcafee (2012) highlights an alarming fact from a study in the UK. He reports that sensitive data is usually passed on to unauthorised users when employees upgrade, change or sell the mobile devices without following the proper disposal procedures which includes wiping the device first. Besides sensitive data that is lost when the device is no longer with the owner, very often the time that the device goes missing is crucial. This can be because of deadlines etc. The owner cannot afford the time that it takes to recreate the data, since this could lead to the business losing its competitive advantage. More often than not this is vital information which is either not backed up or will take some time to be regenerated to its former state. Another issue with data loss is data leakage where the affected user is not aware that data is being misused and the user cannot minimize risk until it is too late. The Ponemon Institute (2012) reports that on average it costs an

organisation 7.2 million US dollars per data breach and on average 214 US dollars per compromised record. Organisations need to ensure that their internal controls are effective at protecting the sensitive information of their clients. Failing to safeguard this data could have the organisation suffering financial losses, legal action and, depending on the severity of the breach, this could cause reputational damage to the business. This in turn could affect their ability to be competitive and conduct business in the future.

2.4.2 Malware

Malware which is short for malicious software is a piece of software code that infects computer systems, causes disruption to the services, gathers sensitive information without permission and causes damage to the device (Moir, 2009). Malware allows criminals to steal sensitive information from computers, like password and credit card information. In some severe cases malware can infect computer systems and mobile devices allowing hackers to control these devices and systems. Tzoumas (2013) explains that malware and viruses are usually accidentally downloaded to the mobile devices. These viruses can cause havoc when they spread onto the company networks. These malicious programs can easily find and open back door entry points to servers and databases allowing hackers to steal organisational data. This usually goes unnoticed before it is too late. As more businesses adopt the BYOD concept, the malware that affects mobile devices has also increasingly been targeting tablets and smartphone software (Drew, 2012; Kaspersky, 2012; Ponemon Institute LLC, 2012). Traditional security measures which organisations usually provide such as firewalls and antivirus software are no longer effective at preventing malicious infections from entering the organisation with mobile devices (Ponemon Institute LLC, 2012). Users who connect to the internet on their mobile devices outside the organisation are at constant risk of being exposed to web threats. The Cisco (2013) survey highlighted that 69% of BYOD users had applications on their devices that were unapproved and dangerous. If the appropriate control measures are not put in place by organisations the corporate sensitive data on

their computer systems and on the BYOD devices could be at risk to malware attacks which could have a negative impact on the business.

2.4.3 BYOD Device Misconfiguration

Unlike the traditional desktop computers that are situated on the premises of the organisation and managed by the in house IT department, BYOD devices are owned and managed by their users. This allows the owner of the device to configure the device to their own preferences, which could leave the device vulnerable to attack. The danger being that all mobile users will not have the knowledge required to secure their devices configuration settings appropriately. Landman (2010) is of the opinion that a significant number of security incidents in the organisation stem from BYOD devices that not configured correctly with the appropriate security controls. Some employees that may not be aware of the BYOD and Information Security policies, or that deliberately violate the policies, can cause significant risks for the organisation (Landman, 2010). Gartner published similar findings that stated up to 75% of mobile security breaches were the result of BYOD misconfiguration (Gartner, 2014).

2.4.4 Software Vulnerabilities

Whitman and Mattord (2004) define vulnerability from an information security viewpoint as an identified flaw within a system that can be exploited. The IT department does not have full control with BYOD making it difficult to monitor and control these devices. As the sales of smartphones and tablets are increasing cyber criminals are targeting these devices and exploiting vulnerability in the software installed and downloaded to them. Malicious applications are downloaded by employees who are often unaware of the dangers such software creates to the information stored on the device. The vulnerabilities allow viruses and malware into the device, which increases the chance of data leakage

and data loss. Compared to desktop software, mobile device software is relatively new and still in its infancy compared. In order to alleviate some of the known priority security issues the top vulnerabilities need to be patched to prevent exploitation by criminals.

2.4.5 Bluetooth and Wireless Connectivity Weaknesses

The ease of connectivity to the World Wide Web, organisational systems and social networks is one of the reasons that mobile devices have become so popular. These devices that depend on the cellular network offer impressive internet connection speeds via 3/4G network technology. These devices offer Wireless connectivity to access work resources at the office or at home, and the devices have Bluetooth connectivity for data sharing and to enable connections to various other devices. Anderson (2013) stated it could be possible for unauthorised users to gain access to organisation data if they are tethered to an authorised device connected to the company network. The Bluetooth and Wireless technology that these devices have built in has been known to be exploited, without difficulty in order to infect the mobile devices with malware or intercept sensitive data being transmitted (IBM, 2011). When BYOD users are connected to unsecured networks the data transferred by the device is susceptible to 'man in the middle' attacks, where the hacker is able to intercept the data being communicated.

When the Bluetooth option is set to discoverable on a mobile device, criminals are able to scan for vulnerable devices, and once connected to the device they are able to access stored personal information (Cisco, 2013). BYOD users who access these Bluetooth and Wireless technology networks should be aware of the dangers that exist when connecting to untrusted connections and networks.

2.4.6 Dangers posed by Applications Downloaded from the Web

Apps (short for applications) have become very popular in recent years as developers have been creating software for smartphones and tablets for a multitude of purposes and interests including but not limited to information retrieval, productivity, social networking, weather and games. Jones (2013) reported at that time there were more than 950 000 apps in the Google Play Store and over 1 million apps in the Apple App Store. Generally it is safer to download applications from an app store than from web site links. However malware can be planted within applications from these stores as well (Botha, Furnell, & Clarke, 2009). Smartphone and tablet owners must not accept that all apps within the App Stores are safe anymore and should rather do their own research first by reading reviews of the apps they are contemplating downloading first (Botha et al., 2009). IBM (2012) stated that with the number of applications being added to these App stores it is not be possible for App Store administrators and owners to conduct in-depth analysis of the software code for each and every application. This leaves the possibility that users who download from these App stores, may still download and be infected with malware and other viruses. Careful consideration needs to be taken before downloading applications, as infected BYOD devices can cause havoc with the network infrastructure of an organisation.

2.4.7 Operational risks (Support Issues)

Traditionally IT departments in a non BYOD environment supported devices and systems that were all located at the premises of the organisation. The IT department was responsible for installation, configuration and maintenance of the hardware and software owned by the organisation. All infrastructure was standardized which made supporting such an environment relatively easy. Rose (2013) indicated that it was becoming increasingly difficult for IT departments to support a wide variety of mobile device models and software versions. The IT staff in such an organisation would need a substantial

amount of training and expertise to support all the different mobile devices. The nature of mobile devices allows the members of staff who own them to operate the BYOD device from any location as long as an internet connection is available. When employees have trouble operating their devices and need support away from the organisation's offices this adds more difficulty since the IT team is expected to provide advice and support telephonically without being able to assist the user face to face. BYOD devices that have not been configured properly by the organisation's IT team run the risk of becoming infected with malware could cause problems for the device and affect sensitive corporate data (Moir, 2009). Enterprise mobility has altered the manner in which IT teams now operate and IT teams that adopt a BYOD strategy are expected to have the knowledge to support the various models of BYOD devices the organisation allows on their corporate network. IT Teams that do not have the processes and procedures in place to support the organisations BYOD program will see an increase in operational risks.

2.4.8 Hidden BYOD Expenses

Although benefits of mobility and BYOD include employee satisfaction, increases in productivity and cost saving for the organisation there are also less obvious increased expenses that the organisation will have to consider (Rose, 2013). With an influx of employees wanting to use their mobile devices within the office environment the organisation will need to consider additional infrastructure including Wireless access points to allow these devices to connect to information systems. Depending on the agreement with the organisation additional telecommunications charges, including voice and data, will be for the employee or the organisations account. The company will need to plan for the increased bandwidth required for mobile device communication, without it negatively impacting on the existing infrastructure that was in place prior to allowing BYOD on the network. Mobile Device Management (MDM) systems and other security controls that are used to manage mobile devices are expensive (Kaneshige, 2012). This includes setup costs of the MDM system, yearly license fees for the number of devices and the infrastructure to host the MDM solution. According to (Kaneshige, 2012) the

research company Aberdeen Group conducted studies that showed BYOD costs businesses 33% more than those that have company owned mobile devices (CYOD).

2.5 Managing BYOD

In the past organisations relied solely on technical solutions to limit the risks to information loss and ensure information security (Ernst & Young 2008). These technical control measures do improve the information security for businesses, but this approach alone is not enough. Success can only be realised if both the technical and socio-organisational aspects are taken into account and addressed (Cavusoglu, Cavusoglu, Son, & Benbasat, 2009). The following sections discuss various organisational, human and technical controls.

2.5.1 Policies

The first step that an organisation needs to take when preparing to allow BYOD, is to create an explicit policy outlining all the rules and regulations that employees must adhere to if they would like to use their own devices on the corporate network. The policy needs to include the appropriate level of detail and be very clear for the users, as this aspect affects the users' view of the security issues to which the organisation is exposed. Purser (2002) recommends that the policies be written clearly and address the topics in a specific manner that is understandable to all users that need to comply with the policy. Once the policy has been finalised the policy needs to be distributed to all users who then need to familiarise themselves with the information within the document and sign off that they understand and will adhere to the acceptable use of the information systems described in the policy.

The policies need to be carefully designed in order to balance productivity as well as cater for the various risks associated with this technology. The security team and the business users need to agree on the design of the BYOD policy. Mansfield-Devine (2012) warns

that if the IT security team does not involve the business users, then the users will find the BYOD policy restrictive and will be less likely to adhere to the policy. In some cases users will find ways to bypass these restrictions. Only devices that meet the requirements of the policy should be allowed to access the company network.

2.5.2 Education and Awareness

Marrow (2012) is of the opinion that the majority of mobile security incidents are as a result of employees not being aware of the dangers of cybercrime, and recommends that organisations should invest in educating their employees about the information security and compliance with the organisation's policies. The most expensive and elaborate technical controls will be ineffective if the employees do not follow the best practices for using mobile devices and guarding information security. These steps will protect their personal information as well as the business data. As more individuals use their mobile devices within the organisation, if cybercrime incidents continue to increase, management will need to ensure that their employees receive regular information security and awareness training. Mansfield-Devine (2012) stated that it is crucial that employees form part of the organisations overall security design. The organisation's security is only as strong as its weakest link and technical controls alone are not enough. Organisations need to have a balance of both technical and non-technical controls to ensure the robustness of the information security posture of the organisation. Albrechtsen (2007) highlighted that employees often do not follow information security policies and procedures and that other work related tasks take preference over security. Post and Kagan's (2007) study indicated that an employee's perception of practising security was seen as a hindrance that kept them from doing their main duties and reduced their productivity. Siponen (2000) argues that employees need to be given all the facts of why information security was vital to the business and themselves, in a logical and rational manner, in order to improve their understanding. This approach will assist in the compliance of employees with policies and guidelines.

According to Albrechtsen and Hovden (2010) organisations that have users participate in regular information security discussions and group training have seen positive results in their employees' awareness and behaviour towards risks. Workshops and training needs to be used to provide the information in a concise and effective manner in order to hold an employee's attention. Walsh and Homan (2012) established that computer based information security training has been more effective than instructor based training: those employees that had received computer training retained much more of the information provided to them after a 60 day period, than those employees who did not. However, after 90 days, the information retained from both types of training was similar, which should prompt organisations to have more frequent sessions, in order to remind users of the threats and of how to conduct safe digital behaviour. Albrechtsen and Hovden (2010) are of the opinion that workshops and training that were not found interesting or motivating by the employees were very unlikely to improve the secure behaviour of users. Hagen, Albrechtsen, and Johnsen (2010) highlights the previous statement as they recommended building an entertaining aspect into information security education programs because it is a major factor that ensures employees and users are involved and motivated in the sessions. The training provided by the organisation will assist the employees to make responsible decisions when downloading applications, to avoid connecting to unsecure free public Wi-Fi networks and avoiding suspicious website links.

Thomson, von Solms, and Louw (2006) argued that employees that are well trained to appreciate the importance of securing the organisation's information assets are the organisation's strongest and most effective component of the information security program. These employees do not need to be experts in this field or have any technical certification but they do need a basic understanding of the concepts, in order to minimize risk in their daily functions. Practical examples should be used when training staff members on the policies and procedures of the information security policies.

2.5.3 Information Security Culture

Every organisation has its own specific culture, which consists of shared values, behaviours and beliefs that direct and shape members behaviours and attitudes in organisations (Smit & Cronje, 1992). In the 1990s organisations started investing in research that relates to culture based on the emerging evidence that culture can actually be linked to organisational success (Leidner & Kayworh, 2006). Ali and Brooks (2008) express their view that the study of culture is rooted in social psychology, sociology and anthropology which allows the researcher to draw from a fairly large data pool of knowledge.

The human side of information security deals directly with the corporate culture of the organisation and how employees view the organisation and their role within the business. The employees' individual values, beliefs and knowledge about the organisation's information security create the Information Security Culture (ISC). Both internal and external security measures must be in place to ensure an organisation's sensitive information is protected, and one side should not exist without the other.

Thomson (2006) states that even though it might not be easily recognised every business has its own corporate culture that can be used as a guide for the practices of its employees. The employees' attitudes and beliefs towards information security are largely determined by the corporate culture of the organisation. It is vital that management places a high priority on improving the information security culture by driving awareness of the importance of information security as one of the organisations goals. Beach (1993) is of the opinion that security culture in organisations guides the activities of employees and a clear distinction needs to be drawn between acceptable and unacceptable behaviour. Schein (1999) stated that corporate culture changes are often painful exercises, resisted and challenged continuously until employees are persuaded by the management hierarchy to accept the changes. For the successful implementation of information security programs within the organisation the message must come from the executive board all the way down the management hierarchy. Schlienger and Teufel (2003) suggested a four staged strategy based on top management commitment, the effective

communication throughout the organisation, awareness and training programs for employees and buy-in from all staff. ISC still remains one of the top concerns of practitioners and academics alike (Kolkowska and Dhillon, 2013).

2.5.4 Enterprise Mobility Management

Enterprise mobility management (EMM) is a comprehensive platform for enabling the secure use of mobile devices including smartphones and tablets. EMM is the collection of people, processes and technology dedicated to managing these devices, the wireless networks they connect to and the other services that contribute to the use of the mobile devices for business purposes (Pinchot & Paullet, 2015). The need for EMM systems has increased with the number of privately owned mobile devices (BYOD) that have been entering the corporate environment over the last few years and there is no sign of this need reducing. The EMM technical system typically has three main components which include mobile device management (MDM), mobile application management (MAM) and mobile information management (MIM).

2.5.4.1 Mobile Device Management (MDM)

MDM software tools assist organisations to manage the mobile devices that connect to their business' network infrastructure (Ghosh, Gajar & Rai, 2013). These MDM tools provide features that include device management, security configuration, and policy enforcement on the mobile devices, remote wipe of the data stored on the device and data encryption. These features allow the organisation to securely manage, monitor and control each device to minimize threats to the employee's and the organisation's data. The MDM tool can manage security settings including digital certificate installation and password management to authenticate BYOD devices. The MDM software installed on the mobile device allocates a specific area which is usually password protected where all

business related information is stored. This business information is kept separate from the users' information. This separation of data is also known as containerization (Yadav, Ganguly, Suman & Puri, 2015). Monitoring of application installations can be completed using this solution allowing IT departments to remotely install software applications and remove undesirable software too. One of the major features of MDM is device management because without this feature mobile devices are difficult to track. Another useful feature is the backup and restoration of data.

The architecture of how MDM functions is displayed in Figure 5 below. The MDM solution allows BYOD devices to connect to the organisations network infrastructure via encryption ensuring that the data communication is not intercepted by cybercriminals. The MDM server is located in the organisation's demilitarized zone (DMZ) which allows the IT department to configure mobile devices that are connecting from the external network. The DMZ is a network that separates the organisation's internal resources from the internet and allows connections from the internet to resources like internet websites and email servers. The certificate server only issues digital certificates to authorized devices which are used for authentication. The directory access servers ensure that approved BYOD devices have the appropriate access rights to resources on the organisation's network. The Sync server ensures that organisational data stored on the device is always synchronised and backed up.

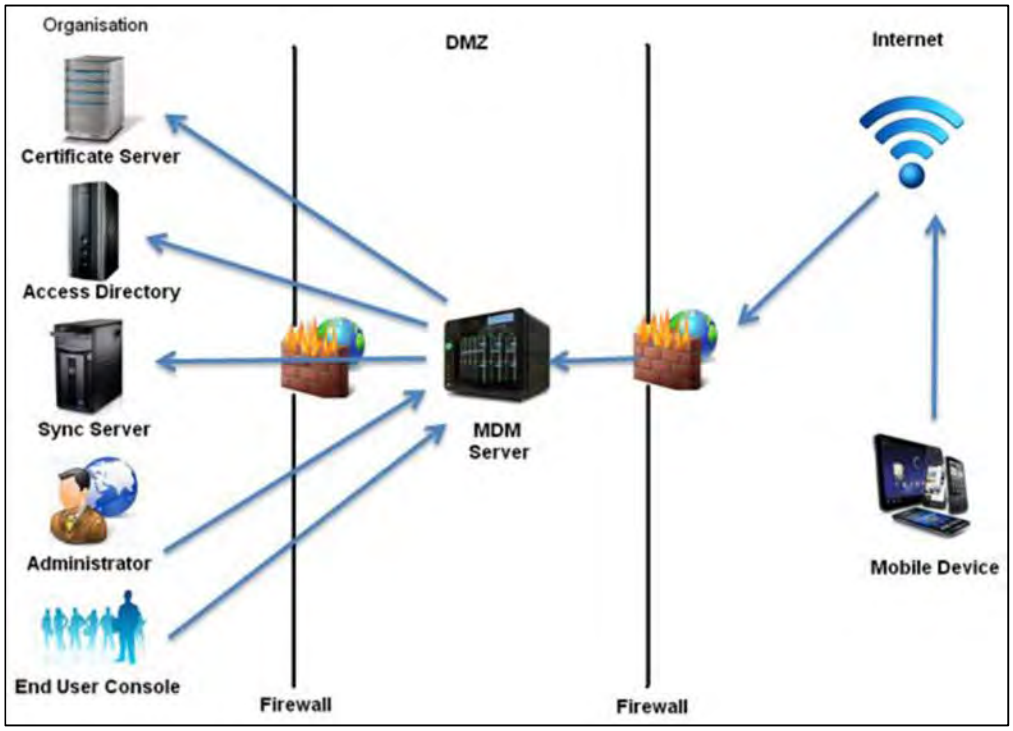

Figure 3. Mobile Device Management architecture (Ghosh et al., 2013)

2.5.4.2 Mobile Application Management (MAM)

MAM provides organisations with mechanisms to deliver enterprise software applications to personally owned and corporate sponsored mobile devices, and enables the organisations to improve the management of the business applications and data on these devices (Rouse, 2014). MAM functionality includes software deployment, software licensing, software configuration, maintenance, policy enforcement and usage tracking. IT administrators can also use MAM to remotely wipe application data and organisational data from mobile devices without affecting any of the users' personal data (Mathias, 2015).

2.5.4.3 Mobile Information Management (MIM)

MIM is a device-agnostic security strategy that focuses on protecting sensitive business information by separating it from personal data and containerizing it, then only allowing authorised users and applications to access it. This is accomplished using encryption (Mathias, 2015).

2.6. Summary

Even though the concept of bring your own device has been around for years it remains topical. As smart phone and tablet sales continue to increase, and organisations seek ways to increase productivity and improve their bottom line in the global economy, BYOD and mobile working are here to stay. BYOD is known to have introduced several risks to organisations including data loss, complexity, privacy and support issues (Calder, 2012; Pieterse, 2014). These risks are widely known to organisations and they are fighting to control their mobile workforce using technologies including MDM (Ghosh et al., 2013). However even the best tools and technologies cannot secure the organisation if employees do not follow security policies and safe cyber practices. In spite of the risks associated with BYOD, organisations have continued to allow employees to use mobile devices because the two benefits of cost savings and productivity increases seem to outweigh the risks. In Chapter 3 all the aspects of the research design are discussed.

3. Research Design

This chapter describes the research methods and overall research design including the research paradigm, research purpose and approach to theory, data collection, and data analysis procedures. The research design is considered to be the road map that the researcher should follow which will assist in answering the research questions (Yin, 1994).

A typical research process follows a list of activities which includes first stating the research problem then conducting a literature review to determine what was previously written on the topic. The research design is formulated after which data is collected and analysed. In the final step of the research process the report is written (Zikmund, 2000).

3.1 Philosophical assumptions

To gain a better understanding of the various methods that are used by researchers it helps to understand the philosophical underpinnings of social research. TerreBlanche and Durrheim (1999) stated that the research process consists of three major elements which include ontology, epistemology and methodology. All the interrelated thinking and practise which stems from the three major elements forms the research paradigm. Researchers construct the design and methodology of the study based on beliefs and assumptions of the research problem. These philosophies influence how the researcher conducts the study including the type of research questions to examine (Orlikowski & Baroudi, 1991).

3.1.1 Ontology

Ontology refers to the philosophical study describing the nature of reality and existence and what we believe about this existence (Stahl, 2008). Ontology questions what kind of things exist and how these things interact with one another. It is ones beliefs of what constitutes social reality and if there is a single or multiple realities. Ontology consists of two aspects: firstly objectivism and secondly subjectivism (Saunders, Lewis & Thornhill, 2009). Objectivism proposes that reality exists independently of the social actors involved in this reality. Subjectivism theorises that reality exists through the experience of the social actors and that they form their reality (Saunders et al., 2009). Subjectivism is the ontological stance taken in this research.

The researcher interacted with participants of the study to gain a deeper understanding of how the new BYOD program affected their realities. These in-depth interactions allowed the researcher to establish to which extent BYOD adoption affected participants, their abilities to handle change since the launch of the BYOD program.

3.1.2 Epistemology

Epistemology refers to the philosophical study regarding the nature and forms of knowledge (Hirschheim, 1992). It questions how knowledge is created, how knowledge can be acquired and shared, and the relationship between the individual seeking the knowledge and what is known. An interpretivist epistemological position was taken in this research to gain a deeper understanding of the phenomena by gaining the insights from IT and Business professionals involved in BYOD programs. According to Klein and Myers (1999, p.69) interpretivism proposes “that our knowledge of reality is gained only through social constructions such as language, consciousness, shared meanings, documents, tools, and other artifacts”.

3.1.3 Methodology

Crotty (1998) stated that the methodology is the plan of action of how the researcher will achieve his research objective. It explains how the research will be conducted which includes the research method, research choice and strategy, how the data will be collected and analysed (Saunders et al., 2009). There are two main research methods to collect and analyse data namely quantitative and qualitative methods (Saunders, Lewis & Thornhill, 2009). According to Saunders, et.al (2009) the quantitative method is used to study the phenomena by collecting mainly numerical data and applying statistical techniques to develop theories and/or hypotheses. The researcher's epistemological and ontological views determine the methodology choices to be used in the study. Qualitative research methods were used to collect the data for this research report. Qualitative research relies on the perceptions of the people involved in the study. In the study broad questions were asked, after which data were collected from participants in the study in the form of text and voice recordings. Denzin and Lincoln (2000) defined qualitative research as a method that produced scientific results even if some of the data obtained does not conform to strict quantification criteria.

3.2 Research paradigm

Taylor, Kermode and Roberts (2007) stated that a paradigm is a holistic perspective of something. The paradigm is the belief and practise patterns that provide the lens and framework that guides the methodological choices that the researcher uses to conduct the study. Saunders et al (2009) concluded that a paradigm is created by an individual or a group's perspective of the world around them. Depending on the philosophical assumptions of the researcher, the research can be either positivist, interpretive or critical.

Positivism is a philosophical theory from the natural sciences. Positivist research believes that reality is objective and it can be measured independently of the researcher's instruments and opinions (Myers, 1997; Orlikowski & Baroudi, 1991). Researchers that

follow this paradigm use mainly a deductive approach where premises and hypothesis are stated and statistical tests are completed on data to prove or disprove the hypothesis (Orlikowski & Baroudi, 1991).

Interpretive research aims to understand the phenomena by understanding the meanings that individuals' assign to them (Orlikowski & Baroudi, 1991). Ethnography, case study and action research are the research methods commonly used in this paradigm. These methods allow the researcher to investigate the phenomena closely by gathering and analysing multiple perspectives of the situation being researched (Oates, 2006).

Critical research aims to challenge social conditions or situations that prevent humans from reaching their full potential (Myers, 1997). It aims to provide emancipation from restrictive, alienating and domineering conditions that people in the phenomena being investigated experience. Orlikowski and Baroudi (1991, p.15) noted that researchers adopting the critical research paradigm "attempt to critically evaluate and transform the social reality under investigation".

The underlying philosophy of this research is interpretive with the aim to investigate what business priorities drive BYOD adoption. This research paradigm allowed the researcher to gain a better understanding of the phenomena being investigated. It allowed for deeper insights of the participants involved including their perception and experience of the BYOD in the organisation. The researcher was able to gain in-depth meaning of the problems and successes of the BYOD program from the interviews and interactions with the participants.

3.3 Research Purpose and Approach to Theory

An exploratory approach was chosen to allow the researcher to describe the study and provide new insights in order to gain a clearer understanding of the problem.

The literature review was conducted prior to engaging with the phenomena, which identified important concepts and acted as a conceptual foundation that was used as a guide for observations. An inductive approach to theory was used as the researcher observed the phenomena being studied. Cavana, Delahaye, and Sekaran (2001) defined the inductive approach as one that starts with data collection then analysing of the data for themes to ultimately develop theory. This is opposed to the deductive approach where the research starts with theory then support or deny hypotheses.

3.4 Research Strategy

Yin (1994) indicated that there are five research strategies namely survey, experiments, ethnographic, action research and case study. Selecting the research strategy depends on various factors like the research question, how the research will be conducted and the environment being investigated. The case study approach was selected as the most appropriate strategy to conduct this qualitative study. The case study strategy allows the researcher to study the subject in great detail within its real life context, where the existing knowledge is limited and phenomenon being studied is broad and complex (Darke, Shanks & Broadbent, 1988). A single case study was used to allow the researcher in-depth investigation and understanding of the situation being experienced in the organisation.

3.4.1 Case Site

The case study was conducted within a large financial organisation. The organisation referred to hereafter as Organisation X is one of the largest financial institutions in South Africa with branches in the United Kingdom, United States of America and a few countries in Africa. The business offers financial solutions that include insurance, financial planning, retirement and investments products and services. The organisation employs

approximately 8,000 staff with the bulk of them situation at the company's head office in South Africa and the remainder at the branches and business units globally. The case site was their head office, located in the Western Cape region of South Africa.

The researcher has been employed at Organisation X for a number of years and understands the company culture. Organisation X is one of the biggest financial services companies in South Africa. The structure of Organisation X's is illustrated in Figure 4. The company comprises of many different business units that collectively form Organisation X. As a financial organisation that invests clients' savings, pension fund and other investments information security and privacy is of utmost importance to the organisation and its clients. A core part of the business' revenue comes from the sale of financial products and the administration fees which the organisation charges their clients for the administration of the clients' funds and investment portfolios. The organisation has recently launched their BYOD program to allow their mobile sales staff to stay connected to the organisation systems when they operate outside the office. Other employees and executives within various other business units of the organisation have also started using their own devices to connect to the various applications and systems. Approximately 14% of total staff at Organisation X use mobile devices.

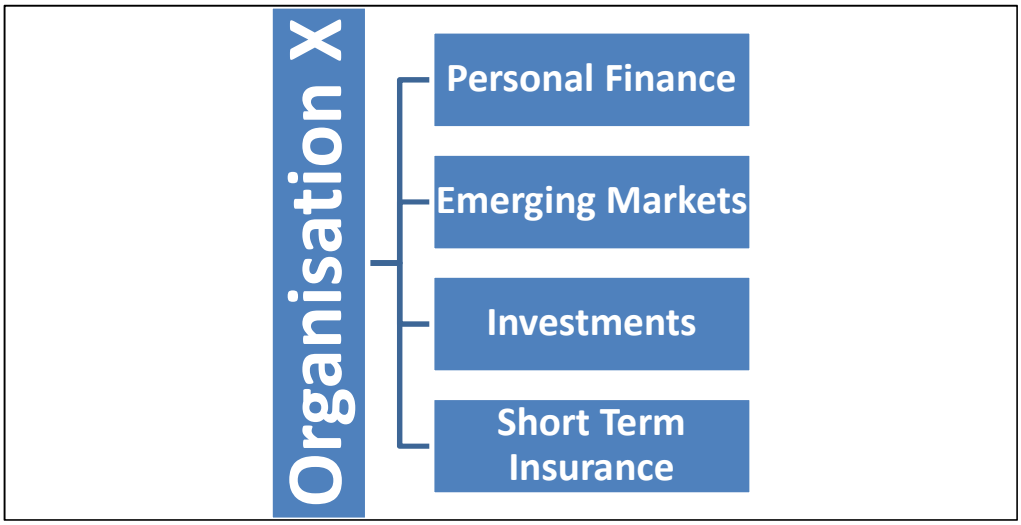

Figure 4. Business structure of Organisation X

3.4.2 Participants

Non-probability (purposive) sampling was used to select participants. The participants displayed in Table 2 all had extensive knowledge and experience in the fields of finance, mobility and information security and are the key decision makers and advisors in these domains. The participants of the study were chosen because they were either directly involved in the strategies and decision making for the mobility program and the introduction of BYOD or they were important users of the mobility program. Many of these participants were already known to the researcher prior to commencing the research report and the others were recommended by the original participants. Participants had more than three years' experience in their current positions jobs.

Interviews were conducted with 15 participants that worked in the following positions:

- Key role players responsible for the information security of the organisation,
- Individuals involved with mobile technology decision making including business management.
- Employees that use mobile devices for work tasks.

Table 2. List of Participants

Participant	Position	Years of experience in current position	Total years of experience
Participant 1	Consultant - Client relations	4	25
Participant 2	Head of IT Development	10	28
Participant 3	The Information Security Officer	8	18
Participant 4	The IT Architect	5	15
Participant 5	The Business Improvement Manager	3	22
Participant 6	The Financial Advisor	20	25
Participant 7	The Client Experience Officer	3	12
Participant 8	The Head of Information Security	15	25
Participant 9	Executive – Client Relations	5	13
Participant 10	The IT Executive	12	28
Participant 11	Head of Product Management	7	23
Participant 12	The Head of IT Solutions	8	31
Participant 13	IT Consultant	10	28
Participant 14	Head of Finance	5	16
Participant 15	Distribution Support Manager	4	12

3.5 Data Collection Techniques

The data was collected by means of interviews and organisational documents like policies, procedures and other artefacts. For the interviews an interview schedule (Appendix A) that consisted of semi-structured interview questions was used. Myers (2009) defined a semi-structured interview schedule as a list of predefined questions that

can be used as a guide during the interview with the participant. This type of interview schedule allows for further questions to be asked based on the response of the participant allowing for deeper information to be extracted. The questions in the interview schedule were designed to explore issues around the research objective and the research questions using existing literature on success and challenges of mobile devices. Organisational documents that included policy documents were also collected and analysed to supplement interview data.

Prior to the commencement of the interviews the researcher contacted the participants telephonically and sent them the interview questions to allow them time to prepare and better enable them to answer the questions thoroughly. Patton (1990, p. 348) suggested that researchers should record the interviews for accurate transcription later. The interviews were recorded using a digital audio recorder, the researcher listened to the recordings then transcribed the data after the additional notes that were taken during the interview were taken into consideration. The researcher listened to these audio recordings multiple times to familiarize himself with the content of the interview. The interviews were transcribed soon after it was recorded so that the interviewer could remember the context of what was being discussed during the interviews and no important information was lost.

Credibility needs to be applied to quantitative and qualitative research. The important factors that determine this credibility are reliability and validity (Saunders et al., 2009). In addition Saunders et al (2009) defined reliability as the ability to reach similar conclusions in another study if the same participants, data collection and analysis techniques were used.

Saunders et.al (2009) stated that there are four threats to the reliability of research. These are subject or participant error, subject or participant bias, researcher error and researcher bias. To ensure reliability the researcher listened to the recorded interviews multiple times then made notes in order to ensure that the reported findings were interpreted correctly. Researcher error was avoided by using an interview schedule to guide the interview process. In order to avoid participant bias the responses from participants were compared to check for irregularities in the data.

Validity is concerned with establishing if the findings of the study reflects the research objective. The two types of research validity that exist is internal validity and external validity. Creswell (2009) stated that internal validity refers to the accuracy of the findings. It questions the credibility of the data analysis procedures, trustworthiness and the legitimacy of the findings. The researcher used literature as well as organisational documents for triangulation to ensure internal validity.

3.6 Data Analysis

Each interview was saved in a Microsoft word document that was then imported into a Computer Assisted/Aided Qualitative Data Analysis Software (CAQDAS) tool. CAQDAS are software packages which comprise of a set of tools that interprets the researchers' qualitative data into themes. The types of qualitative data included text, images, audio and video content (Lewins & Silver, 2009). The CAQDAS tool that was used in this research report was the Nvivo 10 package (QSR International, 2016). The CAQDAS package included a combination of the following tools: content searching tools, querying tools, coding tools, linking tools, mapping or networking tools, writing and annotation tools.

Thematic analysis was used to categorise, organise and code the data into themes to identify patterns and relationships (Braun and Clarke, 2006). Thematic analysis consists of the following stages: data familiarisation, code generation, searching process for themes, reviewing process of themes, naming and defining themes and report production (Braun and Clarke, 2006). In the data familiarisation stage the interviews were read multiple times to understand the content before it was transcribed. During the second stage the researcher identified patterns that reoccurred in the data, called codes. The code generation process evolved over the period of data analysis to refine the final list of codes. The theme searching process involved using the codes to create themes within the data set. In the fourth stage of this process themes were refined by ensuring that the coded data related to the themes and the researcher reviews patterns between themes

by using a thematic map. The naming and defining themes stage involves an iterative process for reformulating the themes in order to represent the analysis. In the report production stage the researcher used the final themes from the data to answer the research questions.
A codebook was extracted from the Nvivo software package and is attached as Appendix B.

3.7 Research Time Frame

The research time frame for this study was cross-sectional as interviews were conducted over a period of two months. Easterby-Smith, Thorpe, Jackson, & Lowe (2008) suggested that cross-sectional studies are best suited to study the relationship between variables at a given time. Longitudinal studies are studies that investigated and analyse data at different stages over a longer great period – this was not feasible within the timing constraints of this study.

3.8 Ethics

Halai (2006) stated that researchers should conduct their study in a moral and ethical manner to ensure that participants and institutions used in the study are not harmed when the results of the research is published. The four essential ethical principles that were applied in this study were informed and voluntary consent; confidentiality of the data collected; anonymity of research participants\institutions and non-maleficence and beneficence (Oates, 2006).

The University of the Cape Town (UCT) strictly enforces a set of guidelines of how research should be conducted in an ethical manner and non-damaging manner. Ethics approval was requested and approval was received from the Ethics Committee of UCT

for this study. Bartunek and Louis (1996) emphasised that respondents must fully understand what is expected of them and researchers must get verbal and written permission from respondents that their contributions can be used in the report.

A cover letter requesting permission to conduct the study at the organisation was presented to the management team. This letter provided details regarding the purpose and benefits of the study; the research consent forms including ethics statements and the main research instrument was the interview schedule. Due to the sensitive organisational information that was shared in this study the organisations' management team insisted on the organisation name being kept confidential. The conditions that were set by the organisation's management was accepted by the researcher. The researcher then received approval from senior management to conduct the research study within the chosen organisation. Participation in the interviews were voluntary and participant identity were kept anonymous.

3.9 Summary

In this chapter the research paradigm, research strategy and data collection techniques were discussed. The research method used in this study was qualitative and the components of the research methodology used is illustrated in the research onion shown in Figure 5. The researchers' choice of each layer of the research onion is circled in the diagram. In Chapter 4 the findings of the study are presented and discussed.

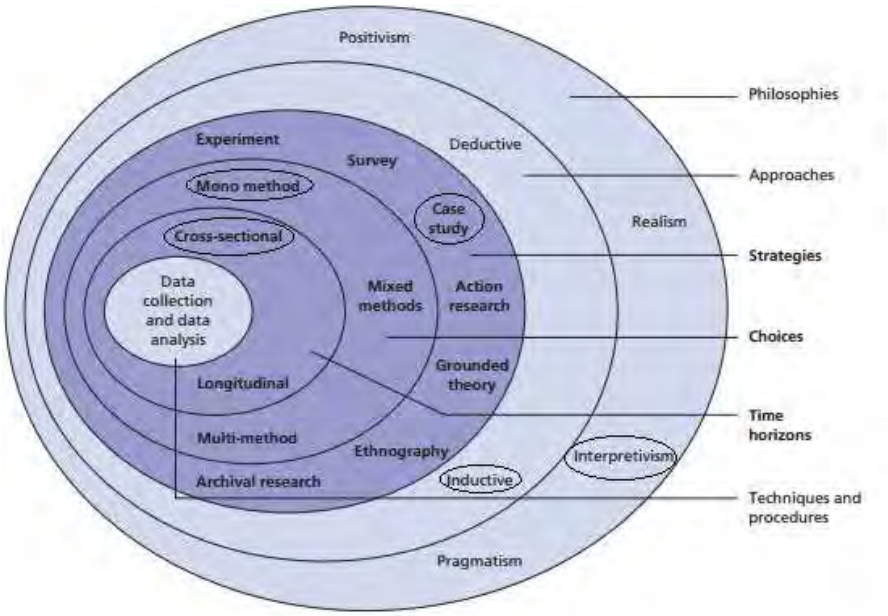

Figure 5. The Research onion (Saunders et al., 2009)

4. Findings and Analysis

This chapter starts with a brief overview of the various reasons the participants have for wanting to use the BYOD program. Thereafter the various themes that emerged from the interviews are presented and discussed. Figure 6 presents a word frequency illustration, extracted from Nvivo, highlighting the terms that appeared more frequently in larger font. Generic words (including bring your own device (or BYOD), organisation, etc.) which were mentioned the most was removed from the word cloud as the researcher felt these words did not add any value to the illustration and the analysis.

Figure 6. Word frequency illustration

4.1 Reasons for BYOD participation

The participants of the study listed numerous reasons for adopting BYOD as illustrated in Figure 7. The number one reason these participants participated in the mobile program were for communication purposes and to access schedule information. Besides listing communication as the main reason for the mobility usage, many also stated that mobile communication was the main reason staff in their respective business units wanted to have access to the mobility program. The second biggest reason the participants of the study wanted access to the mobility program was to gain access to the organisation's Wi-Fi network for Internet access when they moved inside the company premises with their mobile devices e.g., attending workshops and meetings. If these users' used a laptop those devices would by default be setup for Wi-Fi access but mobile devices including cellular phones and tablets needed special authorisation from the individual staff members' direct manager to be granted Wi-Fi access on those devices. Of the participants only two used their mobile device to access the SAP ERP applications\sites to request and approve leave for staff that report to them. Two participants used the mobility program to access the financial approval systems for large approvals when out of the office. The mobile applications developed by the business to provide product information and that allowed financial advisors with functionality to provide financial advice and products to clients was also used by two participants. Only one participant used the calendar feature to keep track of his scheduling information and used this option only because he did not want to process work emails on his personal device. The other reasons included accessing sharepoint sites from mobile devices and reviewing large documents on mobile instead of printing the documents.

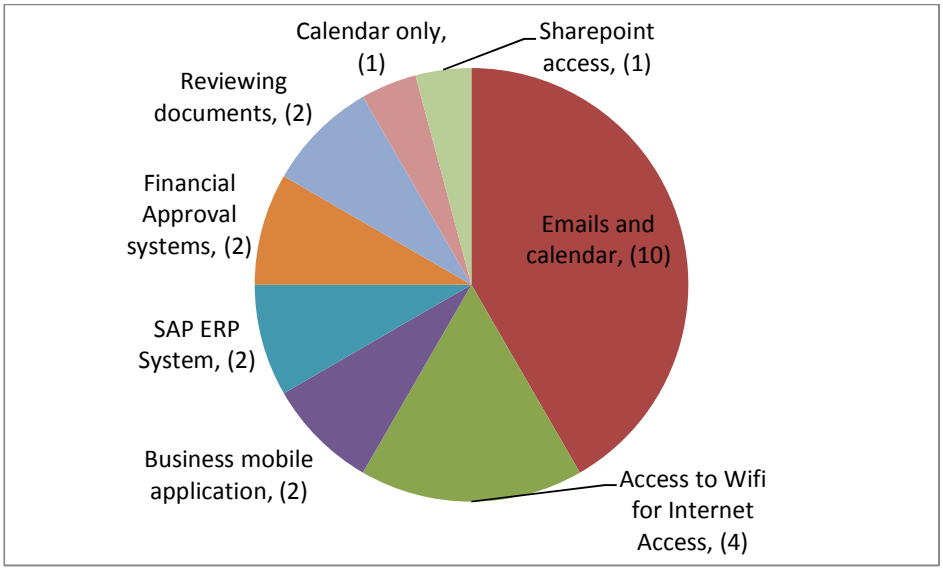

Figure 7. Reasons for BYOD participation

4.2 Theme 1 – Mobility Benefits

4.2.1 Subtheme 1 - Mobile workforce

The majority of the participants agreed their organisation's enterprise mobility strategies needed to align to the overall organisational objectives. When participants that were involved in the mobility decisions, especially around BYOD, were questioned about their businesses mobility requirements their responses varied and were all suited to their individual business needs but all agreed on the importance of mobilizing the workforce. Most of the participants also agreed that going mobile was going to become standard in future and with employees bringing their own devices to work they needed to embrace the change.

All participants stated that the organisation's mobility program allowed their mobile workforce to be more flexible by enabling them to stay connected when they were out of the office. Traveling executives were now able to stay connected with their teams by

responding to important emails, completing large financial approvals on the financial system and gaining access to vital information while away from the office.

Most of the participants of the study agreed that BYOD and mobility is going to have a massive impact on the South African economy. The advances in technology allow businesses to get more work done in less time. Transactions can be completed by mobile workers faster than before. BYOD and mobility makes collaboration of different individuals much easier by allowing them to communicate in real time irrespective of city, country or continent. Mobile devices allow employees to not be restricted by core working hours only so more production gets completed for the business which ultimately drives revenue.

All participants agreed that mobility was vital for the modern organisation. The organisation needs to allow its mobile staff to work with the tools and from any location user is comfortable with when they are not at the office. Mobility allows mobile workers to have access to corporate information quickly which enables them to make decisions faster. Participant 2 noted: *"One of the facts that we did not envision before launching the mobility program was the amount of work staff are doing after hours in their personal time."*

4.2.2 Subtheme 2 – Productivity

Participant 2 said that having the BYOD program they have seen their staff being more productive. "This meant configuring their information systems to have online capability for quotations of their products and front office processes". These systems needed offline capability as well so that when the mobile worker did not have internet access they could capture information then as soon as they could establish a connection synchronize the data back to the organisations systems. Participant 3 agreed stating that he believed enabling the organisations' workforce to be more mobile meant this allowed them to be efficient so they could assist clients more effectively. Participant 9 stated: *"As mobile devices and data become cheaper more users will be using mobile devices for business*

and personal reasons. BYOD allows the users to work with devices that they are more comfortable with which relates to more productive work being completed."

Participants noted that they needed to capitalize on the BYOD phenomenon so that the company could make use of what the employees already had which were their personal mobile devices so that these could also be used for business purposes.

Mobile devices allow employees to increase their productivity by allowing them to access information and complete their daily tasks irrespective of where they are. Participant 4 noted that these mobile users were much more productive because their mobile devices allowed them to communicate with clients and other employees wherever they were without the need to first come back to the office to respond to communication. The Participant 4 also noticed an increase in productivity since BYOD and CYOD are allowed. The surprise finding that decision makers had not predicted was the amount of after-hours work that was being completed by staff. Participant 5 said: *"I find it easier to answer emails in the evening in the comfort of my own home which makes me more prepared for the days' work when I come back into the office the next day and I can get straight into working on my outstanding tasks."*

Smartphones have become the main means of communication for individuals and this is especially true for the African continent. One of the reasons for this is the lack of infrastructure in Africa in terms of roads, telephone and fixed line internet connectivity. *"In South Africa and the rest of Africa the number of mobile internet users is growing and has the greater penetration rate compared to fixed land line internet connections"* (Participant 10). *"These smartphones are driving informal markets allowing consumers to gain access to information via these devices to make purchases and transfer money via these devices. South African businesses are now able to make contact with clients in rural areas via mobile networks and sell their products and services to clients from these regions that the business would otherwise not have access to"*. Participant 12 and Participant 11 stated: *"Our focus in the business must be to make the information about our business, the products and services we offer more accessible and easier to consume the information via mobile devices including smartphones"*.

Participant 1 stated that the Client Relations division's requirement prior to starting the mobile program was to enable their mobile workforce by providing them with the tools that could increase their productivity, allow for process improvement and save on costs. They wanted to operate in a virtual hub that allowed them to plug in their devices and work when they needed to be in the office and where there was no need for permanent office space.

4.2.3 Subtheme 3 - Digital \ Paperless environment

Executives in board meetings are now able to electronically view large board documents that are on the agenda for the meetings. These documents are usually in excess of 500 pages each so not printing these documents assists in costs savings for paper and printing. Participant 3 noted that mobile devices including smart phones, tablets and laptops are making it easier for employees to collaborate on projects and other milestones. These devices facilitate electronic conversations using tools like SMS, email and WhatsApp.

Participant 1 mentioned that the business she represented needed to enable their staff to operate in a mobile manner. This participant was an advocate of the CYOD model. This participant did not want their business information stored on their personal devices. Participant 1 stated: "I prefer one company sponsored mobile device for all business related tasks and wanted a mobile device that could offer a fully integrated solution. This solution needs to allow for a paperless environment and the mobile device functions have to have the following functions: email, Microsoft Lync messenger, WhatsApp, voice calling, Bluetooth for when driving, ability to sign documents digitally, uploading files to backend systems." The researcher noted the amount of BYOD users far outweighed CYOD users in the organisation but the amount of corporately sponsored devices (CYOD) was steadily increasing as managers saw the benefits of having standardized fully integrated mobile devices.

A paperless environment was also important to the Client Relations division that Participant 1 represented where documents could be signed on their mobile devices and stored digitally on protected storage. The mobile devices they required needed to include and allow the following functionality:

1. Tablet\hybrid devices that would allow the users to touch, type documents, digitally sign documents, make voice calls and have video conferencing functions. (These hybrid devices are a tablet with a keyboard that can be plugged into it so that the device operates as a full laptop.)

2. Access emails, SharePoint and backend systems from their tablet\hybrid devices.

The literature shows that the main benefits provided by BYOD is the ability for users to connect to organisational systems irrespective of their physical location allowing them stay connected which provides production benefits for the organisation (Forrester, 2011; Calder, 2013). The findings indicate that the benefits listed in the literature are also experienced by Organisation X in terms of productivity and accessibility of information. The other benefit listed in literature is the cost saving on hardware from BYOD but this benefit did not come through strongly in the findings from participants.

Table 3. Theme 1: Mobility Benefits framework matrix

	Theme 1 : Mobility Benefits
Participant 1	BYOD assists the organisation in enabling our mobile workforce. BYOD has helped most with email communication and having access to information systems including workflow.
Participant 2	The BYOD benefit was about meeting the customer at the place that is most convenient for them. Our employees can now conduct business with clients that are located in rural areas using mobile devices where there is little to no infrastructure.
Participant 3	Mobile communication.
Participant 4	We have 1360 users that connect via the mobile devices to gain access to email.

Participant 5	Productivity - I am able to get more work done on my mobile devices.
Participant 6	I have approximately 1000 clients that I provide financial advice for and I can't see all clients but technology allows me to communicate with them via email. I also use my mobile device to record the meetings I have with my clients because this helps me remember what was discussed during the meeting and I can refer back to the specific instructions given to me and helps me to document everything better.
Participant 7	The mobility program allows access to email on cellular phone and access to organisation resources.
Participant 8	Using my mobile device I am able to keep track of email and my calendar.
Participant 9	Productivity has improved. Mobility - My staff are always on the road and mobile devices keep them connected
Participant 10	Email - Communication. Mobility - Many of our executives use BYOD and this assists them while traveling.
Participant 11 and Participant 12	Access to the Wi-Fi on the organisations network for internet access and to gain access to their email and calendars.
Participant 13	More productivity and have better flexibility.
Participant 14	This participant was only synchronizing their calendar information to their mobile device. Mobility is important for the modern organisation.
Participant 15	The company wanted to capitalise on new mobile technology and developed a mobile application that allowed their advisers to streamline client service. This application enabled financial advisors to view and access customer information from the mobile devices. Productivity has increased.

Participant 16	These devices were mainly used for email and viewing of calendars. Users requesting to use the mobile service in the organisation needed a justified business reason to gain access.
Researcher summary	Benefits included: mobile workforce which included easier communication, increase in productivity and digital \ paperless environment

4.3 Theme 2 - Client Service\Experience

Management guru Peter Drucker stated: “To satisfy the customer is the mission and purpose of every business” (The Economist, 2013). Customer satisfaction is one of the core objectives of any business irrespective of the product or service being offered to the market.

4.3.1 Subtheme 1 - Faster response time to client queries

At the organisation where the data was collected there was a strong emphasis on doing business that focuses on their clients. It’s vital for the business to understand their needs and fulfil their requirements while providing an excellent service experience. Employees using mobile devices are able to respond to client’s queries and other business units quickly. There is no longer a reason to not be connected to company systems while traveling or in-between meetings. Customer relations consultants can assist clients with their queries and changes to their portfolios while visiting clients at their premises.

Participant 1 agrees with the statement above: “*Mobility has improved our communication as Client Service Representatives respond much faster to emails on their tablets in-between meeting and while waiting at Clients premises”.*

An important benefit of mobile devices is that it allows employees to respond to clients queries very quickly and efficiently. More than half the participant mentioned this as a benefit in their business divisions. Participant 1 was responsible for her business units' mobile requirement. The client relations team that the participant represented included several Client Relations Managers which was headed up by a Client Services Executive (who is also a participant of the research study). Mobile devices are an essential working tool as much of the working day includes traveling to and meeting with clients.

Participant 6 noted that he and his fellow advisors are greatly benefiting from BYOD devices by way of the financial application that was developed by the organisation for them to do business remotely on their devices. *"These mobile devices allow us as financial advisors to communicate via email with their clients and also meet with clients at different locations of the clients' preference"*. The application they use allows them to complete analysis of the clients' financial needs to enable them to make better financial choices in terms of retirement plans, investment choices and other financial plans. Participant 6 explained that forms can be filled in on the tablet devices and signed electronically for a better client experience. Capturing these forms electronically helped with improving processes and moves the organisation closer to a paperless environment.

4.3.2 Subtheme 2 – User friendly IT systems\applications

Participant 2 reported that in his area of responsibility IT systems that are client facing are also being developed for mobile devices and lot of thought is being put into the design of this and how information will be displayed on these devices. *"Information about the company's products and services must be made available on mobile devices so that this information can be easily accessible to current and potential clients".*

In order for businesses to engage with their clients effectively they need to ensure their business strategies include the appropriate business models, technology and processes (Hollingworth & Harvey-Price, 2013). Technology has empowered consumers with the ability to access information about products and services in a manner to suits their

preference. While the main communication channels for consumers are company websites then email and social media pages have become a popular channel for communication between businesses and their customers (The Economist, 2013). The latest addition to these communication channels has been mobile applications. Organisation X has business strategies to cater to their clients for all communication channels about their products and services. These include the traditional company websites, emails, television, print media but they also cater for the social media pages and mobile applications for clients available for download in all major application stores. The organisation has already developed their systems so that information can be rendered in a user friendly design for mobile devices making it easier for clients to interact with the information and systems. The findings show that BYOD allows the employees of Organisation X to provide a high level of customer service to their clients whether it be face to face or responding to queries faster than ever possible before.

Table 4. Theme 2: Improved Customer Service framework matrix

	Theme 2 : Improved Customer Service \ Experience
Participant 1	Client facing staff members that use mobile devices for work purposes respond to email queries much faster.
Participant 2	We have designed our mobile applications to be user friendly and very accessible on mobile devices.
Participant 3	Employees are able to respond quicker to email, being able to connect remotely to the office and be fully functional.
Participant 4	We have developed certain web applications to be more compatible to mobile devices.
Participant 5	BYOD allows our staff with mobile devices to provide our clients with great service. You need to be accessible at all times. We need to move more towards digital solutions and if your employees aren't digitally enabled then they can't provide the service that the clients expect.
Participant 6	Advisors are able to do the analysis of the client's financial needs and capture investment choice of the client directly from the client's

	premises and send the information to the organisation information systems via the mobile device.
Participant 7	Staff are able to provide much quicker responses via mobile so they are a lot more accessible to clients and the rest of the business. Response to queries influence the SLA
Participant 9	Before the mobility program there was a big delay in when the staff got back to the client.
Participant 10	The use of the intermediary app is used to check client info, sign documents online and to complete risk profiles.
Participant 11 and Participant 12	The organisations view is to make it easier for their users, intermediaries and brokers to do business as quick as possible with the company.
Participant 15	The mobile application allows staff to provide better client service and improve the client experience.
Researcher summary	The clients experience was improved by staff using their mobile devices to assist clients and the organisation developing customer friendly applications for clients.

4.4 Theme 3 - Competitive Advantage

4.4.1 Subtheme 1 - Innovation

In order for the organisation to stay ahead of the competition the employees need to find innovative ways of doing business. This way of thinking is encouraged throughout all levels of the organisation. Allowing employees to use their own devices that they are more comfortable with encourages this innovative behaviour. *"If the business can't adapt and stay abreast with mobility the business will not be able to remain competitive in the financial industry"* (Participant 12).

Participant 11 has noted that shops with no or little online facilities are closing down fast because they are not catering to the mobile internet user market. "*It is also important to keep abreast of what your competitors are doing so if they are offering consumers mobile internet information platforms your business also needs to do the same and better to avoid losing potential clients".* These two participants believes that mobility allows the organisation to save on costs of doing business with remote clients and if your competitor is conducting business at a cheaper rate than your business then your business will lose out and eventually get cut out of the market that they are competing in.

"The organisation aims to have the best products and services in the industry and having the latest technology including IT systems and mobile devices allows the business to stay ahead of the competition in the industry." "*Professional image – When staff meets with clients having the appropriate technology creates a good impression of the organisations systems and their ability to administer their business. Having outdated technology when presenting to potential clients can have disastrous effects on their perception of the organisation." (*Participant 11).

4.4.2 Subtheme 2 - Professional Image

In the sales portion of the business mobile devices have been an invaluable tool. When the financial advisors, client service and other sales professionals visit clients and use their mobile devices it creates a professional image of themselves and the business (Participant 1).

Participant 2 mentioned a mobile application developed for intermediaries and financial advisors: *"We also have an app now that allows them to access information and assist clients face to face."*

Some participants who were in support of the CYOD model felt that it was important that their staff that was visiting clients was equipped with the right technology to service the client's needs. This meant having devices that had sufficient processing capability but

also assisted with creating a professional image of the staff member and the business. Participant 7 believed that professional image of his staff was important for sales of the business products and services. The mobile devices were typically used in presentations to prospective clients and when servicing existing clients. Participant 1 had the same comments regarding professional image and has also seen that when using cutting edge technology, the devices was often a conversation starter which helped in building rapport with clients. The majority of the participants agreed that it was vitally important to use mobile devices in their business to remain competitive in the industry. If the competition was using mobile devices and they were not the competition would have the edge and do better in the market. Four of the participants were already thinking of new and innovative methods to take mobile devices and the mobile applications to the next level to provide even more benefit to the customers and internal employees.

The organisation can use BYOD and its mobility program as an incentive to attract and recruit younger talented professionals to the business. These younger professionals have grown up with the latest technology and use these tools to find innovation ways of solving problems. Allowing existing employees to use the mobility program assists the company with retaining their talented individuals.

The BT Group conducted research study that surveyed 2000 information technology users including senior managers across 11 countries regarding their attitudes towards BYOD. More than 80% of the IT managers thought that BYOD provided a competitive advantage for organisations that could manage the risks associated with BYOD over organisations that did not offer a BYOD program (Sing, 2012).

The findings above indicate that BYOD and mobility in terms of accessing important information and the ability to make importance decisions based on the information provides a competitive advantage for the organisation. The literature on BYOD's competitive advantage and the information extracted from the participants is aligned.

Table 5. Theme 3: Competitive advantage framework matrix

	Theme 3 : Competitive advantage
Participant 1	The client service managers and sales staff have a professional image using the mobile devices when visiting clients. Having leading edge technology has been a positive conversation starter with clients.
Participant 2	Organisations need to adopt BYOD to remain competitive in the market they are operating in.
Participant 3	It is important to keep up with your competition. If they are doing BYOD so should your organisation.
Participant 4	To be competitive in the industry we have to have the right technology. BYOD allows the user to access emails wherever they are, sign documents etc.
Participant 5	BYOD is important because smartphones are driving the informal markets mainly because of accessibility.
Participant 7	Professional image is important in sales. It is the perception of doing business with technological advance business. Competition is important is the industry we operate in. If our competition are communicating via mobile and we are not we will suffer a disadvantage.
Participant 11 and Participant 12	Your competitors and the market determine what you should be doing to keep abreast and not lose out on business. Mobility makes things cheaper and brings down the cost of servicing and doing business. Mobility is hugely important for the economy and businesses in South Africa.
Participant 15	Doing business electronically improves sales and client facing staff's professional image. Financial advisors using the mobile application are gaining a competitive advantage over others in the industry.

Participant 16	The organisations strategy is to move into developing markets where there is little infrastructure and mobile devices are used extensively because of this.
Researcher summary	BYOD provided competitive advantage by allowing the staff to use technology that created a professional image and allowed the organisation to use the technology to create innovation systems that can assist both clients and staff.

4.5 Theme 4 - Process Improvement

Participant 2 stated that their division had the utility benefits in mind for their mobility program that included providing their financial advisors and brokers with online capability for the business quotations systems, front office processes and the ability for the sales person to fill in the forms and process it online with the customer. These individuals who deal with customers need all the tools available to be able to service the customer at the place that is most convenient for them. Future systems need to be built that allow the company to communicate their product and services with customers of all ages, across multiple platforms including mobile. After the organisation has their mobile program in place that allows employees to use their mobile devices to connect to organisational resources, the program can be used to attract young talented individuals to join the business. Businesses needed to capitalize on the latest mobile technology in the market and use this technology to forward their business goals.

Clients can complete and sign documents electronically on these mobile devices, with the assistance of the client-facing staff. Mobile devices also allow for the business to go paperless as all documentation is stored electronically at the business premises instead of in large filing cabinets. Finding customer information in filing cabinets is time consuming and these file take up lots of storage space that is expensive. Participant 15 stated that *"Productivity is improved because access to the information and processes are much faster using mobile technology and the application."*

"Our mobile application allowed the intermediary to fill out the forms with the client on the broker's mobile device without the need for papers. Our focus is to make it easier for intermediaries to do business with our company." - Participant 11 and 12

In research by Mcafee and Brynjolfsson (2008), the authors' state that investment in the organisations IT systems aids in process improvement, which leads to higher company performance. The technology giant Dell released the results of their Global Technology Adoption Index 2015 which revealed that companies that have adopted technologies, including mobility, cloud and big data experienced 50 percent higher growth than companies that did not adopt those technologies (Dell, 2015). According to the study, companies experienced a 39 percent increase in improved efficiency and 21 percent increase in business process improvement. The findings of the study as well as literature prove that BYOD does assist with business process improvements.

Table 6. Theme 4: Process improvement framework matrix

	Theme 4: Process improvement
Participant 1	One of the organisations business drivers is process improvement. We want to be able to sit with clients and have them sign documents online and have the ability to upload to the backend systems. We want to work in a paperless environment.
Participant 2	There was a need to have online capability in the web space for our quotations and front office processes.
Participant 3	With BYOD our intermediaries and advisors are now able to complete online contracts etc. and engage with the client, accessing the required information and completing that application from a mobile device.
Participant 4	Client are able to sign documents on the mobile devices in the presence of our financial advisors allowing the process to go much faster than having to fill in forms and have them scanned etc.
Participant 6	Advisors are using the applications that were developed to process forms online.

Participant 11 and Participant 12	The organisation developed an application for the intermediaries and clients to access the company's product information, they can login, check other financial information, financial news and it allowed the intermediary to fill out the forms with the client on the broker's mobile device without the need for papers.
Participant 15	Using mobile devices allowed the companies staff to move away hard copy paper forms.
Researcher summary	The BYOD program and the applications specifically designed for BYOD and the online capabilities of this technology is improving processors in the business.

4.6 Theme 5 - BYOD risks

Mobile devices have a higher risk to an organisation compared to desktop computers that are permanently fixed and located on the organisation premises and protected by the security firewalls and other security measures. Mobile devices are constantly moving with the owner of the device and the problem is it can be easily lost or stolen. As the technology that these devices are built with has improved over the years the size of these devices have become smaller also making them more prone to be misplaced (Calder, 2012).

4.6.1 Subtheme 1 - Information Security Concerns

Of the many risks associated with the mobile devices information security of the organisations was the most common risk stated by participants. Sensitive information can include client information and strategic business information, new product development not yet in the market and sensitive internal communication. Corporate data stored on the device is also moving outside the perimeter of the organisation and is difficult to control. Participant 1 stated that one of the main functions that they use their

mobile devices for is to respond to emails which contains sensitive personal information of their clients as well as other important internal communication that should only be viewed by certain individuals. If that information got into the wrong hands and was used maliciously it could be detrimental to the organisation. This participant emphasized the role the organisation had in protecting their clients' personal information and loss of this information could lead to serious legal implications for the organisation. If the organization was exposed and valuable information was compromised it would affect the organisations reputation which would lead to loss in revenue (Participant 3).

One of the concerns for Participant 2 was the uncertainty of where the information was after it was stored on the mobile devices and what copies existed elsewhere. With the current tools available it made it impossible to have an accurate view of this. This risk was also mentioned by the Information Security Officer that noted the dangers of synchronizing data to mobile devices and other IT services. Available cloud services like Dropbox allows the possibility for staff to synchronize business data to the cloud without the knowledge of the organisation. These cloud services have been known to be vulnerable to attack by cyber criminals.

Two of the participants believed that in South Africa mobile devices were mainly stolen for the monetary value of the device and not the information stored on the device. They did say it is was vitally important that the organisation and individuals tasked with Information Security responsibilities protect sensitive data though but data theft and data leaks was not accounting for mobile device theft. The majority of these thefts were from break-in's to staff vehicles where mobile devices including laptops and tablets were being stored when the employees were away from the vehicles.

As stated in the literature review the number one concern for organisations using BYOD is information security (Calder, 2012; Lohmeyer et al. 2002; Ransbotham and Mitra, 2009). Similar to the literature the main BYOD concern for participants was Information Security.

4.6.2 Subtheme 2 – Regulatory Privacy Compliance

Most of the participants were concerned about how difficult it was to manage data on mobile devices and how this would affect compliance to the Protection of Personal Information (POPI) act. This act which promotes the protection of personal information and guides how this information is processed was signed into law and once the commencement date is set companies will have one year to comply or face hefty financial penalties. This legislation will force companies to report on lost data including customer records so having data stored on mobile devices will make it difficult to comply with this legislation (Participant 3).

Participant 4 stated that more focus should be placed on where sensitive data is stored so as to understand the risk exposure from a reputational risk point of view. This will enable the organisation be better prepared to protect sensitive data and ensure compliance to the POPI act.

4.6.3 Subtheme 3 - Financial Risks

Other financial risks related to mobility and BYOD are the IT systems that are being developed to cater for mobile use. These development costs of these systems are usually high. When developing applications that clients and internal staff can use there is always the chance that the mobile system including apps will not be as successful as it was originally projected and the number of users that continually use these systems are lower than expected.

4.6.4 Subtheme 4 – Malware, Unsecured Wi-Fi and theft of mobile devices

As with risks for the organisation the mobile user also runs the risk of losing their personal information stored on their mobile device. Organisational information that was stored on mobile devices can be backed up on storage at the organisation's premises but if the mobile device is lost \stolen or corrupted then often the users' personal information is lost. Participant 8 stated that research showed that mobile devices are a lot more vulnerable than laptops as the smaller devices are often misplaced and lost. One of the reasons for this could be that tablets and smartphones cannot be locked to the desk like laptops can with cable locks. The loss of these devices is for the users' own account. The insurance costs for their devices and the costs for replacement are their responsibility. Mobile devices are also damaged more easily than its laptop counterparts (Participant 9).

Participant 8 noted that other risks facing mobile users are connecting to unsecured wireless access points that provide wireless networking and internet access. Cyber criminals use these unsecured networks to intercept unencrypted communications sent and received by the mobile user.

This participant points out that there has been an increase in malware that has been developed to exploit and infect mobile devices. The purpose of this malware is usually to steal sensitive login information that includes credit card and banking login details. According to him there has not been an increase in malicious software like viruses since launching the mobile program.

Participant 1 felt that the risks for laptops and tablets\smart phones were similar as all these devices moved with the mobile user compared to the traditional desktop computer that stayed at the office. This participant who was an advocate of the company sponsored mobile device was of the opinion that the less mobile devices the user carried with them the better. So instead of having a laptop, a business tablet, personal tablet and smartphone they were transporting to and from the office combine the functionality of certain devices then this reduces the risk to the organisation and the user. Their division

was using corporate sponsored hybrid devices that had the functionality of a laptop and the versatility of a tablet and smartphone that was also partially covered by the business. That enabled employees to only carry two devices compared to four.

Table 7. Theme 5: BYOD Risks framework matrix

	Theme 5 : BYOD Risks
Participant 1	There is a risk in terms of the cost of the mobile device and more importantly the sensitive information stored on the device. Information security risks.
Participant 2	The risks the organisation has using mobile devices is security of the business information stored on the device and the uncertainty of where the information moves to from there.
Participant 3	Information security risks. Privacy issue if data is lost. Reputational damage if client's data or finances are lost.
Participant 4	Risks included the confidential information stored on the device and if information was lost and misused what the impact would be to the organisation from a reputational and financial standpoint.
Participant 5	The risk lies in sensitive documentation stored on mobile devices.
Participant 6	Emails received with client's attachments are stored on the mobile devices. Loss or misuse of this sensitive information can be detrimental to the organisation and the client.
Participant 7	Security is the highest risks which have more of a reputational impact for the company and from that it could lead to financial risks.
Participant 8	From a corporate perspective you could lose corporate information or expose it. People are more likely to connect to potentially malicious wireless access points with their personal devices than with their laptops. Stealing of the individuals credentials like banking passwords which it is more of a personal than corporate risk.
Participant 9	Security of data stored on mobile devices.

Participant 10	The risk for the organisation is it is difficult to manage unstructured data especially on mobile devices.
Participant 11 and Participant 12	Sensitive information on byod devices could be lost or misused.
Participant 13	Loss of information stored on mobile assets. Reputational damage.
Participant 16	The risk exposure was the information going onto these devices and the ease of use these devices provided but this contradicted information security.
Researcher summary	The BYOD risks included loss or misuse of sensitive information, privacy issues, financial risks and technical risks like malware, unsecured Wi-Fi.

4.7 Theme 6 - Management of BYOD

The organisation uses the following best practises to manage it mobility risks.

4.7.1 Subtheme 1 - Policies

When questioned about the management of BYOD risks the majority of the participants felt that in order to protect the organisation's information and especially on mobile devices a combination of internal and external security controls was required. Using one type of security control alone was not adequate in protecting the organisations information assets. Nearly all the participants from the information technology side quoted policies as their first method of controlling mobile risks.

The organisation had recently rolled out their digital behaviour policy where a major component of this policy was dedicated to mobile device security. This policy and other

information security policies in the organisation prescribed the rules and regulations that all users of the organisation network infrastructure and IT systems had to adhere to. This policy also advised users on how to use their devices, IT systems and the internet safely to minimize their chances of being exploited or having corporate information exploited by cybercriminals. All users from all the business units in the organisation had to sign off on this policy. Prior to the signoff of the digital behaviour policy all users were required to read regular email communication regarding this as well as complete a compulsory online training session that quizzed the users on their understanding of the policy. Another method to entice users to understand this policy was the creation of a series of animated videos covering various information security topics. At the end of the videos staff was asked a few simple questions and if they answered correctly they could enter a competition where they stood a chance of winning prices that included tablet and smartphone devices.

Mansfield-Devine (2012) highlighted the importance of an information security policy and this should also cover the rules for safe BYOD usage. The policy should strike the right balance of security while also not being too restrictive to prevent the users from working.

4.7.2 Subtheme 2 - Information Security Training and Awareness.

Participant 3 of one of the companies within organisation stated that when new employees start their employment at the organisation they are required to attend a compulsory information security training session. At different intervals throughout the year workshops are held to educate and familiarize the staff with important current information security topics. When there are new security protocols and practises or changes to existing one the organisation runs internal advertising campaigns to raise awareness and understanding. The IT Security team also developed an internet website dedicated to information security practises that assisted people to use the internet in a safe and responsible manner (Participant 4).

4.7.3 Subtheme 3 - Passwords

Only users that have received departmental management approval are allowed to use their mobile devices to access the organisations mobile network and internet connection. There is a monthly charge against the business department for this mobile connectivity. Participant 10 said that when connecting to this mobility program users are forced to use a password on their devices with a minimum of four characters. Other employees not using this mobility program are also encouraged to do so for their own protection. To access services like email and IT systems the mobile user is required to use their network credentials. This network credentials need to be configured on the mobile devices of the user and updated by them each time their password changes on the network.

4.7.4 Subtheme 4 - Mobile Device Management

Many of the participants in this study were involved in the requirement analysis, evaluation of mobile device management (MDM) products on the market and were involved in the decision to purchase the MDM systems that the organisation currently uses. Participant 3, Participant 8, Participant 4 and others all emphasized the importance of the MDM solution that allows the organisation to administer mobile devices including smartphones and tablets. Some of the functions that were mentioned by participants included containerization where corporate data including emails and corporate applications and data were stored in a separate encrypted container on the users' mobile device. The other important feature is remote wiping capability that cleans all corporate information and personal data on mobile devices. In the event that a mobile device is lost or stolen the affected staff member needs to report this to their IT department immediately so that the information stored on it can be remotely wiped before sensitive data is leaked.

In BYOD literature MDM is listed as one of the best practises for BYOD management (Rouse, 2014; Mathias, 2015). This technology is implemented at Organisation X as stated by the participants above but this security technology is expensive.

4.7.5 Subtheme 5 - Secured Communications

Encryption technologies are used for communication between the mobile device and the organisation's network. This is accomplished via virtual private networking that allows all communication to be secured through the communication tunnel. All new laptops issued in the organisation have built-in encryption which helps if the device gets into the wrong hands then the information can't be accessed (Participant 4). Figure 8 illustrates the important factors for the successful management of BYOD within an organisation.

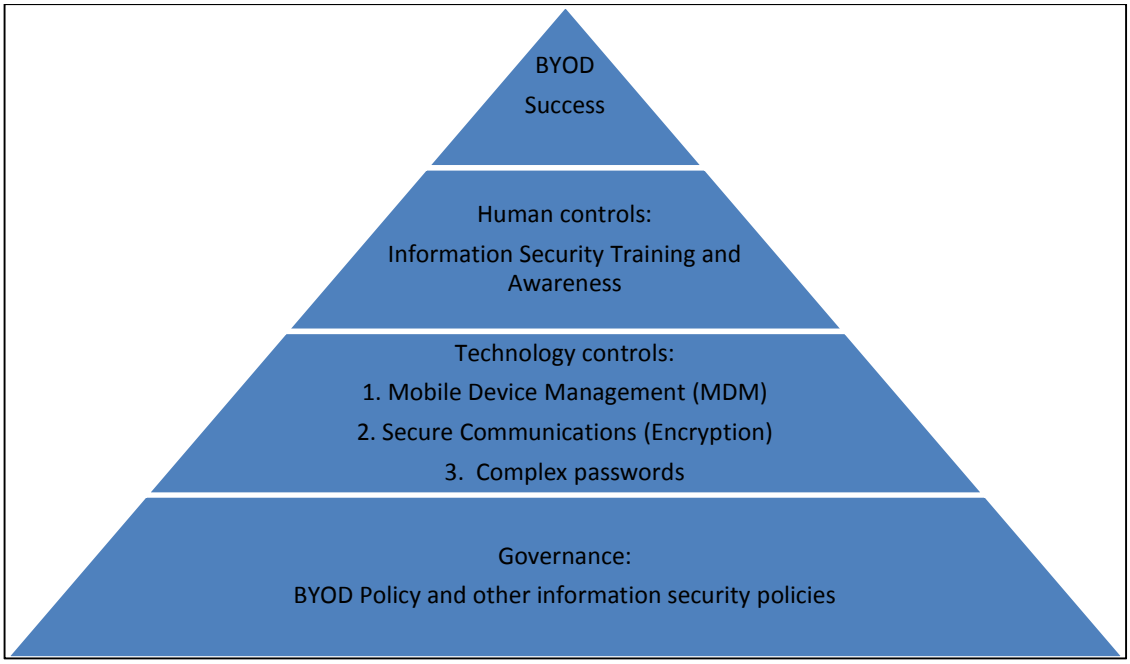

Figure 8. Important factors for the successful management of BYOD

4.7.6 Subtheme 6 - Support challenges for mobility

Participant 3 noted that with the addition of mobile devices in the organisation the requests for support have increased. The IT Helpdesk team prepared for the additional influx of requests for assistance by adding additional staff members. The team dealing

with these requests needed specific mobile experience and additional training to support the needs of the organisations mobile workforce.

4.7.7 Subtheme 7 - Complexity and compatibility

The mobile devices used by the users come in different brands and types making complexity a big issue for the organisation. Not all of the software developed in house is compatible for all the types of devices. The Participant 2 stated that it is very difficult to accommodate all the technology of the mobile devices within the business. For example when certain web applications are developed they do so for certain browsers and mobile operating systems. He also mentioned that a lot of complexity issues arise when going from one version of the software to the next.

4.7.8 Subtheme 8 - Security controls on mobile devices

The IT team responsible for the security controls set these controls to provide an adequate level of security for the users and the business without being too restrictive. All the IT participants agreed that if the security controls were too restrictive the employees would either not use the mobile services or try and find ways around the security so they needed to find the right balance.

When the user starts using the companies mobile program they are forced to use a four digit pin. The majority of the organisations users don't have any issues with this and other security controls. They understand that it is necessary to have this protection. There were a few participants that paid for their own mobile devices (BYOD) that felt entering the four digit pin each time they wanted to use their device was restrictive. For example when they needed to make a call quickly they needed to enter this pin code first (Participant 1 and Participant 11).

After the digital behaviour policy that included mobile device usage was issued by the business there were a number of users and business divisions that refused to sign the policy. Some of the reasons for this included disagreeing with some of the security controls and not understanding these controls. Some users were concerned that the IT team could see their personal information on their devices. After communicating to these users that the technology did not allow the IT team to see the user's personal information the user's signed the digital behaviour policy. Users that refused to sign and agree to the terms of the policy and mobile program simply would not be authorised to use the mobility program.

Table 8. Theme 6: Management of BYOD framework matrix

	Theme 6 : Management of BYOD
Participant 1	Sensitive data on mobile devices should be backed up in case the device is lost or stolen. If the mobile device is lost or stolen it should be remotely wiped.
Participant 2	We have the ability to wipe those devices and the organisation has a policy that guides the appropriate use of mobile devices. The users were educated and asked to sign off on the mobile device policy.
Participant 3	Mobile device management Password protection via pin. Policy.
Participant 4	The organisational rolled out the BYOD policy that guides users on how to use these mobile devices safely. Policy forces users to have 4 digit password on device. EMM enterprise mobile management. Containerization - that splits business and personal information on the mobile device.
Participant 5	I have ability to remotely wipe my devices if it is lost or stolen.
Participant 7	Password protection on devices and remote wipe.

Participant 9	Only authorised staff can receive approval to receive BYOD program access. All devices must have password.
Participant 10	Mobile device screens locks within a few minutes. The user needs to enter password to unlock each time. Policy guides users. Mobile device management Encryption Sandboxing - allows split of business and personal data.
Participant 11 and Participant 12	Encryption technology. BYOD and security policy. Remote wipe capability.
Participant 13	Usage Policies. Mobile device management. Educating and raising awareness amongst staff of the risks. Containerization of data separating corporate and personal data.
Participant 16	The organisation has an internet site dedicated to educating users about secure digital behaviour. The participant felt that If they were going to be successful they needed to assist users on how to be safe in their personal capacity not only when interfacing with the corporate systems. Policies help manage BYOD.
Researcher summary	Best practises for BYOD management include policy creation and enforcement, Information security training and awareness, Mobile Device management which includes remote wipe facilities. Password protection of devices should be compulsory.

4.8 Conceptual model for BYOD adoption

The conceptual model in Figure 9 below represents the findings of this study. This conceptual illustrates the benefits organisation X is receiving from the BYOD program and how the program is managed. The requirements are highlighted in blue, the themes are highlighted in turquoise and the subthemes are highlighted in pink.

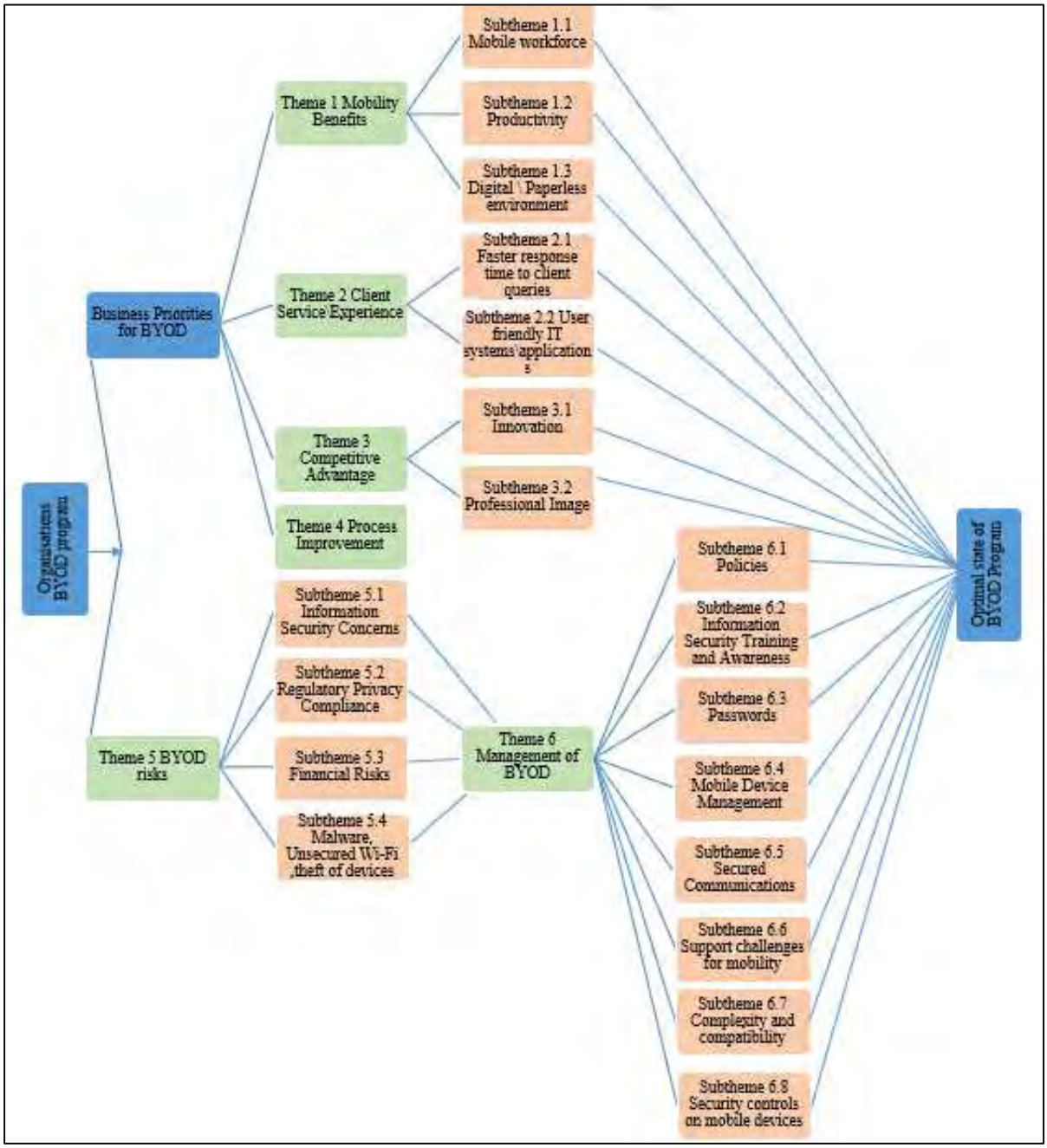

Figure 9. Conceptual model for BYOD adoption

Theme 1 - Mobility benefits is made up of Subtheme 1.1 - Mobile workforce, Subtheme 1.2 - Productivity and Subtheme 1.3 - Digital \ Paperless environment. There is a strong relationship between these three subthemes as mobility leads to an increase in

productivity of staff and mobility is only possible using a digital environment and technology (Wood, 2012).

Theme 2 - Client Service\Experience includes Subtheme 2.1 - Faster response time to client queries and Subtheme 2.2 - User friendly IT systems\applications. BYOD users are able to provide fast response to clients because the necessary information to easily accessible on their mobile devices. Organisations need to build its applications to make information more user friendly on mobile devices for their clients and staff (Hollingworth & Harvey-Price, 2013). A relationship exists between Theme 1 - Mobility and Theme 2 - client service\experience themes since the organisations' staff will not be able to provide a quality service to their clients without mobility.

Theme 3 - Competitive Advantage consists of Subtheme 3.1 – Innovation and Subtheme 3.2 - Professional Image. Without continuous innovation and enhancement of a business' products and services the business will not remain competitive in its industry (Sing, 2012). Theme 1 – Mobility is a driver of Competitive advantage. Subtheme 1 – Innovation is needed to create User friendly IT systems\applications – Theme 2.

Theme 4 - Process Improvement is one of the main benefits experienced by companies that have adopted BYOD (Mcafee and Brynjolfsson, 2008; Dell, 2015). When businesses processes improve by way of BYOD this has a positive effect on Subtheme 1.2 - Productivity and Theme 2 - Client Service\Experience.

The introduction of the BYOD program and the priorities in Themes 1-4 also introduces risks in Theme 5 to the organisation.

The implementation and effective execution of Theme 6 - Management of BYOD minimizes Theme 5 - BYOD risks. If these BYOD risks in Theme 5 are not successfully managed it has a negative effect on Themes 1 - 4 and their Subthemes. The negative effects include information loss, financial loss and reputational damage to organisations. On the other hand organisations that manage BYOD risks experience the benefits of a BYOD program which leads to organisational growth in terms of satisfied customers and increased revenue.

5. Conclusion

Securing the information assets of an organisation has always been a concern for all stakeholders, but it has become a top priority in recent times, with many companies falling victim to data breaches and experiencing loss of sensitive information. BYOD programs have made it even harder for companies to protect their information assets. The aim of this study was to provide insight into the business priorities that drive BYOD adoption and to investigate the how the organisation is dealing with the challenges that is associated with BYOD. A literature review was conducted to understand the various benefits that BYOD provides organisations, the risks BYOD introduces to businesses and how these risks are managed. Qualitative data was collected by means of semi-structured interviews to provide the answers to the research questions.

5.1 Primary Research Question Revisited

The primary research question was: *How do business priorities drive the adoption of BYOD in the organisation?* The concept of BYOD started when consumerisation of IT began. Consumers started bringing their own devices into the workplace and wanted to use their devices for work purposes. Rather than resist the trend Organisation X decided to develop strategies that would allow the organisation to benefit from this. The data from the interviews show that the factors that contribute to the adoption of the BYOD program are mobility, client service improvement, competitive advantage, and process improvement.

In order for the organisations mobile workforce to be productive while they were seeing clients or traveling the organisation needed to create systems and strategies to allow these users to connect to the corporate systems securely. The Organisation X has seen significant increase in mobile workers productivity. A surprise finding was the amount of after-hours work that mobile users were completing. BYOD enabled the mobile workers

to provide better service to their clients because they were able to respond to queries much faster.

The organisation used technology which included BYOD and its innovative mobile platforms to create a competitive advantage over other competitors in the market. The organisation was able to use the digital capabilities of BYOD to improve certain processes which included allowing clients to fill in digital forms for faster processing and storage. Finding customer information was found to be much easier in the paperless environment compared to the old filing cabinets used in the past.

A practical implication for organisations that are considering introducing, or not realising the benefits of, BYOD is that they need to clearly understand and work towards the reasons they want BYOD in their organisations.

5.2 Secondary Research Question Revisited

The secondary research question was: *How are the benefits, risks and costs of implementing and managing a BYOD program realised by the organisation?* Organisation X was able to recognise the potential benefits BYOD can provide early as the consumerisation trend was beginning to take off. This early awareness also stood the organisation in good stead when it came to planning the architecture which would allow the mobile connectivity. BYOD has allowed the organisation to access rural markets where they were previously not able to by allowing mobile staff members to access clients in these regions. As productivity increases so does the revenue of businesses. In the literature productivity is stated as one of the main benefits of BYOD and this is true in the experience of the case organisation (Forrester, 2011; Wood, 2012; Calder, 2013).

The introduction of BYOD has improved many business processes including allowing the financial advisor to visit clients and assist them with financial planning. When the clients have decided on a product or service they are able to digitally sign documents\contracts

and this is then processed in the organisations back office. The financial advisors are also able to track the clients request on the workflow systems via their mobile devices. Having digitally stored documentation has made it much easier for staff to find information and help the clients. Less printed paper copies aids in the organisations overall green strategy to limit its carbon footprint.

The findings show that setting up the IT infrastructure for BYOD is very costly for organisations. These costs, which are not often mentioned in literature, include the connectivity, security, IT support and development costs for mobile platforms.

The major concern that organisations have with BYOD is the possible loss of sensitive information located on the mobile devices and protecting their information assets is a high priority. To ensure that these information assets are protected a combination of technical and human controls are a necessity. Firstly the organisation needs to create appropriate information security and BYOD policies that govern the use of mobile devices and the organisations IT systems and the appropriate use and processing of sensitive organisational data. It is important that the staff understand these policies, accept consequences of being in contravention of the policy and sign off that they agree with the terms. The organisation needs to establish which security systems will be appropriate for the organisation's needs.

Findings in the literature and in the empirical research suggest organisations incorporate enterprise mobility management solutions that include mobile device management (Ghosh et al., 2013; Pinchot & Paullet, 2015). Here functions like remote wipe of the information stored on lost devices are some of the important functions. On the non-technical side the organisations need to provide the staff with training and awareness to educate them on safe cyber behaviour that will limit threats. Having IT professionals with the right amount of skill and experience is key to a successful BYOD program.

5.3 Contribution of this research

This study makes an academic and practical contribution to the body of knowledge for BYOD.

The theoretical contribution of this study is the conceptual model representing the factors that affect BYOD adoption. This conceptual model can be used by academics to understand BYOD usage in organisations. The conceptual model can be further developed in other empirical studies with different criteria. This research highlighted that Organisation X as well as other organisations can use BYOD to improve client service, gain competitive advantage and improve their processes using their digital devices and backend systems.

A limited number of studies on BYOD have been conducted in South Africa. This research extends this body of knowledge by capturing Organisation X's experience with BYOD including the benefits they are deriving from their BYOD program and how they are dealing with the threats. Recommendations of how organisations implement and manage their BYOD program was also suggested.

There has been a high mobile penetration rate and broadband usage has recently overtaken fixed line internet usage. The factors that affect BYOD usage in South African differ from the more developed North American and European countries. Barriers that affect Internet usage in Africa and specifically South Africa include poor fixed line infrastructure and high telecommunications fees. BYOD can be used by organisations to access clients living in rural parts of the country and the African continent.

A practical contribution of this research is to show organisations considering adopting a BYOD program the benefits achieved by Organisation X and also how the risks are managed. Organisations that are considering introducing, or not realising the benefits of, BYOD need to clearly understand the reasons they want to introduce BYOD in their organisations. This information can be used to build a business case for the new BYOD program, gain top management support for the program and to receive buy in from the

relevant stakeholders. The conceptual model can be applied by practitioners in their organisations to achieve their business objectives.

5.4 Limitations

The study was conducted within one large financial services organisation and the empirical data is from this organisation's perspective. Research from other organisations in a different industry may yield different results. In addition, small to medium organisations might have different criteria for choosing BYOD leading to different findings.

This study mainly considered the organisations perspective on BYOD but gaining the end-users' perspective might introduce different factors. Eisenhardt (1989) was of the opinion that if the population was suitable it aids in generalisation. The researcher chose purposive sampling to select the participants of the study that would be best suited to answer the questions that was under investigation. Whether the results of the study is transferable should be tested with a larger sample.

5.5 Future research

Future research can be conducted from multiple case sites to determine if new factors can be identified that can assist organisations. Research within multiple case sites could also highlight differences between those sites. This research was conducted in a financial services organisation and further research can be conducted in other industries which could introduce other elements that might not have been covered in this study.

Future research could question whether BYOD does provide cost savings for the organisation because the practical implementation and management is expensive. Understanding the financial impact of adopting and maintaining the BYOD program will

aid decision makers of the organisation to determine whether the BYOD program is worth the risks and financial costs.

Future research can also examine how BYOD risk assessments are completed and who signs off on this risk. Completing the risk assessment will enable the organisation to identify possible risks, who or what might be affected, what level of risk will be acceptable, appropriate actions to limit the risks and who is responsible to carry out actions. This research could be extended to explore how to effectively manage the risks that were identified.

References

Akbari, H., & Land, F. (2005). *Theories Used in IS Research: Socio-Technical Theory*. Retrieved March 18, 2014, from http://www.istheory.yorku.ca/sociotechnicaltheory.htm

Albrechtsen, E. (2007). A qualitative study of users' view of information security, *Computers & Security*, 26(4), 276-289.

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computer Fraud & Security*, Volume 2012, (9), 8-14.

Ali, M., & Brooks, L. (2008). *Culture and IS. National Cultural Dimensions Within IS Discipline*. Proceedings of the 13th Annual Conference of the UK Academy for Information Systems, Bournemouth, United Kingdom, 1-14.

Anderson, C. L., &. Agarwal, R. (2010). Practising safe computing: A multimethod empirical examination of home computer user security behavioural intentions. *MIS Quarterly*, 34(3): 613–643.

Anderson, N., (2013). Cisco Bring Your Own Device - Device Freedom Without Compromising the IT Network, s.l.: CISCO.

Bartunek, J. M., & Louis, M. R. (1996). *Insider/outsider team research*. Thousand Oaks, CA: Sage.

Baskerville, R. (2011). Individual Information Systems as a Research Arena. *European Journal of Information Systems*, 20(3), 251-254.

Basole, R.C. (2007). The Emergence of the Mobile Enterprise: A Value-Driven Perspective. Retrieved March 1, 2015, from: http://www.ti.gatech.edu/basole/docs/Basole.ICMB2007.MobileEnterprise.pdf

Basole, R.C., & Rouse, W.B. (2007) *Mobile Enterprise Readiness and Transformation*. Retrieved June 19, 2015, from http://ti.gatech.edu/basole/docs/BasoleRouse.MobileReadiness.2007.pdf

Bauer, R.A. (1967). *Consumer Behaviour as Risk Taking. In Risk Taking and Information Handling in Consumer Behaviour*. D.F. Cox Ed., pp. 23-33, Harvard University Press, Cambridge, USA.

Beach, L.R. (1993). *Making the right decision. Organizational culture, vision and planning*. Eaglewood Cliffs, New Jersey: Prentice Hall.

Bostrom, R. P., & Heinen, J. S. (1977). MIS Problems and Failures: A Socio-Technical Perspective PART II: The Application of Socio-Technical Theory. *MIS Quarterly* 1(4), 11–28.

Botha, R. A., Furnell, S. M., & Clarke, N. L. (2009). From Desktop to Mobile: Examining the Security Experience. *Computers & Security*, 28(3-4), 130–137.

Braun, V. & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3, 77-101.

Brodin, M., Rose, J., & Ahlfeldt, R, M. (2015). Management issues for bring your own device. *European, Mediterranean & Middle Eastern Conference on Information Systems 2015*. Retrieved July 17, 2015, from http://www.researchgate.net/profile/Martin_Brodin/publication/277007698_Management_issues_for_Bring_Your_Own_Device/links/55704fb708aec226830aeaa3.pdf.

Calder. (2013). Is the BYOD Movement Worth the Risks? *Credit Control*, 34 (3), 65-70.

Cavana, R., Delahaye, B. L., & Sekaran, U. (2001). *Applied Business Research: Qualitative and Quantitative Methods*. Australia: John Wiley.

Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. (2004). Economics of IT Security Management: Four Improvements to Current Security Practices. *Communications of the Association for Information Systems* (14), 65-75.

Cavusoglu, H., Cavusoglu, H., Son, J.-Y., & Benbasat, I. (2009). *Information Security Control Resources in Organizations: A Multidimensional View and Their Key Drivers*. Working paper. Sauder School of Business, University of British Columbia.

Chen, L., & Nath, R. (2011). Impediments to mobile work: an empirical study. *International Journal of Mobile Communications*, 9(5), 522-540.

CISCO. (2013). *Cisco Connected World—International Mobile Security: Survey Research Highlights and Considerations for Enterprise IT*, s.l.: s.n.

Citrix. (2011). *IT Organisations Embrace Bring-Your-Own-Devices*. Fort Lauderdale: Citrix. Retrieved June 30, 2014, from http://www.citrix.com/go/lp/pgm/byoindex2011.

Conlin, M. (2006). Smashing the Clock. *BusinessWeek*, 60–68.

Couldwell, C. (2011). Technology is helping SMBs to become a global force. *The Wall Street Journal*. Retrieved November 10, 2015 from http://online.wsj.com/ad/article/execdigest-technology

Couture, E. (2010). *Mobile Security: Current Threats and Emerging Protective Measures*. SANS Institute InfoSec Reading Room. Retrieved August 18, 2014, from http://www.sans.org/reading_room/whitepapers/incident/wireless-mobile-security_33548

Creswell, J. W. (2009). *Research Design: Qualitative, Quantitative, and Mixed Method Approaches (3rd Ed.)*. Thousand Oaks: Sage Publications Inc.

Crossler, R. E. (2010). Protection motivation theory: Understanding determinants to backing up personal data. Paper read at 43rd Hawaii International Conference on System Sciences (HICSS) (January 5–8). Retrieved April 25, 2015, from http://www.computer.org/csdl/proceedings/hicss/2010/3869/00/07-03-04-abs.html

Crossler, R. E., A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, & R. Baskerville. (2013). Future directions for behavioural information security research. *Computers and Security 32* (1): 90–101.

Crotty, M. (1998). *The foundations of social research: Meaning and perspective in the research process*. Thousand Oaks, CA: Sage.

Darke, P.; Shanks, G. & Broadbent, M. (1998). Successfully Completing Case Study Research: Combining Rigour, Relevance and Pragmatism. *Information Systems Journal* (8), 273 – 289

Dell. (2015). *Dell Study Reveals Companies Investing in Cloud, Mobility, Security and Big Data Are Growing More Than 50 Percent Faster Than Laggards*. Retrieved January 19, 2016 from http://www.dell.com/learn/us/en/vn/press-releases/2015-10-13-dell-global-technology-adoption-index

Dell and Intel. (2011). *The Evolving Workforce: Expert Insights*. Round Rock, Texas, USA.

Denzin, N. K., & Lincoln, Y. S. (2000). *'Introduction: The discipline and practice of qualitative research'*, in N.K. Denzin & Y.S. Lincoln (eds.), Handbook of qualitative research, 1-29. Second Edition. California: Sage Publications, Thousand Oaks

Disabato, M. (2015). How to Create a Mobile Strategy. *Gartner Catalyst Conference*. San Diego.

Drew, J. (2012). Managing Cybersecurity Risks. *Journal of Accountancy*, 8, 44-48.

Easterby-Smith, M., Thorpe, R., Jackson, P., & Lowe, A. (2008). *Management Research*. 3rd Edition. London: Sage.

Eisenhardt, K.M. (1989). Building Theories from Case Study Research, *Academy of Management Review*, 14(N/A), 532-550.

Ernst & Young. (2008). *Moving Beyond Compliance: Ernst & Young's 2008 Global Information Security Survey*. Retrieved August 19, 2014 from https://www.eycom.ch/publications/items/giss_2008/2008_EY_GISS.pdf

Ernst & Young (2011). Into the Cloud, Out of the Fog - Ernst & Young's 2011 Global Information Security Survey. Retrieved February 21, 2013, from

http://www.de.ey.com/GL/en/Services/Advisory/2011-Global-Information-Security-Survey---Seeing-through-the-cloud

Featherman, M.S., & Pavlou, P.A. (2003). Predicting E-Services Adoption: A Perceived Risk Facets Perspective. *International Journal of Human-Computer Studies*, 59 451-474.

Floyd, D. L., Prentice-Dunn S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology,* 30(2): 407–429.

Forrester (2011). *IT Managers Selectively Embrace Consumerization*. Cambridge: Forester Research Inc. Retrieved May 20, 2014, from http://download.microsoft.com/download/B/3/A/B3ABAFBF-B96E-496A-8A96-51EAE5091C07/IT%20Managers%20Selectively%20Embrace%20Consumerization_FINAL%2002172011.pdf.

Forrester. (2012). *Mobile Is The New Face Of Engagemen*t. Retrieved January 7, 2016, from https://www.forrester.com/Mobile+Is+The+New+Face+Of+Engagement/fulltext/-/E-RES60544

Gartner. (2012a). *Gartner Executive Programs' Worldwide Survey of More Than 2,300 CIOs Shows Flat IT Budgets in 2012, but IT Organizations Must Deliver on Multiple Priorities*. Retrieved June 21, 2015 from http://www.gartner.com/newsroom/id/1897514

Gartner. (2012b). *Gartner Says the Personal Cloud Will Replace the Personal Computer as the Center of Users' Digital Lives by 2014*. Retrieved June 15, 2014 from http://www.gartner.com/newsroom/id/1947315.

Gartner. (2013). *Gartner Says Worldwide PC, Tablet and Mobile Phone Combined Shipments to Reach 2.4 Billion Units in 2013*. Retrieved April 5, 2014 from http://www.gartner.com/newsroom/id/2408515

Gartner. (2014). *Gartner Says 75 Percent of Mobile Security Breaches Will Be the Result of Mobile Application Misconfiguration*. Retrieved December 05, 2015, from http://www.gartner.com/newsroom/id/2753017

Gartner. (2015). *CIOs name BI and analytics No. 1 investment priority for 2015*. Retrieved January 07, 2016, from http://gartnerevent.com/NABI13Survey

Glesne, C. (2011). *Becoming Qualitative Researchers: An Introduction*. Fourth Edition. Pearson.

Ghoda, A. (2009). *Pro Silverlight for the Enterprise*, pp. 249-266, New York: Apress.

Ghosh, A., Gajar, P. K., & Rai, S. (2013). Bring Your Own Device (BYOD): Security Risks and Mitigating Strategies. *Journal of Global Research in Computer Science* (4:4), 62-70.

Hagen, J., Albrechtsen, E., & Johnsen, S. O. (2011). The long-term effects of information security e-learning on organisational learning. Information Management & Computer Security, 19(3), 140-154.

Hannam, K., Sheller, M., & Urry, J. (2006). Editorial: Mobilities, Immobilities and Moorings. *Mobilities*, 1(1), 1–22.

Harley, L. (2013). *The Consumerization of IT and Bring Your Own Device*. Retrieved March 1, 2014, from http://www.hrtalentmanagement.com/2013/12/09/the-consumerization-of-it-and-bring-your-own-device/

Hartzel, K., Craig, D., Ngirimana, E, N., Alhaiki, Z., Evans, B., Civitarese, F., Galucci, A., & Shitemi, M. (2013). A study of BYOD and its implementation in real world cases. *Northeastern Association Of Business, Economics and Technology*. Retrieved March 1, 2014, from http://www.nabet.us/proceedings-archive/NABET-Proceedings-2013.pdf.

Hirschheim, R., & Klein, H,K. (1994). Realizing emancipatory principles in information systems development: The case for ethics. *MIS Quarterly*, 18(1), 83-109.

Hollingworth, L., & Harvey-Price, A. (2013). *Technology and skills in the digital industries*. E-skills UK. Retrieved November 5, 2015, from www.gov.uk/government/uploads/system/uploads/attachment_data/file/305376/evidence-report-73-technology-skills-digital-industries.pdf

IBM, (2011). *The New Workplace: Supporting "Bring your own*", s.l.: IBM.

IBM, (2012). *Securing end-user mobile devices in the enterprise*, s.l.: s.n.

ISACA. (2008). Glossary of terms, 2008. Retrieved 02 July 2014 from http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf

Jacoby .J., & Kaplan ,L. B. (1972). The components of perceived risk. In: Venkatesan M, editor. *Advances in consumer research*. Chicago: Association for Consumer Research.

Jones, C. (2013). *Google Play Catching Up To Apple's App Store*. Forbes. Retrieved May 25, 2014 from http://www.forbes.com/sites/chuckjones/2013/12/19/google-play-catching-up-to-apples-app-store/

Kaneshige, T. (2012). ComputerWorld UK BYOD - *Five hidden costs to a bring-your-own-device programme*. Retrieved January 5, 2016 from http://www.computerworlduk.com/in-depth/mobilewireless/3349518/byod--five-hidden-costs-to-a-bring-your-own-device-progamme/

Kaplan ,L. B., Szybille ,George, & Jacoby, J. (1974). Components of perceived risk in product purchase: a cross validation. *Journal of Applied Psychology*. 59(3), 278–91.

Kaspersky, (2012). *Security Technologies for Mobile and BYOD.* s.l.: s.n.

King, R. (2012). Forrester: 53% of employees use their own devices for work. Retrieved May 21, 2014 from http://www.zdnet.com/article/forrester-53-of-employees-use-their-own-devices-for-work/

Klein, H. K., & Myers, M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *Management Information Systems Quarterly*, 23(1), 67-88.

Kolkowska, E., & Dhillon, G. (2013). Organisational Power and Information Security Rule Complinace. *Computers and Security*. 33:3-11.

Kornak, A., Teutloff, J., & Welin-Berger, M. (2004). *Enterprise guide to gaining business value from mobile technologies*. New York: Wiley.

Landman, M. (2010). Managing Smartphones Security Risks. *Information Security Curriculum Development Conference*, 145-155

Lee, M. C. (2008). Predicting behavioral intention to use online banking. *Proceedings of the 19th International Conference on Information Management*. Taiwan.

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems,* 18(2), 177–187.

Leidner, D.E., & Kayworth, T. (2006). Review: A review of Culture in Information Research. Towards a Theory of Information Security Culture Conflict. *MIS Quarterly*. 30(2), 357-99.

Lewins, A., & Silver, C. (2009). Choosing a CAQDAS package. CAQDAS Networking Project and Qualitative Innovations in CAQDAS Project. (QUIC). Retrieved November 03, 2015 from http://eprints.ncrm.ac.uk/791/1/2009ChoosingaCAQDASPackage.pdf

Liljander, V., & Strandvik, T. (1992). Estimating Zones of Tolerance in Perceived Service Quality and Perceived Service Value. *International Journal of Service Industry Management*, 4(2): 6-28

Liu, Y., Yang, Y., & Li, H. (2012). *A Unified Risk-Benefit Analysis Framework for Investigating Mobile Payment Adoption*. International Conference on Mobile Business.

Lohmeyer, D. F., McCrory, J., & Pogreb, S. (2002). Managing Information Security. *The McKinsey Quarterly, Special Edition: Risk and Resilience* (2), 12-16.

Mansfield-Devine, S. (2012). 'Interview: BYOD and the enterprise network'. *Computer Fraud & Security*, vol.2012, 4, 14-17

Mathias, C. (2012). *Enterprise mobility management options: MDM, MAM and MIM*. Retrieved January 25, 2015 from http://searchmobilecomputing.techtarget.com/tip/Enterprise-mobility-management-options-MDM-MAM-and-MIM.

McAfee. (2012). Putting IT Back in Control of BYOD. *Osterman Research Inc*. USA

Moir, R. (2009). "*Defining Malware: FAQ*". Technet.microsoft.com. Retrieved July 5, 2014, from http://technet.microsoft.com/en-us/library/dd632948.aspx

Morrow, B. (2012). 'BYOD security challenges: control and protect your most sensitive data', *Network Security*, 12, 5-8.

Moschella, D., Neal, D., Opperman, P., & Taylor, J. (2004). *The Consumerization of Information Technology*. El Segundo, California, USA: CSC.

Myers, Michael. (1997). Qualitative Research in Information Systems. *MIS Quarterly*, 21: 2.

Myers, M. D. (2009). *Qualitative Research in Business & Management*. Los Angeles: SAGE.

Oates, B. J. (2006). *Researching Information Systems and Computing*. London: Sage.

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information Systems Research Journal*, 2(1), 1-28.

Patton, M.Q. (1990). *Qualitative evaluation and research methods*. 2nd Edition. Newbury Park, CA: Sage.

Pieterse, I. (2014). *BYOD – It's about more than just security*. Iweek. Retrieved July 24, 2014 from http://www.iweek.co.za/special-report/byod-it-s-about-more-than-just-security

Pinchot, J., & Paullet, K. (2015). Bring Your Own Device to Work: Benefits, Security Risks and Governance Issues. *Issues in Information Systems*, 16(3), 238-244

Ponemon Institute LLC. (2012). *Global Study on Mobility Risks*, s.l.: s.n.

Post, G.V., Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security*, 26(3), 229–237.

Purser, S. (2002). Why access control is difficult. *Computers & Security*, 21(4), 303-309.

QSR International. (2016). QSR - NVivo Data Analysis Software | QSR International. Retrieved March 15, 2015, from http://www.qsrinternational.com/

Rains, J. (2012). *Bring Your Own Device (BYOD): Hot or Not?* United Business Media, London.

Ransbotham, S., & Mitra, S. (2009). Choice and Chance: A Conceptual Model of Paths to Information Security Compromise, *Information Systems Research* 20(1), 121-139.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology: Interdisciplinary and Applied*, 91(1), 93–114.

Rose, C. (2013). BYOD: An examination of Bring Your Own Device in Business. *Review of Business Information Systems*, 17(2), 65-70.

Roselius T. (1971). Consumer rankings of risk reduction methods. *Journal of Marketing*. 35(1), 56–61.

Rouse, M. (2014). *Mobile Application Management*. Retrieved March 15, 2015, from http://searchmobilecomputing.techtarget.com/definition/mobile-application-management-MAM.

Rouse, W.B., & Baba, M.L. (2006). Enterprise Transformation. *Communications of the ACM*, 49(7), 67–72.

Ruggiero, P., & Foote, J. (2011). Cyber Threats to Mobile Phones, US-CERT United States Computer Emergency Readiness Team, 2011 Carnegie Mellon University, Produced for US-CERT.

Saunders, M., Lewis, P., & Thornhill, A. (2009) *Research methods for business students*, 5th ed., Harlow, Pearson Education.

SC Magazine. (2012). "BYOD: OMG! Or A-OK?" *Haymarket Business Publications*, 18-23.

Schein, EH. (1999). *The corporate culture survival guide*. Jossey-Bass Inc.

Schlienger, T., & Teufel, S. (2003). Information security culture – from analysis to change. *South African Computer Journal*.

Seybold, A.M. (2008). The Convergence of Wireless, Mobile, and the Internet and its Relevance to Enterprises. *Information Knowledge Systems Management*, 7, 11–23.

Siponen, M. T. (2000). A conceptual foundation for organisational information security awareness, *Information Management & Computer Security*, 8(1), 31-41.

Singh N. (2012). B.Y.O.D. Genie Is Out Of the Bottle – "Devil Or Angel". *Journal of Business. Management & Social Sciences Research* (JBM&SSR), 1(3), 3 - 4, 8, 10-12.

Smit, P.J., & Cronje, G.J. (1992). Management Principles: A Contemporary South African Edition. Juta.

Stahl, B.C. (2008). *Iriformation Systems: Critical Perspectives*. New York: Routledge

Stone R. N., & Gronhaug K. (1993). Perceived risk: Further consideration for the marketing discipline. *European Journal of Marketing*, 27(3), 39- 50.

Takesue, M. (2007). *Emerging Security Information, Systems, and Technologies*. SecureWare.

Takeuchi, L. (2011) *Families matter: Designing media for a digital age*. New York: The Joan Ganz Cooney Center at Sesame Workshop. Retrieved October 23, 2014, from http://joanganzcooneycenter.org/upload_kits/jgcc_familiesmatter.pdf

Taylor, B,. Kermode, S., & Roberts, K. (2007). *Research in nursing and health care: evidence for practice*, 3rd edn, Thompson, Australia.

Terre Blanche, M., & Durrheim, K. (1999). *Research in practice*. Cape Town: University of Cape Town Press.

Thomson, K.-L., von Solms, R., & Louw, L. (2006). *Cultivating an organizational information security culture*. Centre for Information Security Studies, Nelson Mandela Metropolitan University, South Africa.

Tzoumas, C. (2013). The BYOD World. *BusinessWest*. 30, 45.

Unhelkar, B., & Murugesan, S. The Enterprise Mobile Applications Development Framework, *IT Professional.* 12(3), 121-133.

Venkatesh, V., Morris, M., Davis, G., & Davis, F. (2003). User acceptance of information technology: toward a unified view. *MIS Quarterly*, 27(3), 425-478.

Weiß, F., & Leimeister, J. (2012). Consumerization - It Innovations from the Consumer Market as a Challenge for Corporate It. *Business & Information Systems Engineering*, 54 (6), 363-366.

Whitman, M. E., & Mattord, H. J. (2004). *Management of Information Security*. Thompson Course Technology

Wood, A. (2012). 'BYOD: The Pros and Cons for End Users and the Business', *Credit control*, 33(7/8), 68-70

Yadav, S., Ganguly, U., Suman, S., & Puri, P. (2015). Threats and Vulnerabilities of BYOD and Android. *International Journal of Research*. 2(8)

Yin, R. K. (1994).*Case study research: Design and methods*. Thousand Oaks, CA: Sage.

Zielinski, D. (2012). Bring your own device. *HR Magazine-Alexandria*, 57(2), 71–74.

Zikmund, W. G. (2000). *Exploring marketing research*. Fort Worth: Dryden Press.

Appendix A - Interview Guide

Exploring the utility benefits and risks that BYOD create within an organisation.

Management

1. Before launching the BYOD program what utility benefits did the organisation envision?
2. Now that the BYOD program is operational have these utility benefits been realised? If not, why?
3. What risks (costs) has the organisation experienced since using the BYOD program?
4. How has the organisation dealt with these risks?
5. What best practises for managing BYOD have emerged?

General Use \ Utility benefits - Users

6. What were your reasons for wanting to participate in the BYOD program?
7. Which work aspects does BYOD assist with most?
8. Which other positive aspects has your participation in BYOD led to?

Risks and other challenges - Users

9. What are the risks that you experience with BYOD eg. Financial, performance, reputational damage, security, privacy?
10. As a BYOD user how do you feel about your device being monitored in terms of the personal information that is stored on it?
11. How restrictive are the security controls set to your device by the organisation, towards personal tasks that you use your device for?

Concluding questions for organisation and users.

12. What factors beyond utility and risk affected the BYOD decision?
13. Can you make any recommendations on how to increase the utility while minimizing the risks of BYOD to the user and organisation?
14. How important is BYOD within the modern organisation?
15. What role does BYOD have in the South African economic environment?

Appendix B – Codebook

Name	Number Of Sources Coded	Hierarchical Name
reasons for participation	12	Nodes\\reasons for participation
Utility Benefits	12	Nodes\\Utility Benefits
Risks (costs) organisation	11	Nodes\\Risks (costs) organisation
management of risks	10	Nodes\\management of risks
Realised Benefits	10	Nodes\\Realised Benefits
BYOD and modern organisation	8	Nodes\\BYOD and modern organisation
factors beyond utility benefit and risks	8	Nodes\\factors beyond utility benefit and risks
Risks (Users)	8	Nodes\\Risks (Users)
best practises	7	Nodes\\best practises
BYOD and economy	7	Nodes\\BYOD and economy
Improved Customer Service	7	Nodes\\Improved Customer Service
Mobility	7	Nodes\\Mobility
BYOD assisted most with	6	Nodes\\BYOD assisted most with
BYOD challenges	6	Nodes\\BYOD challenges
monitoring usage	5	Nodes\\monitoring usage
Organisation objectives	5	Nodes\\Organisation objectives
competitive advantage	4	Nodes\\competitive advantage
mobility requirements	3	Nodes\\mobility requirements
Professional image	3	Nodes\\Professional image
possible risks not yet experienced	3	Nodes\\possible risks not yet experienced
Ranking of mobility - BYOD risks	3	Nodes\\Ranking of mobility - BYOD risks