A FRAMEWORK FOR ENHANCING CORPORATE DATA SECURITY IN A BRING YOUR OWN DEVICE (BYOD) ENVIRONMENT: A CASE OF GOVERNMENT ORGANIZATIONS IN KENYA.

BY

GEOFFREY K. SOWEK

MASTER OF SCIENCE IN DATA COMMUNICATIONS

KCA UNIVERSITY

2018

A FRAMEWORK FOR ENHANCING CORPORATE DATA SECURITY IN A BRING YOUR OWN DEVICE (BYOD) ENVIRONMENT: A CASE OF GOVERNMENT ORGANIZATIONS IN KENYA.

GEOFFREY K. SOWEK

13/03426

SUPERVISOR: DR. LUCY MBURU

THIS DISSERTATION IS SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTERS OF SCIENCE IN DATA COMMUNICATIONS IN THE FACULTY OF COMPUTING AND INFORMATION MANAGEMENT AT KCA UNIVERSITY

OCTOBER, 2018

DECLARATION

I declare that this dissertation is my original work and has not been previously published or submitted elsewhere for award of a degree. I also declare that this contains no material written or published by other people except where due reference is made and author duly acknowledged.

Student Name: **SOWEK GEOFFREY KIPKEMOI** Reg. No: **13/03426**

Sign: _____ Date: _____

I do hereby confirm that I have examined the master's dissertation of

SOWEK GEOFFREY KIPKEMOI,

And have approved it for examination.

Sign: _____ Date: _____

DR. LUCY MBURU

Dissertation Supervisor

ABSTRACT

Information and Communication Technology (ICT) has become an integral part of the lives of many people today. In the business scene, ICT has been embedded into the fabric of many organizations. The modern business environment is highly dynamic and is characterized by increased competition and changing employee and customer demands. Emerging technologies such as Cloud Computing, Mobile Computing and Bring Your Own Device (BYOD) have shifted the trajectory of how Information Technology (IT) is consumed. This shift has resulted in a phenomenon referred to as IT Consumerization. Proliferation of mobile devices such as smart phones and tablets has led to a notable shift in the way organizational resources are accessed by employees. Organizations are now adopting BYOD which allows employees to use their personal devices to access sensitive organizational data both within the organization and remotely. The greater capability and flexibility that these cutting-edge devices offer make them popular among many employees especially the younger generation. Adoption of BYOD by organizations presents various benefits such as increased employee productivity, better customer service and increased efficiency. Government agencies in Kenya are increasingly adopting the BYOD concept in line with the Government's digitization program aimed at increasing efficiency of Government services and as a cost-cutting measure. However, the biggest challenge to successful adoption is the security of sensitive data. BYOD adoption presents data security risks such as loss of data, data leakages, distributed denial of service (DDoS), malware and other vulnerabilities. Various Government agencies have in the recent past experienced cyber-attacks from criminals targeting sensitive and confidential information stored by these agencies. Recent cyber security reports have also identified Government agencies as the most vulnerable organizations in terms of cyber security risk. Despite the increased security risks brought about by BYOD adoption, Government organizations continue to implement traditional security frameworks which may not address the unique vulnerabilities brought about by BYOD. It is therefore important to identify the specific risks and challenges facing BYOD adoption in Government organizations and to review the frameworks that have been put in place by these organizations to address these challenges. The study identified these challenges, reviewed the effectiveness of the existing frameworks and developed an enhanced holistic framework that would ensure secure BYOD adoption. This would enable the organizations to enjoy the benefits of BYOD while at the same time ensuring that the security of sensitive data is not compromised. The target population for this study was the ICT experts, administrators, or managers in 90 government agencies in Kenya. The study results would be useful to government organizations including the Ministry of ICT and other policy makers and IT professionals because it pointed out the specific issues or risks facing BYOD adoption in Government and recommended possible solutions to these challenges through a multi-layered security framework.

Key words: *BYOD, Mobile Virtualization, IT Consumerization*

ACKNOWLEDGEMENTS

I am truly grateful to the Almighty God for His sufficient grace and this far He brought me.

I am grateful to my supervisor Dr. Lucy Mburu for her fruitful guidance and support to this successful project completion. Her precious contribution made it possible for me to achieve the objectives set out the commencement of this Project. May the Lord keep on enlarging her territories.

I thank my dearest wife Janet Chepkorir and our lovely kids Claire, Ryan and Ethan for their patience and encouragement throughout the time I was engaged in this project. Your understanding and moral support gave me the strength and energy to complete this project. May our Lord the Almighty bless you abundantly.

To my classmates and panelists, your critiques and comments were awesome. I say thank you very much

Above all I sincerely thank the Lord for giving me the room and capability to work on this project. May your holy name be forever glorified.

DEDICATION

I dedicate this dissertation to my wife and family members. Your prayers and support during the time of doing this research brought me to this moment and to my supervisor, Dr. Lucy Mburu and faculty panels, friends and classmates who have given me full support to engage this work.

ACRONYMS AND ABBREVIATIONS

AAC	Access Application Control
AUP	Acceptable Use Policy
BYOD :	Bring Your Own Device
DDos	Distributed Denial of Service
DoS	Denial of Service
ERP	Enterprise Resource Planning System
IAM	Identity and Access Management
IAP	Internet Access Policy
IFMIS	Integrated Financial Management Information System
ICT	Information and Communication Technology
IT	Information Technology
IPRS	Integrated population registration system
MAM	Mobile Application Management
MDM	Mobile Device Management
NAC	Network Access Control
PDAS	Personal Data Assistants
RBAC	Role Based Access Control
SaCCOs	Savings and Credit Cooperative Societies

DEFINITION OF TERMS

BYOD	the policy of permitting employees to bring personally owned devices (laptops, tablets, and smart phones) to their workplace, and to use those devices to access privileged company information and applications.
Cloud computing	the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer
Ecitizen	Official Digital payments platform that enables Kenyan *citizens* , residents and visitors access and pay for government services online
E-procurement	the business-to-business or business-to-consumer or business-to-government purchase and sale of supplies, work, and services through the Internet as well as other information and networking systems
Ihub	a globally recognized organization that is deeply steeped in the local tech innovation culture
IT Consumerization	The blending of personal and business use of technology devices and applications.
ITax	a web-enabled and secure application system that provides a fully-integrated and automated solution for administration of domestic taxes.
IT Infrastructure	an enterprise's entire collection of hardware, software, networks, data centers, facilities and related equipment used to develop, test, operate, monitor, manage and/or support information technology services.
M-PESA	a mobile money transfer service from Safaricom limited, a mobile operator based in Kenya.
NaiLab	a business incubator that offers an entrepreneurship program focusing on growing innovative technology driven ideas**.**

Contents

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION

1.1 Background to the study

The modern business environment is highly characterized by the use of advanced technologies as a key component of an organization's business model. A robust technology infrastructure has become a vital component of an organization's fabric. Rapid changes in technology have revolutionized the way in which organizations operate and therefore necessitating the need for impeccable information management frameworks in these organizations. The field of Information Technology continues to witness tremendous developments and their subsequent adoptions. There are various trends and emerging issues, which include Cloud Computing, Mobile Computing and Bring Your Own Device (BYOD) which continue to change the way IT is consumed, usually referred to as IT Consumerization. In the recent past, there has been a notable shift in the way organizational resources are accessed by users. The proliferation of mobile devices like smart phones, laptops, palmtops and tablets has led to many corporate organizations allowing their employees to bring their own personal devices to work and even access corporate and often sensitive data as opposed to the traditional arrangements where corporate IT departments used to provide company-owned devices for use and only at the designated workplace. This arrangement is called Bring Your Own Device (BYOD) (IBM, 2012; (Leavitt, 2013; Gheorghe & Neuhaus, 2013). Deloitte (2013) also defines BYOD as the use of employee-owned devices to access corporate content and the enterprise network. People are now able to enjoy the benefits of high-quality computing at their palms due to cloud-based applications and mobile devices.

In this rapidly growing trend, employees want to be able to perform both personal and work-related tasks using any devices and in any place. Through BYOD programs, employees have the liberty to purchase devices that meet their specific personal and work-related needs and use them in the workplace to perform various tasks (Citrix, 2013). These personal devices are also used by the employees to access corporate data from outside the organization's environment. Well implemented BYOD programs allow employees to use their own devices to access sensitive corporate data at work through company IT infrastructure (Li, Peng, Huang, & Zou, 2013).

The explosive adoption of mobile computing in the recent past has been attributed to the falling prices of mobile devices such as smartphones and tablets. These devices are also increasingly being adopted because of their ability to support a wider range of applications. In addition, the design of corporate networks today is characterized by mobility which therefore makes Wireless Local Access Network enabled devices more popular among employees (Namisiko, Sakataka & Sugut, 2015). Globally, the number of mobile devices continues to grow exponentially. By the end of 2018, it is estimated that there will be more than 10 billion mobile devices in the world (Namisiko, Sakataka & Sugut, 2015). A mobile statistics report by the Radicati Group, also estimates that every business user will have about 2 mobile devices by the end of 2018.

	2014	2015	2016	2017	2018
Worldwide Mobile Users (M)	**5,674**	**5,808**	**5,945**	**6,085**	**6,228**
Total Mobile Devices* (M)	**7,733**	**8,627**	**9,628**	**10,825**	**12,165**
Mobile Devices Per Business User	1.36	1.49	1.62	1.78	1.95

Figure 1.1: Worldwide Mobile Users vs. Mobile Devices, 2014-2018; Source: The Radicati Group, Inc

Kenya is recognized as a leader in the advancement and adoption of technology in the East African region and in the continent as well. The country is often referred to as the 'Silicon valley' of Africa. According to the Communications Authority of Kenya, the country is among the African countries that have the highest mobile and internet penetration (Communications Authority of Kenya, 2017). The country is also known for pioneering revolutionary applications such as M-PESA mobile money transfer service which has now spread to several countries in the world. The presence of ICT innovation hubs in the country such as iHub and Nailab which have successfully incubated several revolutionary ICT startups and attracted the attention of the world underscores the position of the country as Africa's Tech capital.

Mobile technology has therefore been embedded into every-day life of individuals, especially the younger generation. This technology savvy generation is enthusiastic about the greater capability and flexibility that mobile devices offer as well as the sense of fashion that comes with it (Trend Micro, 2012). Organizations are keen to leverage on the advancements in technology to increase their competitive advantage through increased employee productivity, better customer service and increased efficiency (Ernest and Young, 2013). This makes a good case for adoption of BYOD. Employees are able to bring cutting-edge devices that they are more familiar with into the workplace and enjoy using them to perform assigned tasks (Cisco, 2014). A study conducted by Mbalanya (2013) on the drivers of BYOD adoption by firms listed at the Nairobi Securities Exchange identified efficiency and improved productivity as the main reasons why the firms adopted BYOD. Other benefits of BYOD adoption include the fact that it offers employees flexibility to work at any time unlike the traditional office hours, cost savings in terms of expenditure on purchase of devices and boosting the morale of employees (Company85, 2014; Kamau, 2013).

The BYOD concept and trend has been fuelled by the greater capabilities these mobile devices especially tablets and smart phones have become compared to the recent past. This great processing power has encouraged workers to use them to perform complex tasks and assignment at their work places. While there are enormous benefits that enterprises derive from this adoption like cost saving and employee motivation and retention, there is a downside which is introduction of new security challenges. Madden (2013) terms this situation as a 'double-edged sword' because it involves striking a delicate balance between the benefits of this emerging trend and the security risks that come with it. This need for a balance calls for the implementation of robust policies to govern the deployment of BYOD in order to avoid compromising the security of sensitive company information.

BYOD in Government Organizations in Kenya

Kenya Cyber Security report of 2015 ranked government organizations as the most vulnerable group in terms of cyber security risk (Serianu, 2015). In the report, the ranking of other sectors in order of their cyber security risk is as follows; banking, financial services, manufacturing, Savings and Credit Cooperative Societies (SaCCOs), telecommunication, insurance, retail, hospitality and professional services. In the recent past, the public sector has implemented various technologies in a bid to improve service delivery, enhance efficiency and eliminate avenues of corruption. Government systems such as IFMIS, E-procurement, E-Citizen, iTax, and IPRS contain huge volumes of sensitive data belonging to Kenyans and the government. This sensitive data include personal information, government expenditure management and reporting, immigration data, land registries and tax-related data among others. Some of the government systems even have the capability to approve payments and transfer funds from the exchequer. However, despite the huge cyber security risks that these government information systems face,

investment in information security is still limited (Serianu, 2015). The adoption of BYOD in government institutions therefore makes the situation even more critical because criminals can use employees' mobile devices to infiltrate government information systems and access sensitive data.

The ministry of devolution and Arid and Semi Arid Lands in Kenya reported a cyber-security case where unknown people used stolen credentials to access the system and approved fraudulent tenders (Serianu, 2015). In the same year, a similar incident was reported in Garissa County where illegal payments were approved in the system using stolen credentials of senior staff members. Chinese hackers were also arrested in the country and found with sophisticated hacking tools (Serianu, 2015). In April 2016, a cyber-attack at the ministry of Foreign Affairs, about one terabyte of data including emails, security data and trade agreements were stolen and leaked. The Integrated Financial Management Information System (IFMIS), National Environment Trust Fund, as well as the Immigration services systems may have also been affected (Serianu, 2016). The fact that such information security breaches have occurred in the past points to the need for a robust security framework that takes into account all possible sources of security risks.

In February 2017, the government through the ministry of ICT announced that it is set to move away from acquiring equipment in large scale to BYOD programme for its civil servants (CIO East Africa, 2017). According to the Ministry, the programme would allow employees to acquire devices that they can use for both government and personal work. Successful implementation of this program would require a robust BYOD policy that would address privacy and security concerns for both the government and the civil servants (CIO East Africa, 2017).

1.2 Problem Statement

Government agencies are increasingly adopting the concept of BYOD in line with the government's digitization strategy. However, the adoption of BYOD is a double-edged sword providing various benefits on one side whilst presenting serious security risks on the other (Madden, 2013). According to the Kenya Cyber Security Report of 2015, government agencies were ranked first in terms of cyber security risk. Government information systems contain very sensitive and confidential information that is continuously being targeted by cyber criminals (Serianu, 2015).

In a BYOD environment, there are various security challenges facing corporate data that result from great use of employee owned devices. These challenges include the fact that manufacturers' security techniques are not mature enough (Leavitt, 2013), mobile devices come in very many open mobile platforms and Operating Systems making them more vulnerable (Salem et al, 2008). Furthermore, the devices being personal make it more difficult for IT departments control them and that traditional security frameworks like use of passwords and firewalls continue to exist in BYOD environments despite the additional challenges or security complications that BYOD devices introduce (Constantino et al., 2013). The devices may also get lost or stolen therefore jeopardizing the security of sensitive government information because unauthorized persons may gain access through the stolen mobile devices

These security loopholes often result in malicious attacks, data leakages, and distributed denial of service among other vulnerabilities (Morrow, 2012). There is therefore, an urgent need to put in place a holistic security framework in government agencies that clearly addresses the specific risks that are inherent in BYOD programs.

Existing literature on BYOD especially in the Kenyan context focuses on organizations such as Universities, Banks, Insurance Companies, Manufacturing companies and the hospitality sector. Very little attention has been given to government agencies by researchers yet these are the most vulnerable organizations in terms of cyber security risk. The study therefore sought to address this gap by focusing on BYOD in Kenyan Government agencies.

1.3 Main Objectives

The study had the following main objective:

To develop a framework for enhancing security of corporate data in a Bring Your Own Device (BYOD) Environment.

1.4 Specific Objectives

The study had the following specific objectives:

i. To identify the extent of BYOD adoption in Government agencies in Kenya and review the existing BYOD security frameworks and related security challenges.
ii. To design a BYOD security framework based on the findings from objective i above.
iii. To develop a holistic BYOD security framework that would guide Government agencies in securely adopting BYOD.
iv. To validate the developed framework.

1.5 Justification of the study

The recent reports of malicious attacks targeted at government agencies call for concerted efforts to address the huge risks that face government information systems. The adoption of BYOD by various government agencies increases the risk of attacks and the possibility of sensitive data landing on the wrong hands. Government agencies hold huge volumes of sensitive information whose security needs to be guaranteed at all times. It was therefore necessary to clearly identify the specific risks and challenges that government agencies face in regards to BYOD and to

provide solutions to these challenges through a holistic framework that will enhance security of information systems and allow secure adoption of BYOD in Government organizations. The limited literature on BYOD adoption, challenges, risks and security in the public sector points to the need to focus BYOD research efforts on this sector. Therefore, it was important to carry out this study because it would go a long way in addressing the bottlenecks of secure BYOD adoption in the public sector and other sectors as well.

1.6 Significance of the Study

The public sector has been identified as the most vulnerable sector in terms of cyber security risk (Serianu, 2015). As the government continues to invest in information technology as a key driver of its Vision 2030 development blueprint, cyber security risk stands in the way of realizing the full benefits of digitization in government agencies. The government is also increasingly adopting BYOD programmes in the public sector as a cost-cutting measure as well as other benefits such as increased employee productivity, flexibility of working hours, and employee motivation especially among the younger generation public servants. However, the biggest challenge for these organizations remains how to successfully implement BYOD while at the same time ensuring that the security of information stored in their information systems is not compromised (Namisiko, Sakataka & Sugut, 2015). This study would therefore be immensely useful to government organizations including the Ministry of ICT and other policy makers and IT professionals because it pointed out the specific issues or risks facing BYOD adoption in government and recommend solutions to these challenges through a framework that would ensure secure adoption of BYOD.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

Bring Your Own Device (BYOD) is an Information Technology trend where employees in an organization are using their own private devices like laptops, tablets, and mobile phones to manage corporate data wherever they may be (Millard, 2013). This new mantra has empowered employees to innovate their way of working using the technology of their preference. This implies that employees can choose and buy the device they like and uses them in the office to access corporate information.

The primary motivation for adopting BYOD concept is that they save on acquisition costs and even boost morale for employees, which boosts productivity. Also, the concept makes employees flexible and attractive, which increases employee retention in organizations that have adopted them (Mahesh & Hooter, 2013). Employees would much like to use the devices and applications of their choice as well as their software and cloud services of their choice. The convenience of using the device and software one is comfortable with is vital to creating the best employee-working environment.

This chapter discusses the literature on the concept of the BYOD. The study explored the existing literature on the extent of BYOD adoption as well as the security challenges that accompany this concept. The study also explored and review the existing security frameworks.

2.2 The Prevalence of BYOD in Government Agencies

The use of personal devices for work commitments is generally considered to be inevitable across all industries worldwide, which includes government agencies (Leavitt, 2013). Although government agencies have not been recognized as hotbeds of technology, their retro status has

convinced employees to bring their own devices to workplaces. This early adoption of BYOD in public-sector companies has allowed employees to use personal devices to access company data. Either the employees select the device of their choice from a catalog of authorized services and devices or they are given the liberty to use their own devices at their work places.

2.2.1 BYOD in Government Agencies around the World

In the world stage, according to a report by Cisco (2012), BYOD has become an inevitable concept, and the only challenge is in the management of BYOD. The use of BYOD has enabled organizations to embrace this flexibility through choice to push employees to use specific devices and services for work purposes. In the survey of government agencies by Cisco (2012), there is a prevalent trend of the use of BYOD across parastatals and government companies. According to the data, 58% of government workers use their own devices and smartphones for work purposes without consideration of the specific devices the government supports. This data implies that despite the government specification, these employees use their devices for work without consequences.

However, in the same data, some government officials allow this to happen. The desktop service director at the provincial government department in Canada described that they see more demand for tablets because the government does not offer them, they allow. The report shows that 25% of tablet users and 16% of smart phone users did purchase their devices from a list of authorized devices from their government agencies.

In the US, a report survey by Lookout (2015), 50% of federal employees use their devices to access work-related email, and 49% use these devices to download all their work documents. Though this is just an example of huge volume data movement from work accounts to personal

accounts, government organizations, should strive for control and visibility over the changes of its data (Lookout, 2015).

2.2.2 BYOD in Kenya

In Kenya, the BYOD concept has been incited by the increase in competition in the mobile telecommunication industry. In a report by the Communications Authority of Kenya (2016), telecommunications market leader Safaricom has been collaborating with various mobile manufacturers to push demand for mobile, and tablet devices through to its 25.1 million subscribers on 3G and latest 4G network. The flooding of mobile devices with latest operating software technology affects the usage of these personal devices in workplaces, which includes in government agencies.

Data from the Kenya Cyber Security report (2016) indicates that approximately 62% of government agencies in Kenya have allowed the use of BYOD. In Tanzania, 61% of government organizations allow the BYOD usage for work accounts. This statistic implies that government employees can access critical and sensitive social and economic information from their devices. The extent of BYOD in government agencies is very high and is becoming a force that cannot be ignored (Serianu, 2015).

2.3 Security Challenges facing BYOD adoption

Despite the benefits of BYOD in companies, there are many security risks associated with the concept. BYOD has become a double-edged sword. The increase in the number of smart phone owners has led to the rising adoption of BYOD in many organizations, which could pose a threat and act as a gateway for hackers to access confidential information. The security breach through hackers is a global problem whose solution is constantly being sought through enterprise security frameworks and regulations.

In the research survey of the United States by Lookout (2015), 18% of federal employees in several government institutions claimed to have encountered malware problems on their devices, that is, tablets and mobile devices, and government approved devices. Despite this encounter rate, it was noted that 49% of all federal employees did not have any security applications on their devices to counter the malicious malware.

According to the Kenya Cyber Security Report (2016), despite the high levels of investments in information technology and automated processes in government agencies in Kenya, there are no security frameworks to contain the cyber threats brought about by the BYOD concept. This statistic alone confirms that the government is vulnerable from cyber-attacks through BYOD. In 2016, the Ministry of Foreign Affairs suffered from cyber attacks where 1 terabyte of data was stolen, which included sensitive information. Several government programs were also compromised including the Immigration and Registration of persons, the National Environment Trust Fund, and the Integrated Financial Management Information System (IFMIS).

Traditional security mechanisms like passwords, firewalls, and antivirus no longer serve to assure the security of corporate information in a scenario where employees own and have total control of their devices. This is due to the fact that BYOD presents a problem from within the enterprise and not without as has been the case earlier. According to Gessner et al., (2013), one of the main security challenges of BYOD is the risk of loss of data or loss of the device which can lead to sensitive data landing in the wrong hands. In addition, BYOD can result in bandwidth strains as well as cyber-attacks targeted at the organization's information system through the mobile devices. Sensitive data leakage, malware and distributed denial of service (DDoS) have also been identified as the key security risks posed by this emerging trend (Morrow, 2012).

Data leakages may occur as a result of malicious use of the mobile device by an employee, vulnerabilities of the applications within the devices and remote access to an organization's information system through an employee's mobile device. Lack of proper training among employees on the organization's security framework as well as the reluctance by the employees to back up data have also been identified as causes of data leaks (Armando et al. 2014). Distributed denial of service is likely to result from malicious attacks as well as vulnerabilities within the organization's network that can be exploited by attackers. According to Miller et al. (2012), one of the key concerns of BYOD is the privacy of personal employee information. Since employees use their personal devices at work, the devices contain both personal and corporate data and, therefore, it is difficult to effectively implement strict security controls on BYOD devices (Ghosh, Gajar & Rai, 2013).

According to Constantino et al. (2013), nearly half of organizations that have allowed employees to bring their own devices and use them in the workplace or allowed them to connect to the organization's environment have reported an actual or attempted data breach. These data breaches have dire consequences because they often involve litigations, severe costs and loss of customer trust (Harris & Patten, 2014). A research by Ernest and Young (2013) that top four challenges or concerns for BYOD are Mobile device security, data breach security concerns, mobile data security concerns and mobile application security concerns as shown in the chart below. Ernest and Young established many other challenges and concerns.

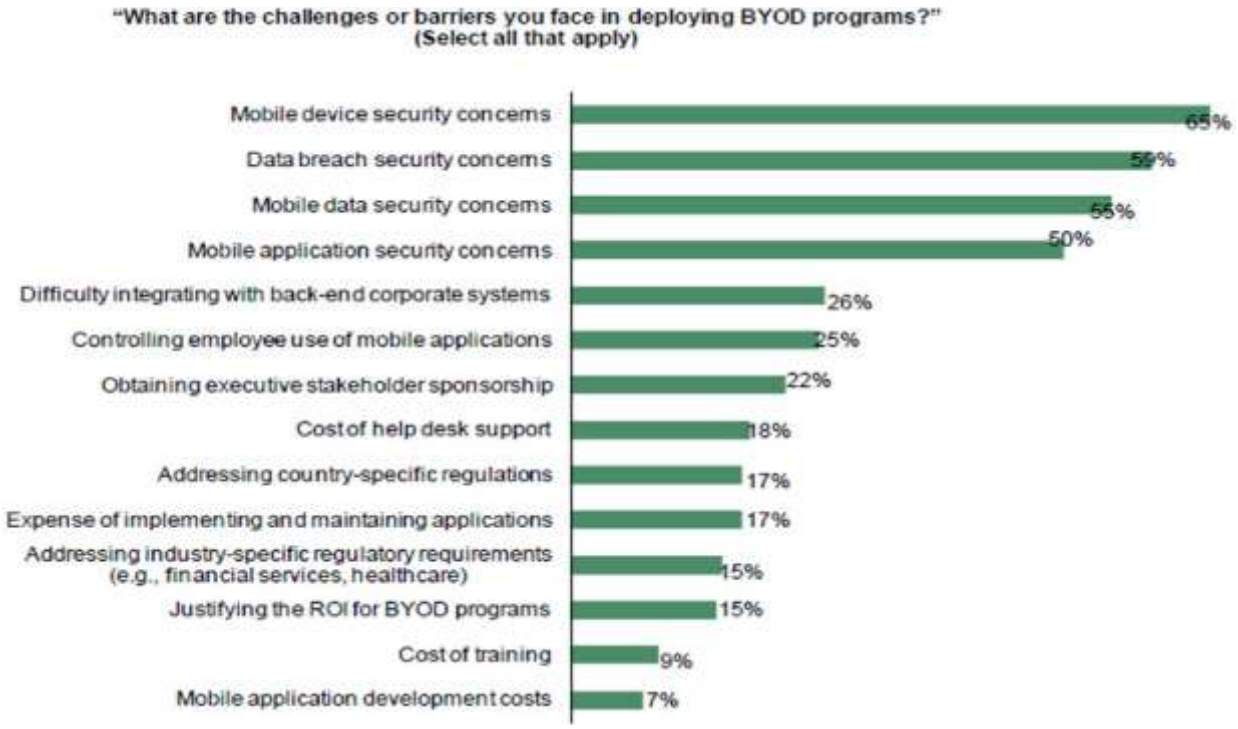


Figure 2.1: *BYOD challenges with security concerns at the top (Forrester, 2012)*

To tackle the security challenges that government agencies face, the study discussed the various sections that BYOD security aspects connect them. The BYOD concept faces security challenges from its strategy and policy frameworks, the security threats can also be internal from its employees, and the security threats can also originate from the technical infrastructure of the BYOD and the government agency's databases.

2.3.1 BYOD Strategies and Policies

According to Li et. Al. (2015), BYOD programs and policies are helpful in empowering employees to choose the best devices for use when working with them. The BYOD policies and frameworks encourage employees to be flexible with their work. The primary purpose of the strategies is to allow employees to use BYOD without risk of sharing the sensitive government

information and save on costs for the agencies through allowing employees to use their preferred devices rather than providing the very same devices on the agency's budget.

Research by Thielens (2013) concluded that having a secure and scalable BYOD strategy and policy is a critical requirement to manage the risks that the BYOD concept may introduce when the devices are lost or stolen, or even after employee termination. Policies in this research indicated the consequences and protocols that an agency should follow on in case of the three scenarios mentioned above.

Among the challenges in security due to adoption of BYOD is that there are no policies in place for most organizations, including government agencies to govern the use of BYOD for access of confidential company details and documents (Matinde, 2015). The effect of this gap in policies will raise the insecurity levels in government agencies and opens up the government databases to cyber attack and other cyber threats.

According to the Kenya Cyber Security report (2016), 41% of all the companies in Kenya with BYOD concepts have developed BYOD policies to control BYOD devices. The lack of the best BYOD policies and practices is a high risk that organizations take in cybersecurity. The report recommended that every company should develop specific BYOD policies to monitor their usage as the first line of defense. The first step is scoping, which defines the extent of any BYOD program. Lack of a BYOD policy will not limit the extent that a personal device can reach when dealing with sensitive information.

2.3.2 Employees of Government Agencies

Companies can be under siege from their employees particularly those who can bypass their current systems, and define its protocols (Matinde, 2015). Disgruntled employees can use their

gadgets to get access to unauthorized information from government agencies. This information can be sold in the dark web to the highest bidders from the comfort of their living room. The sale of sensitive information from the government is espionage and is considered treason against the country.

In the Kenya Cyber Security Report (2016), the risk due to the high percentage of employees with personal laptops, PDAs, smartphones having multiple access to databases, email accounts and applications makes the threat a significant challenge. The need for government organizations security strategies to address this challenge is a key priority. The report continued to mention that employee threat can be caused by revenge, blackmail, and competitive advantage because the other main reason for this challenge is substantial is that employees already have access to the government agencies' systems. Therefore, the possibility of detection is very low since some of them may be well versed with the systems security protocols and can cover their tracks.

According to a research by Olalere (2015), another BYOD security challenge brought about by employees is data leakages. Data leakages occur when access to an organization's data by employees is shared with the public without the consent of the organization. Such employee-driven BYOD risks are difficult to control due to the personal devices access. This security threat is also related to social engineering. Social engineering occurs when employees leak vital data because a third party manipulates them into sharing their passwords and credentials. This threat poses a threat to BYOD concept in organizations.

2.3.3 BYOD Infrastructure challenges

The BYOD infrastructure involves software applications, wireless connections, and mobile phone services, which allow BYOD concept to function in workplaces smoothly. Hormazd (2014) found that wireless capabilities have been on the rise thus increasing security threats to

information security. The study noted that malware attacks can be implemented through rogue access points by an attacker into the BYOD infrastructure. This poses a danger to a BYOD environment. Another mode of attack through wireless capability is through a BYOD device, which has accessed a malicious website. The report explains that the smart device that has accessed such sites can be used to access an organization's server using a malicious code.

Watch Guard (2013) found that another challenge to the BYOD infrastructure is the lack of enough insight into the corporate networks. The absence of strong IT support to manage BYOD devices affects BYOD security. Lack of network support gives time for espionage cases and cyber-attacks enough time to get away without a trace in the system. For the organizations that lack IT management, there is no visibility into operations of the BYOD devices in and out of the organizations. The lack of log files and reports reflects the absence of the devices on the company's database, which results in the companies being powerless when managing BYOD because you cannot protect what you do not know.

In the report by Watch Guard (2013), the study described the risk that must be addressed from the adoption of BYOD concept. The study mentioned that there was too much risk of data loss from using mobile devices. Since BYOD devices include smartphones, there should be tight security because they are the most easily accessed and encrypted devices. For government agencies, the loss of sensitive data from the databases makes it a target. Since the device are mobile, they can be easily stolen, and after encryption, the information can expose government agencies and damage the reputation of the agency or may even be costly when it involves litigation. Another device-specific challenge for BYOD is the risk of a malware attack via the mobile devices. Several smartphones lack anti-malware software, which exposes the organization's data when the mobile devices access confidential information. According to

Watch Guard (2013), such malware, which includes Trojan horses, keyloggers, and viruses can be used to capture user passwords, steal data, crash computers or servers, and may even delete sensitive information. The research further explained that the malware can widely spread the damage to the company by providing entry points for a hacker or also sometimes interrupt business practices.

In the National Institute of Standards and Technology (NIST) report (2011), unknown third-party mobile applications and software can be downloadable by the employees. The threat introduced through mobile apps and software is a DoS attack. A DoS attack is a coordinated attack on the company's service provision center on the network, which can be initiated through an application. The DoS attacks the entire system, which makes it a threat to adoption of BYOD.

2.4 Existing BYOD Security Frameworks

Various BYOD security models have been suggested by researchers who have developed frameworks that act as guides for implementation of BYOD. The following measures have been implemented in various companies to address specific challenges:

2.4.1 Mobile Device Management (MDM)

MDM tools are used to give aid to organizations on how to control mobile devices, in the BYOD concept, to the company's network infrastructure. The MDM tools lock down the mobile devices, wipe out data remotely or locally, encrypt the devices and are even used to enforce policies for all connected devices. The MDM tools are beneficial because they enable the organization to monitor, protect and control the BYOD mobile devices, which addresses the security threats from the BYOD concept. The MDM tools manage passwords, installs digital certificates on the mobile devices for authentication, monitoring installed applications, and enforce security settings when necessary.

Hernández & Choi (2014) found that MDM tools offer access to a secure presence in BYOD mobile devices with Android operating systems that allow organizations to provide encryption and have automatic access control to the employees' smartphones. In support of this research was Ghosh et. Al. (2013) whose report suggests the MDMs are useful when monitoring BYOD mobile devices. He further suggests that the MDM tools generate reports of all the connected devices, and their software and applications. Also, they have the capability of profiling and filing all the activities from these BYOD smartphones. The report discusses how due to their capability of automatic access control, MDM tools can restrict a BYOD user from downloading and installing specific applications and software, which do not meet the company's security requests.

There are several MDM tools in the online market, which are used by organizations to monitor control, and protect BYODs. According to Dahlstrom & Difilipo (2013) who reviewed but a few, Divide MDM solution is the best BYOD solution regarding deployment, ease of use and its features. Its setbacks include the fact that they only support iOS and Android smartphones only. AirWatch MDM solution is the complete product whose features include a separate MDM, file management, mobile control service, and an integrated console delivered in the organizations' location or from the cloud.

In a report by Rhee et. Al. (2012), MDM tools use the exchange of certificates in a particular company's BYOD to communicate with the MDM agents installed in their mobile devices to allow these devices to access a company's databases and confidential data. The report further explains that MDM is useful in enforcing access rights, trigger remote data wipes on stolen smartphones, update software and applications, support VPN connections on BYODs, provide activity reports, and conduct anti-malware scans. MDM solutions are very valuable for

companies to implement BYOD strategies and frameworks swiftly, in a centralized and simplified manner.

2.4.2 Network Access Control (NAC)

NAC is a tool which controls the devices that connect to the company's network infrastructure. This tool is useful in maintaining security from cyber-attacks through the company's network access points. The Network Access Control model limits the number of connected devices, regulates permissions of access and denies unrecognized BYOD devices access to the organization's internal network. The Network Access Control ensures there is a low probability of data leakages from the company's network, reduces company-wide malware infections to other infrastructure components, and other cyber-attacks.

According to a report by Dell Inc. (2015), other Network Access Control variations perform the same role as the NAC in a customized manner. The Identity and Access Management (IAM), which is a variation of NAC, applies the same protection protocols but is customized to devices used for access controls in a network. The IAM can also manage to allow single sign in and separation of duties. Similarly, the Access Application Control (AAC) is installed on smartphones to perform identity access control functions for software and applications.

2.4.3 BYOD Security Framework

The BYOD Security frameworks are guidelines that are made to govern and manage BYOD implementation. Each framework is made specific to their environment or company. According to Zahadat et. Al. (2015), the BYOD security framework is divided into seven stages to create a framework that manages the BYOD concept in a particular company. The phases include; one, planning, in which one identifies its users and resources that they have to access. In this phase, one is also required to understand the concept of the business or company.

The second phase is identifying, in which the devices are registered, undergo approval, and provided with an appropriate security certificate. The third stage is protection, in which the information held within the BYOD devices is given protection. In the fourth phase, detection, the organization is required to protect, and react to intentional or unintentional threat level events that were identified. The fifth phase, response, requires that the organization respond to the identified threats, by either erasing data, deleting malware, or seclusion of the device that is infected.

In the sixth phase, recovery, the company must be able to recover completely from the attack event, by confirming the safety of the confidential data and return to normalcy after the intentional or unintentional attack. The last phase is assessment and monitoring, where the company investigates the competence level of the BYOD security program and continuation of the supervision of the BYOD frameworks. The whole framework can be represented by the figure below.

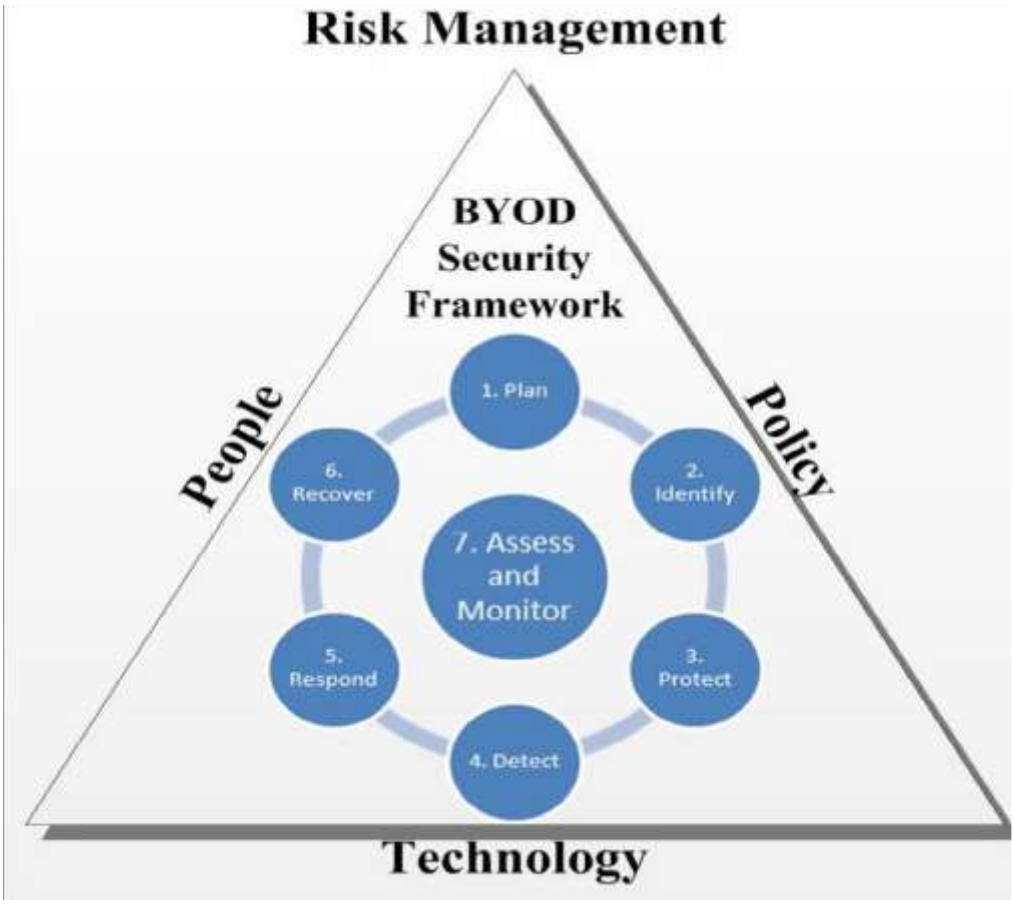


Figure 2.2 BYOD Security Framework (Zahadat et. Al., 2015)

The figure illustrates the seven phases incorporated with the three pillars of a BYOD concept: the organization's employees, the BYOD policy, and the BYOD infrastructure.

In their study, Titze et. Al. (2013) designed a BYOD framework that allows the organizations to run automated security checks that are tailored to the specified security requirements of the company, on the BYOD devices applications and software. The framework program runs parallel to the public application markets and does regular checks to confirm the presence of applications that are allowed by the company on employee's BYOD devices. The BYOD framework also includes plug-in installations that run security services to scan for malware, unknown configurations, and misbehaving applications.

2.4.4 BYOD Privacy & Culture Governance Framework

The BYOD privacy and culture governance framework is the BYOD implementation framework that maps the company's culture and privacy concerns in an agency. Selviandro et. Al. (2015) concluded that the mapping is done to develop a BYOD policy, which is prescribed to the following components; ensuring that the company culture and privacy are unaffected after a security framework is implemented. The first component is to determine the culture within a company from employee experiences.

The second component is to outline the features of the company's culture into specific concerns. The third component of the privacy and culture framework is to identify the privacy concerns that apply to the organization and incorporate in the BYOD framework policies. The fourth component is to highlight the personal and employee specific concerns regarding their privacy and include in the framework policies (Selviandro et. Al., 2015).

The fifth component when making policies according to the report is that a company should conduct a valuation based on the employee privacy concerns to ensure employee satisfaction in the formulation process. The sixth component in the formulation process is the development of the BYOD policies, which take into account the valuation concerns, and the final component is the implementation of the management control about the company's culture and privacy wishes (Selviandro et. Al., 2015).The following figure is a representation of the BYOD privacy and culture governance framework.

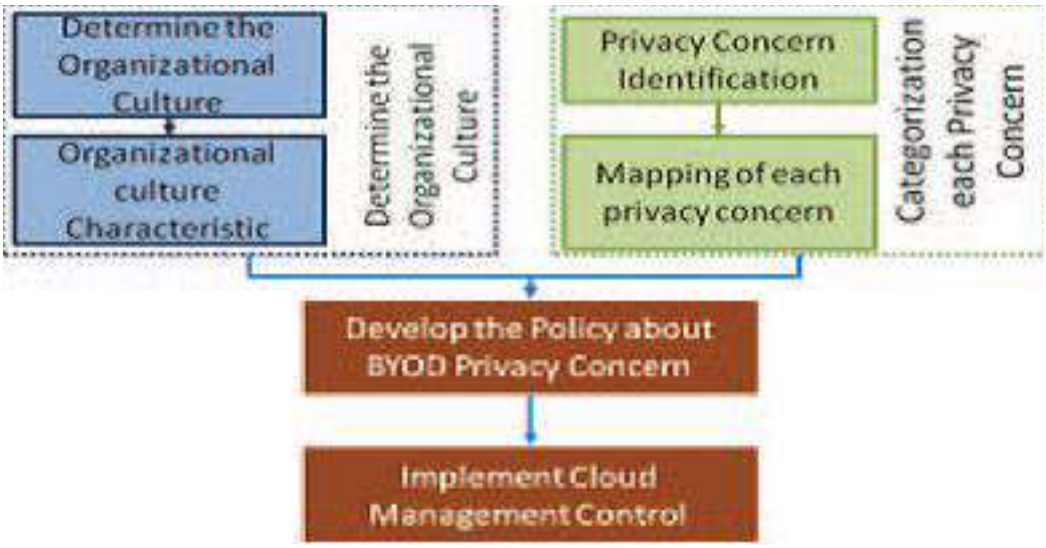


Figure 2.3: The BYOD Privacy & Culture Governance Framework Components (Selviandro et. Al., 2015)

Gheorge & Neuhaus (2013) noted that BYOD privacy frameworks aim to protect the employees' and users' privacy within the company's internal networks and protects them from the outside with a vision of allowing communication between the management and employees in the company. The report designed and evaluated a concrete privacy program called Privacy-Preserving Accountability for personal Devices (PriPARD) for BYOD smartphones used in the corporate environment. The privacy mechanism worked by enabling a slight trade-off between monitoring data in a network and maintaining privacy within the BYOD concept communication in the company environment (Gheorge & Neuhaus, 2013).

The works of Werthmann, Hund, and Davi (2013) who addressed the open problem also supported the study by Gheorge & Neuhaus (2013). Their research produced a program based on the BYOD policy that ensured there were no privacy leaks and simultaneous strengthening of the BYOD security framework against runtime attacks on iOS mobile devices. The BYOD security

framework ran on a program designed and implemented similarly to the PSiOS, which is a tool that features a BYOD policy enforcement framework for the iOS.

2.4.5 Enterprise and BYOD space BYOD Security Framework

The main purpose of the Enterprise and BYOD space BYOD Security Framework is to enhance the security of an organization in a BYOD environment (Wang, Wei, and Vangury, 2014). The framework comprises to two main arms, i.e. the BYOD side and the Enterprise side.

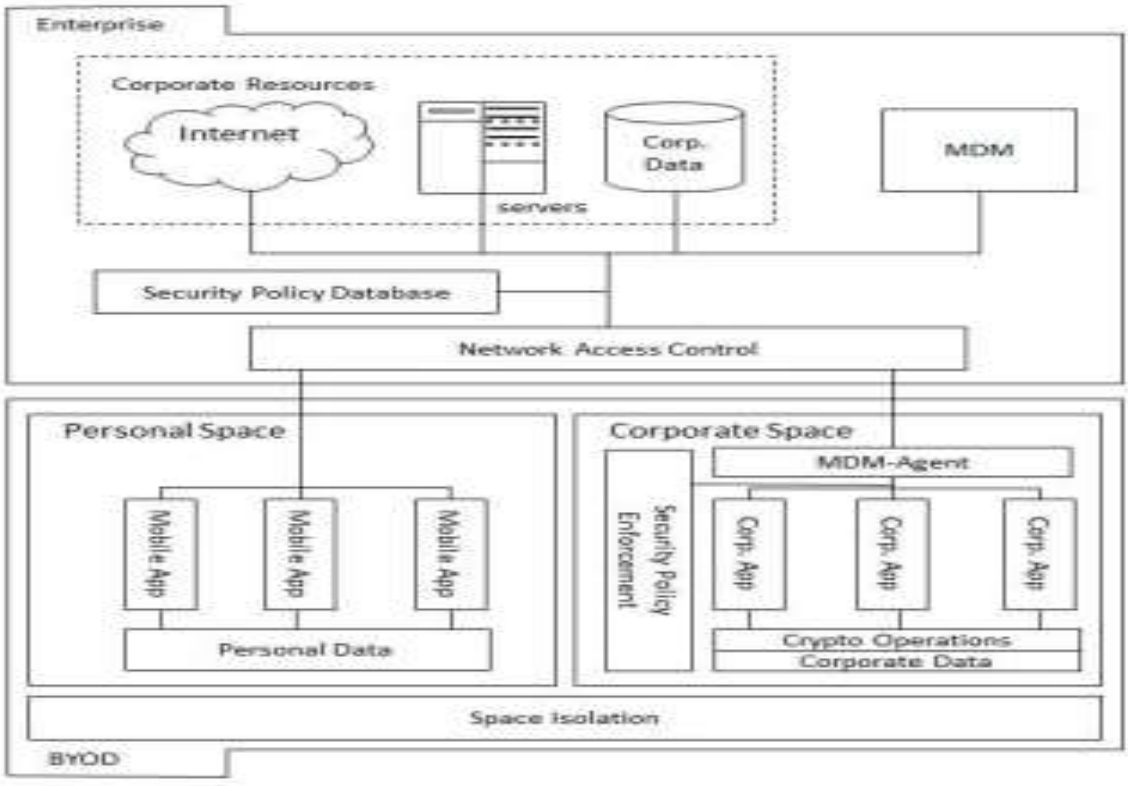


Figure 2.4: Enterprise and BYOD space BYOD Security Framework (Wang, Wei, and Vangury, 2014).

In the BYOD side, the framework provides for separation of personal data from corporate data as well as protection of organizational data while the Enterprise side addresses the management of devices and corporate resources.

2.4.6 High level BYOD Management Framework

Fani, von Solms and Gerber (2016) developed the High Level BYOD Management framework after their review of the literature identified gaps in the existing frameworks. They noted that the existing frameworks were not adequately aligned with eight important characteristics of BYOD security namely risk identification, stipulation of security requirements, consideration for the organizational context, analysis of BYOD devices, contextualization of employee role, IT administration in the organization, existence of a BYOD policy, and compliance with the BYOD security policy. The High level management framework involves four phases i.e. analysis of the problem, design, evaluation of the designed solution against the objectives, and the diffusion/finalization phase (Fani, von Solms and Gerber, 2016).

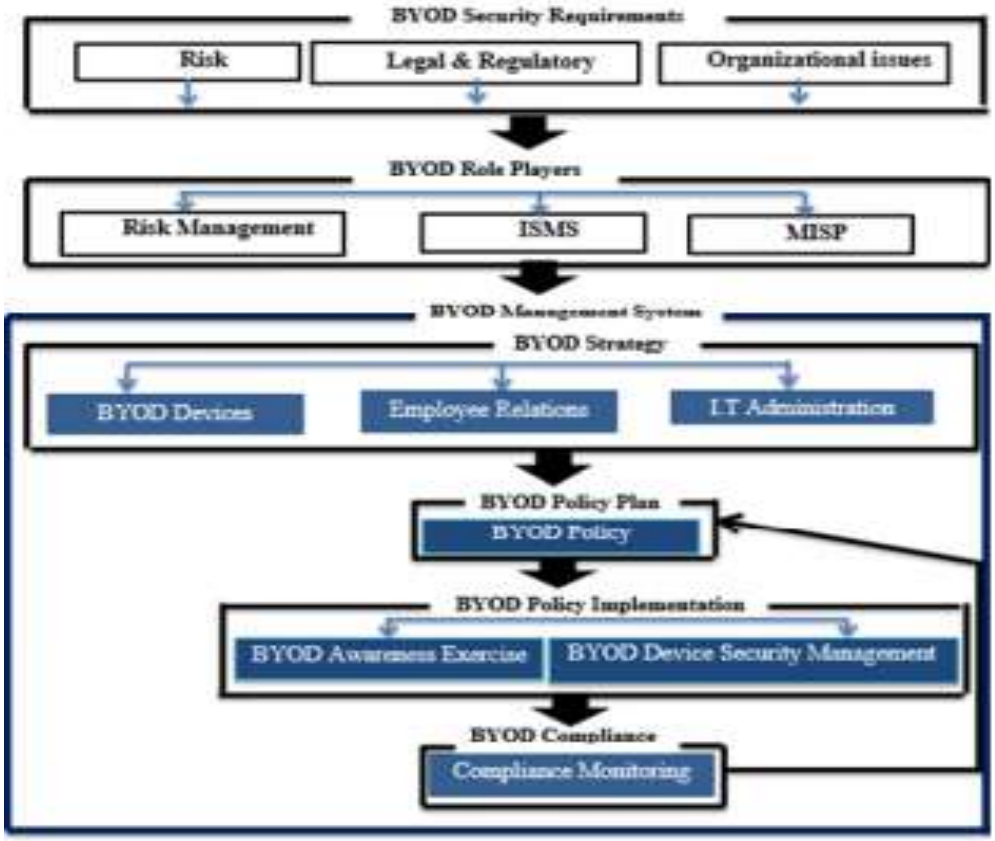


Figure 2.5: High level BYOD Management Framework (Fani, von Solms and Gerber, 2016).

2.4.7 BYOD framework for a management system

Brodin (2015) developed the BYOD framework for a management system whose objective was to provide a strategic approach to information security for an organization that adopts BYOD. The framework involves three main steps namely analysis, design and action. In the analysis step, an organization that is adopting BYOD identifies the strategic objectives of the organization including the information security objectives. In the design step, the organization updates the existing policies and implements new ones that are in line with the information security objectives. Finally, the action step involves risk assessment and implementation of the information security strategy (Brodin, 2015). However, this framework does not consider the specific BYOD related security challenges and does not emphasize on compliance.

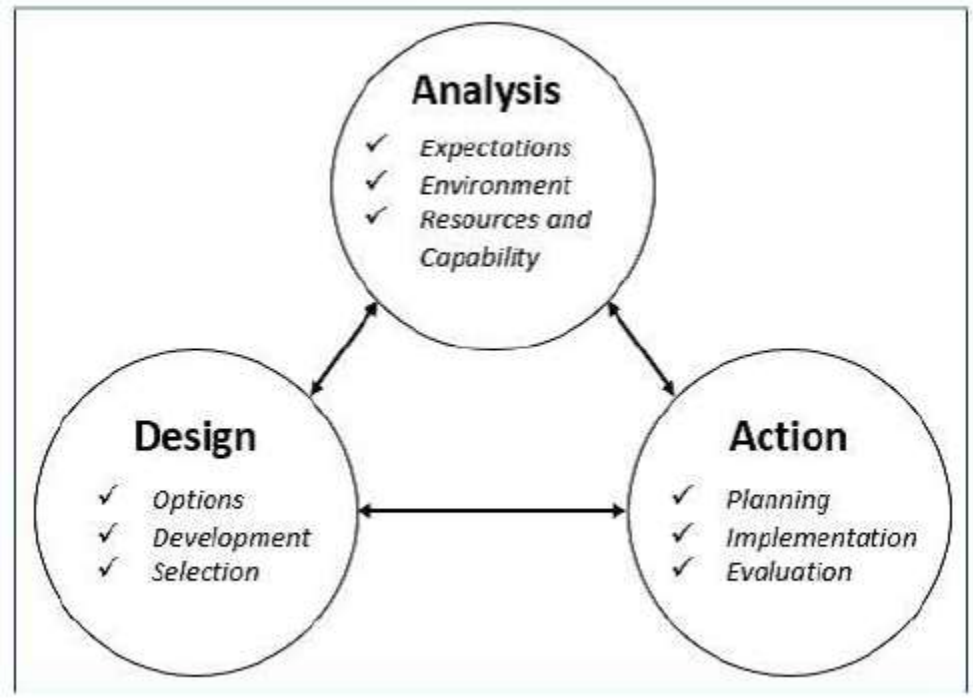


Figure 2.6: BYOD framework for a management system (Brodin, 2015).

2.4.8 BYOD Policy Framework for Educational Institutions

In developing a policy framework for adoption of bring your own device (BYOD) by institutions of learning in Nigeria, Oluranti and Sanjay (2016) came up with a policy framework that has five main elements. The framework is shown in the figure below.

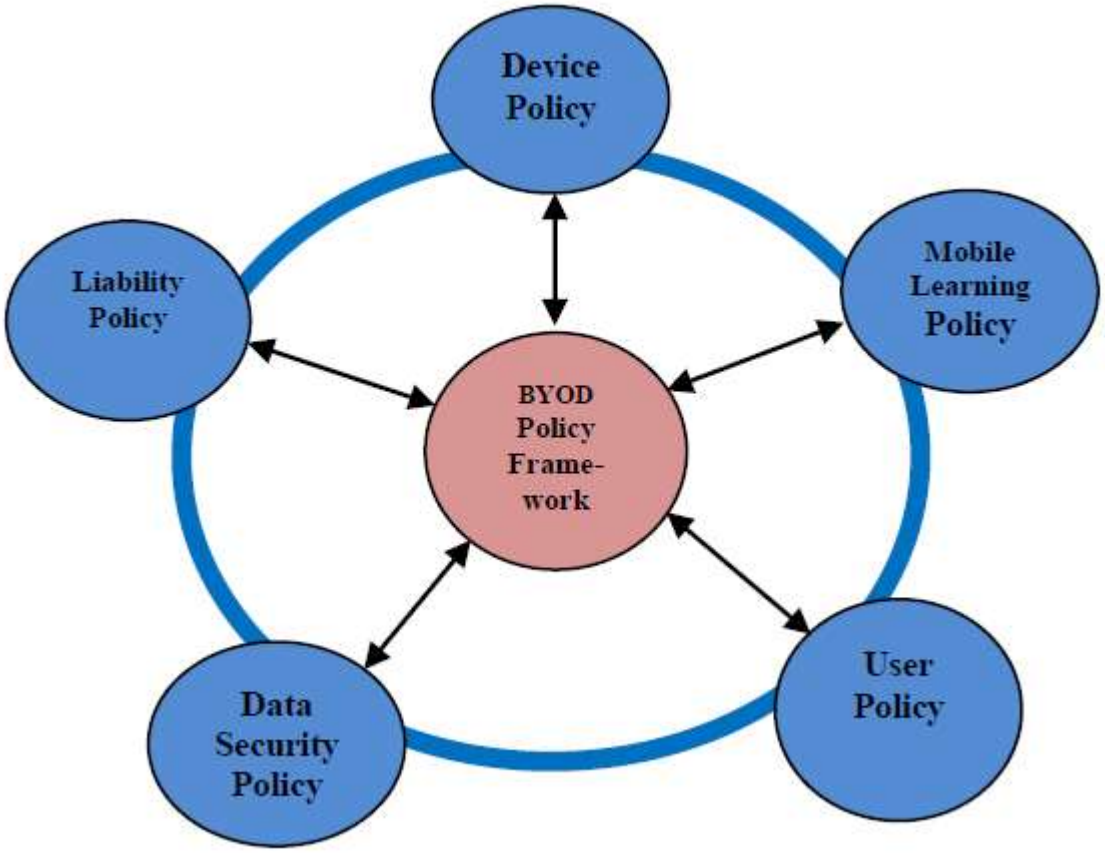


Figure 2.7: BYOD Policy Framework for Educational Institutions (Oluranti& Sanjay, 2016).

The device policy involves the selection of devices allowed to access the organization's resources. Highly restricted device model involves specifying specific devices while the flexible model allows users to bring any devices without restrictions. The user policy involves user authorization, user education and training while the data security policy involves device registration, data separation, VPNs, data encryption, enabling remote access and password management. The mobile learning policy involves the use of mobile device functionalities to

support learning. Finally, the liability policy involves agreements on the settlement of bills incurred in the course of using BYOD (Oluranti& Sanjay, 2016).

2.5 Review of BYOD Security Frameworks

Despite the existence of these BYOD security frameworks to protect BYOD devices and sensitive information from cyber-attacks, each of the frameworks has its own limitations. Based on existing literature, the study reviewed each security framework against their goals and primary objectives.

The primary goal of the NAC is to protect the internal network from entry of malware and access of cyber-attacks from rogue access points. However, the NAC cannot single-handedly detect malicious activity, and once the infected applications enter the internal network, the NAC will have little control over the resulting damage and actions. A report by Dongwan et. Al. (2015) notes that other limiting setbacks of the NAC include that there is increased strain on the IT administrators who monitor the network traffic. The research was complemented by the works of Pell (2013) who notes similar downfalls of the NAC including the fact that Application Access Control (AAC) is prone to dismissal by employees because of its intrusive nature of access control in the company network.

MDMs are also a controversial BYOD security framework. According to Hormazd (2014), the MDM security framework subjects all smartphones applications, software, and data to security protocols that it enforces. The security protocols are an endpoint, access control solution, which is mainly a reactive measure. Therefore, the lack of preventive measures still exposes the mobile devices to inappropriate use if they are stolen or lost. Koh et. Al. (2014) complimented these findings and added that the other controversial issue that MDMs security frameworks faced was rejection by employees due to their restrictive nature and their invasion of privacy security

protocols that the BYOD owners surrender. According to Leavitt (2013), the MDMs security frameworks can be laborious during maintenance due to the constant variation in the number of connected devices, and the regular updating of BYOD devices.

The BYOD security frameworks, as well as BYOD privacy and culture frameworks are also limited by how strongly the administering organizations enforce them. Morrow (2012) found several reasons may limit the effectiveness of the BYOD security, privacy and culture frameworks. General negligence of the organization, human error during implementation, and failure in compliance to the BYOD security framework policies may contribute to security breaches and loss of intellectual properties. The research by Thomson (2012) supported these findings and added that auditing, compliance, and agreements to the BYOD policies that are not specific to an organization are prone to resistance by employees who have malicious intent or who disagree with the frameworks.

Knowledge gaps

Following the literature survey, the following is a summary of the similar previous works done by various authors in this area, their findings, identified knowledge gaps and strategies used to address the identified gaps:

Table 1: Previous works, findings, knowledge gaps and strategies to address gaps

S/No	Researcher(s)	Study focus	Findings	Knowledge Gap(s)	Strategy
1	Hernández & Choi (2014)	Mobile Device Management (MDM)	MDM tools offer access to a secure presence in BYOD mobile devices with Android operating systems	frameworks may face rejection by employees	Data separation
2	Dongwan et. al. (2015)	Network Access Control (NAC)	NACmodel limits the number of connected devices, regulates permissions of access and denies unrecognized BYOD devices	NAC cannot single-handedly detect malicious activity	Use NAC in with MDM, MIM and MAM
3	Zahadat et. al (2015)	BYOD Security Framework	BYOD security involves Planning, Identification of devices, Protection, Detection, Response, Recovery, Monitoring & Evaluation	BYOD education, sensitization Data separation not addressed.	BYOD education strategies & Data separation
4	*Selviandro et. Al*	BYOD Privacy & Culture Governance Framework	Protects the employees' and users' privacy within the company's internal networks and protects them from the outside with a vision of allowing communication between the management and employees in the company. Ensures that the company culture and privacy are unaffected after a security framework is implemented	Employee role and user access management not considered.	Role based controls, employee involvement, User access management tools and policies
5	Wang, Wei, and Vangury (2014)	Enterprise and BYOD space BYOD Security Framework	The BYOD side of the framework provides for separation l data .	Remote data monitoring not addressed	Data monitoring and remote wiping;
6	Fani, von Solms and Gerber (2016)	High level BYOD Management	The High level management framework involves four phases i.e. analysis of the problem, design, evaluation of the designed solution against the objectives, and the diffusion/finalization	Specific risk management tools & Data separation also not addressed.	Specific risk management tools & Data separation will be included.
7	Brodin (2015)	BYOD framework for a management system	Involves 3 steps; analysis, design and action.	Does not emphasize on compliance.	Strict compliance monitoring
8	Oluranti & Sanjay	BYOD Policy Framework for Educational Institutions	Deals only on policies	leaves out infrastructure requirements	infrastructure requirements to be included

2.6 Theoretical framework

P. Norman, H. Boer, and E. R. Seydel (2005) developed the Protection Motivation Theory (PMT) which illustrates how fear influences changes in attitude and behavior. In understanding the security challenges or reasons why organizations have not adopted BYOD, PMT helps bring out the concept of security threats and risks. According to the theory, the adverse consequences of failing to take recommended actions are referred to as fear appeal. Cognitive appraisal then triggers protection motivation which creates attitude change. At the protection motivation stage, the person evaluates both the threat and the decision to cope. Threat evaluation or appraisal involves comparing the maladaptive behavior and the severity of the consequences. On the other hand, coping involves taking actions to remove the threat which involves analyzing the cost of the action/response, efficacy of the action/response and self-efficacy (Norman, P; Boer, H; and Seydel, E.R, 2005).

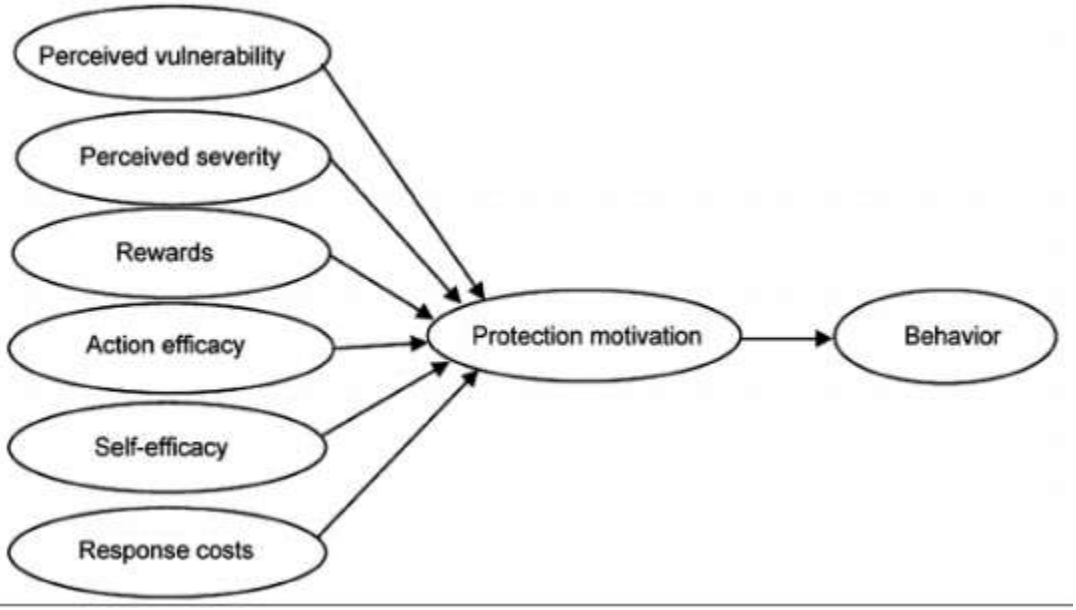


Figure 2.8: Protection Motivation Theory (Norman, P; Boer, H; and Seydel, E.R, 2005)

Making inference from PMT, organizations' assessment of the potential security risks and the likelihood of occurrence of the risks may slow down the adoption of BYOD. The fear of these risks may also lead organizations to take preventive measures to reduce or remove or reduce the threat. These preventive actions may involve doing away with BYOD completely or bearing the costs of security measures to guard against BYOD security risks.

2.7 Conceptual framework of the developed BYOD security framework

Having reviewed the existing literature, the study identified the key elements that are essential in securing corporate data. Firstly, the security and integrity of mobile applications is an essential component that ensures that there is no unauthorized access to sensitive corporate data. Secondly, information security policies have to be developed and enforced to ensure that strict guidelines are in place to secure the corporate network through acceptable use of resources, secure access to the internet as well as secure use of BYOD devices. Another critical element in securing corporate data is User Access Control and Device Identification. It is important to effectively control access to the corporate network and to identify each device that accesses the network. This can be done through password management, user agreements, and encryption among other tools.

Enhancing the security of corporate data also involves carrying out effective and continuous training and sensitization of all users. This will raise awareness on a continuous basis on the importance of information security, the users' role in securing corporate data, new security threats, and the security measures put in place by the organization. Monitoring and protecting corporate data is also an essential factor in enhancing information security. Organizations have to monitor access to corporate data on a real-time basis and have the capacity to detect and take

quick proactive and reactive actions whenever a security breach occurs. In addition, corporate data should also be separated from personal data so that street security measures are imposed on corporate data without infringing on the privacy of BYOD users.

Adequate software, network and hardware infrastructure is also vital in implementing a robust information security framework. An organization should have a proper financial and sustainability plan that ensures that resources are available and that the implementation of the framework is sustainable. However, a good security framework is characterized by low resource consumption. Having implemented an information security framework, it is also important to ensure that there is continuous monitoring and evaluation of every component of the framework to ensure strict compliance to policies, continuous review, and making adjustments where necessary to enhance optimum performance of the framework. The conceptual framework for this study is summarized in figure 2.6 below.

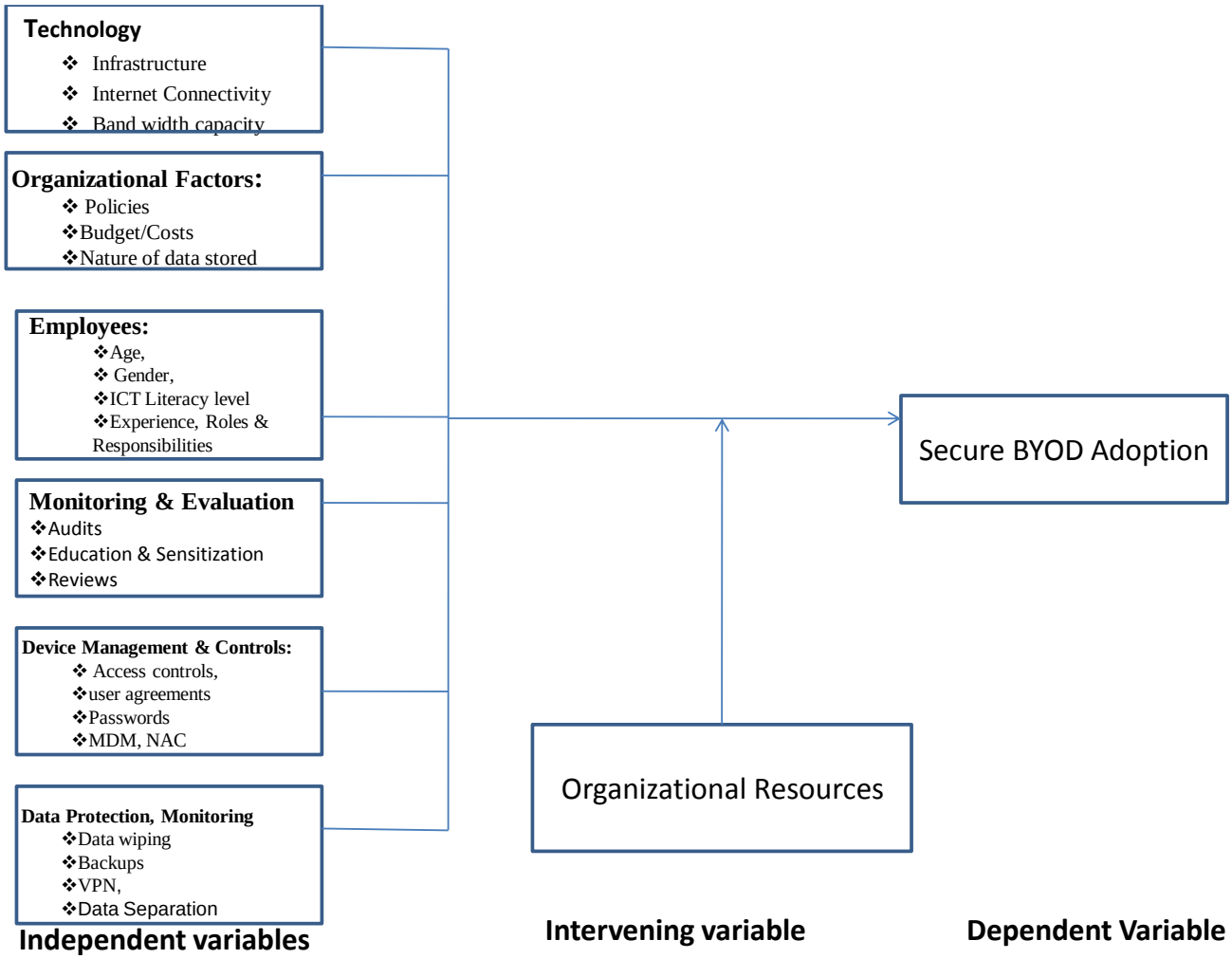


Figure 2.9: The conceptual framework of the developed security framework

2.8 Features and objectives of a BYOD Environment secure for Corporate Data

Based on the Literature review and surveys carried out, the following are the desired goals of a Secure BYOD Environment for BYOD.

Table1: Features and objectives of a BYOD Environment secure for Corporate Data

S/NO	Functionality	How it was achieved in the developed Framework
1	Corporate Data Monitoring and Protection	i. Cryptography and VPN ii. Data Wiping (Locally and Remotely) iii. Creating Mobile Data Backup iv. Locate or lockout the device remotely v. Mobile Information Management Tools vi. Desktop Virtualization models vii. Integrated data security plan
2	Security Policy Enforcement	i. Internet Access Policy ii. Acceptable Use Policy iii. BYOD Policy iv. Regular audits and policy review
3	Mobile Application Security and Integrity	i. Certifications and Signature ii. Trusted Downloading from controlled locations iii. Mobile Application Management (MAM) tools iv. Blacklist & White list Approaches v. Risk Management/Assessment
4	Non-intrusiveness	i. Intrusion detection systems ii. Network Access Control (NAC) iii. Firewalls
5	Space Isolation	Data separation
6	User Access Control and Device Identification	i. Password Policies ii. User agreements iii. Mobile Device Management (MDM) tools iv. Authentication v. Encryption of BYOD devices vi. Network Segregation vii. Role-Based Access Controls (RBAC) viii. Determining devices/platforms to be allowed ix. Compatibility testing
7	Low Resource Consumption	i. Financial and sustainability plan ii. Network Infrastructure plan
8	Training and sensitization	i. Regular sensitization of all users ii. BYOD information portals iii. BYOD education curriculum iv. Operational/procedure manuals
9	Monitoring and evaluation	i. Periodic audits ii. Continuous review of policies iii. Continuous improvement of controls iv. Continuous BYOD education v. Being up to date with new security measures and tools

CHAPTER THREE

METHODOLOGY

3.1 Introduction

This chapter discusses the methodology that this study adopted. The chapter begins by discussing the research design which details the logical and systematic steps for arriving at the answers to the defined research objectives stated as described by De Vos et al, (2005). The main objective and the specific objectives of the study have been outlined in chapter one. This chapter then proceeds to show the methodological approach which describes the process of planning, design, preparation, data collection, analysis and conclusion of this research study. The chapter then discusses sample selection, questionnaire design, data collection, how data was analyzed, the design and development of the framework and finally how validation was accomplished.

3.2 Research Design

A research design guides the researcher in carrying out the study and provides an implementation framework which determines the planning of the study as well as the collection and analysis of data (De Vos et al, (2005). The research design helps the researcher to get answers to the research questions. Knight (2010) defines it as the architecture of the study which guides the process of collecting and analyzing data and interpreting the output.

The Research Process

This defines the path that was followed in order to achieve the goals and objectives of the study. Figure 3.2 provides a conceptual schema of this research process.

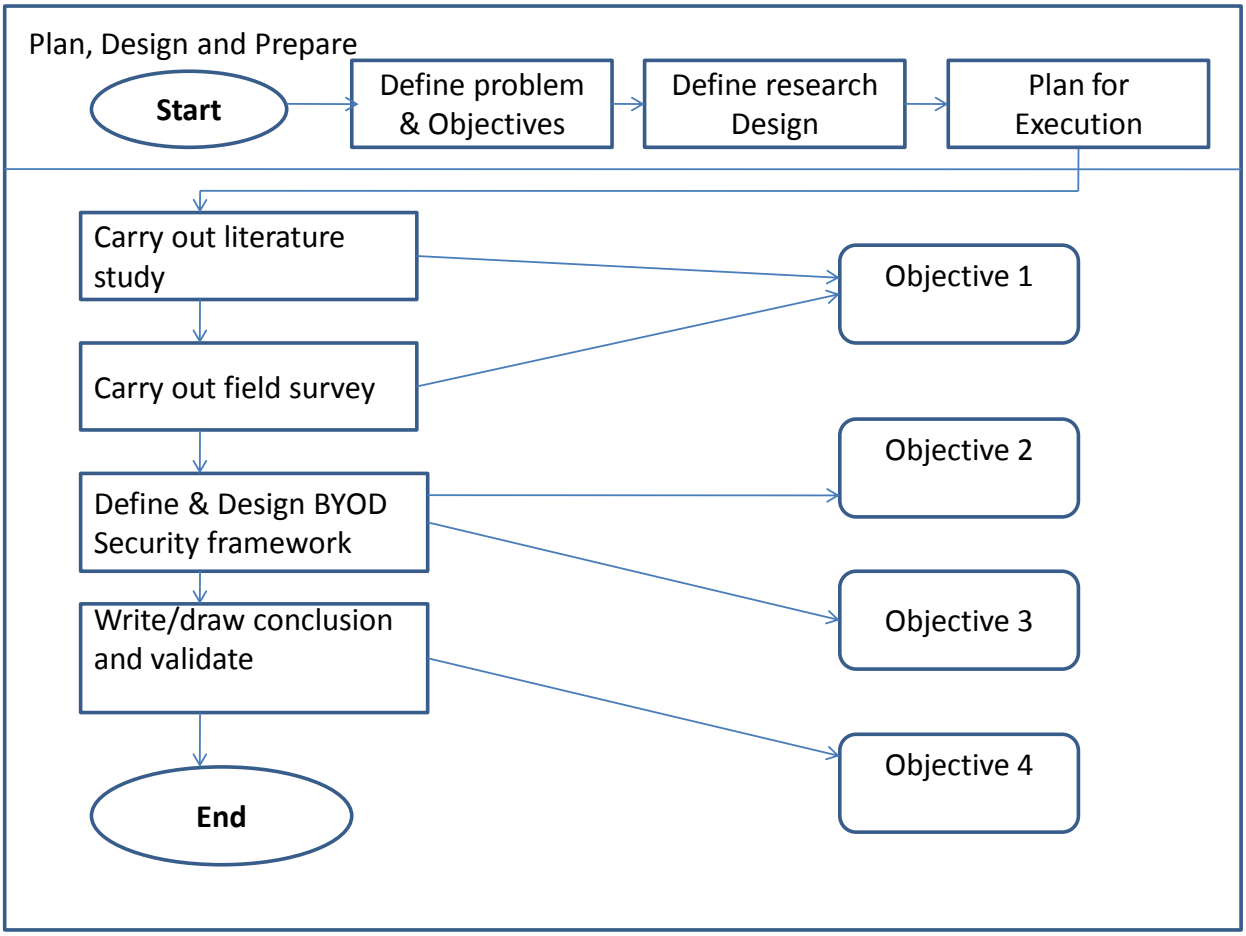


Figure 3.2: Conceptual schema of the research process

This study adopted an exploratory survey in order obtain a deep understanding of the security challenges facing BYOD adoption in government agencies. Through exploratory research, it was possible to gain more insight on the research topic and enabled the researcher to delve deeper into the phenomenon of interest (Mooi & Sarstedt, 2011). A survey approach was also considered to be appropriate for this study because of the interest in answering the research questions regarding BYOD adoption and security challenges in a population of government agencies. A survey approach is extensive and accurately provides targeted results when

administered appropriately (Mathiyazhagan, 2010). The survey was conducted using a questionnaire which included both open-ended and closed-ended questions.

3.3 Population and Sampling

3.3.1 Population

The target population for this study was the ICT personnel or managers in the government agencies in Kenya. The choice of ICT personnel as the targeted population was informed by the fact that this group of people were at the core of information security management in their organizations. Therefore, they were best suited to provide responses and insights that would be useful in addressing the research questions.

3.3.2 Sampling

The study adopted a purposive sampling approach. According to Lee and Lings (2008), purposive sampling is appropriate when the researcher needs to choose the respondents based on how relevant they are to the specific research questions. Based on the research questions for this study, only ICT personnel, or managers in government agencies and parastatals that have implemented BYOD were selected. This was to ensure that the informants in the survey had the competence and understanding of the research topic (Elbanna 2010).

3.3.3 Sample size

The survey was rolled out to participants (ICT heads) in government agencies which is a total of around 200. Out of this number, a total of 90 were randomly selected for the study and only those who indicate that they have implemented or tried to implement or are planning to implement BYOD were considered for the study.

3.4 Questionnaire design and data collection

The data collection technique for this study was the use of a questionnaire. The questionnaire was designed to address each specific research question and included both open-ended and closed-ended questions. Open-ended questions were useful in the exploratory study because they allowed the researcher to obtain deeper insights into specific issues in the study. The inclusion of both structured and unstructured questions is based on recommendations by Mooi and Sarstedt (2011) that the degree of structure is an important consideration in designing a questionnaire. A proper design enhances the validity and reliability of the data collected.

The questionnaire was administered through Survey Monkey online survey tool. The link to the survey was sent to the respondents via email. Survey Monkey was convenient for the respondents since all of them were IT savvy and allowed them to respond to the questions at their own time and in an online environment that they are used to. The questionnaire included an introductory letter (see appendix I) that informed the respondents about the purpose of the survey. The letter also highlighted the ethical guidelines that guide the study. Respondents were assured that the information they provided would be treated with utmost confidentiality and that it would be used only for purposes of the study in an aggregate form. Responses were not linked to the individual respondents. The letter also provided contact details for the University in case a respondent would need to inquire or raise an issue regarding the study directly to the university. Once a respondent completes the questionnaire, the researcher would receive a notification from Survey Monkey.

3.5 Data Analysis

The objective of this section was to organize the raw data into an easily manageable form and apply statistical techniques to make inference through patterns and summaries (Mugenda

&Mugenda, 2003). Data from completed questionnaires were collated and checked for errors and then tabulated for purposes of analysis. Frequency distribution tables, means and standard deviation for the data were obtained in order to understand the distribution and tendency of the data. Percentages were also obtained in order to present and interpret the responses for each question. The results were presented in form of tables, graphs and charts and inference were made from this output.

3.6 Design and Development of the framework

The study used the Design Science Research approach to design and developed the framework. According to McKay, Marshall, Hirschheim (2012), design can be described as shown in the diagram below:

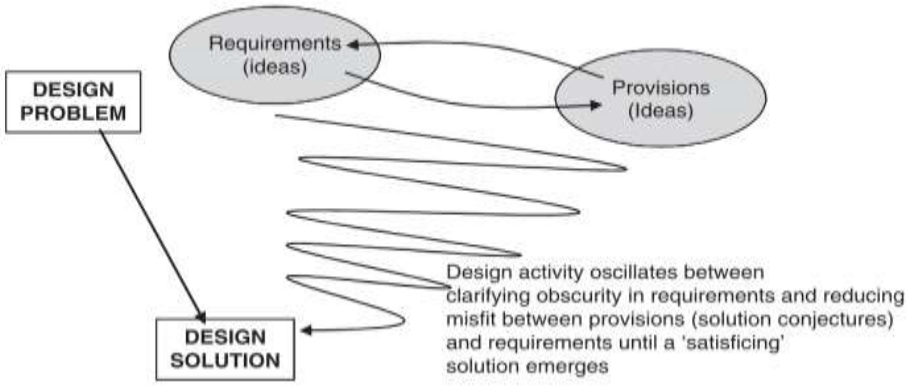


Figure 3.3:McKay, Marshall, Hirschheim: The design construct in information systems design science. JIT (2012) 27, 125–139

CHAPTER FOUR

RESEARCH FINDINGS AND DISCUSSIONS

4.1 Introduction

In this chapter, the study presents the results achieved for each of the four objectives of the study.

Objective number 1

The first objective of the study was to identify the extent of BYOD adoption in Government agencies in Kenya and to review the existing BYOD security frameworks and related security challenges.

To achieve this objective, analysis of data that was collected was carried out. The data was collected through questionnaires administered through the Survey Monkey online survey tool. The tool was chosen because it creates convenience for the respondents by enabling them to respond to the questions at their own convenient time and in an online environment which they are used to as IT personnel. As a result of this approach, the study was able to realize an average turnaround time of fourteen (14) days on the responses.

The link to the online survey was sent through email to 90 respondents in Government ministries and parastatals/agencies. Out of the 90 respondents targeted, 47 completed the questionnaire. This represents a response rate of 52.2%. The response rate was within the recommendation given by Mugenda and Mugenda (2003) that a response rate of 50% is adequate for carrying out analysis and making conclusions in a study. Baruch (1999) also studied the average response rates in academic studies and found that the response rates were between 48.4% and 55.6%.

4.2 Demographic Information

4.2.1 Type of Government organization

Figure 4.1 below shows the composition of the Government organizations from which the study received the responses. There were 8 respondents from ministries and 39 from government agencies/parastatals.

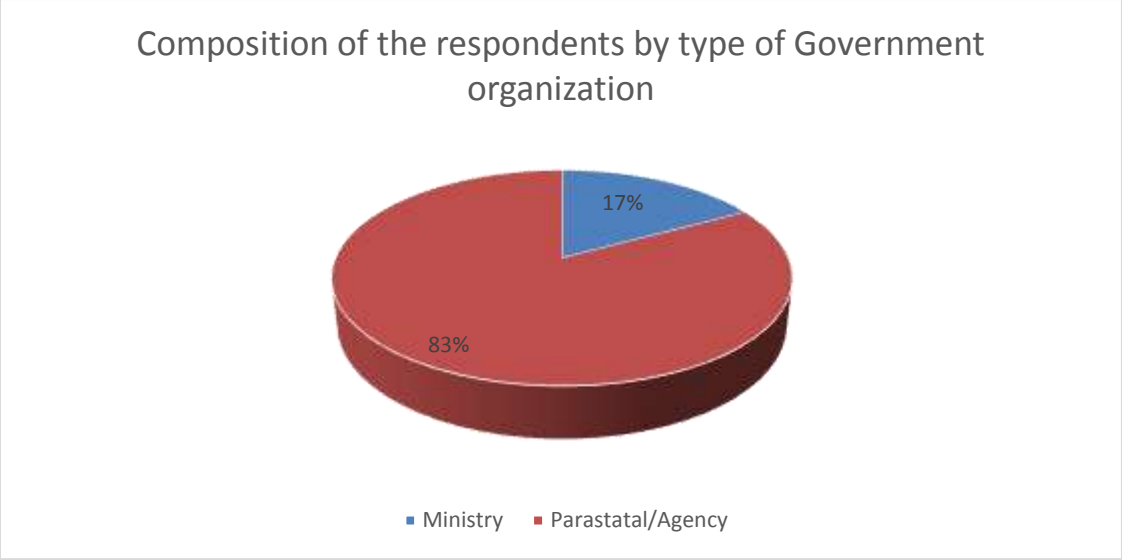


Figure 4.1: Composition of the respondents by type of Government organization

4.2.2 Role of the respondent in the organization

The study sought to establish the role or job title of the respondent in the organization in order to ensure that the respondents were in positions that put them at the core of ICT operations or Information Security in the organization. This was to enhance the reliability of the results. Figure 4.2 below shows a summary of the number of respondents and their roles.

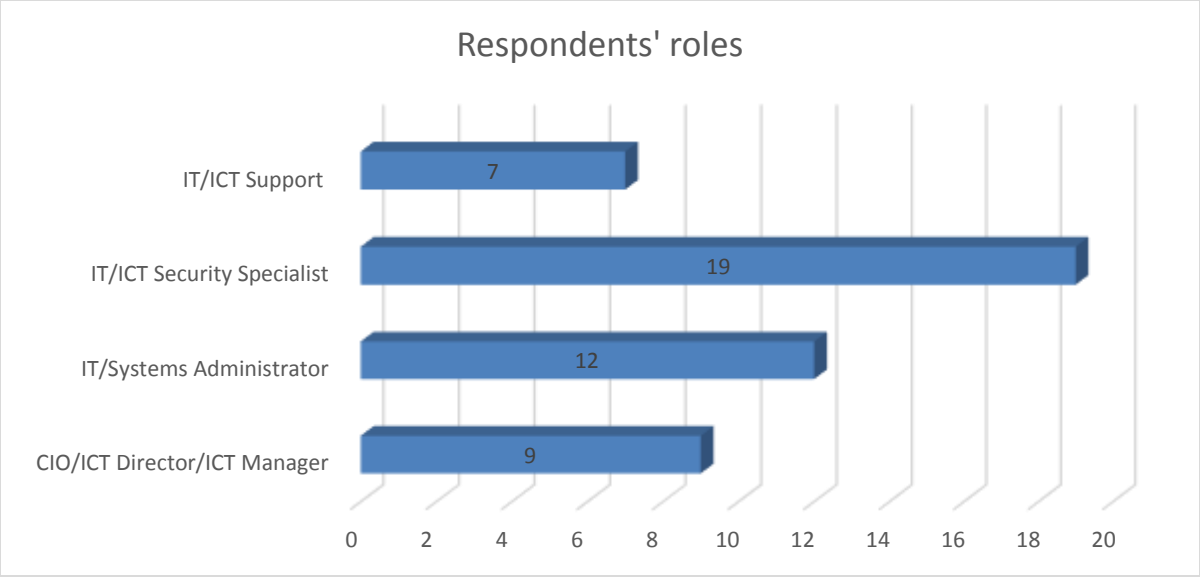


Figure 4.2: Respondents' roles

From the results in table 4.2 above, the highest number of respondents were Information Security specialists followed by IT/Systems administrators. Chief Information Officer (CIO)/ICT Director/ICT Manager roles had 9 respondents while IT support role had 7 respondents.

4.2.3 Age of the respondents

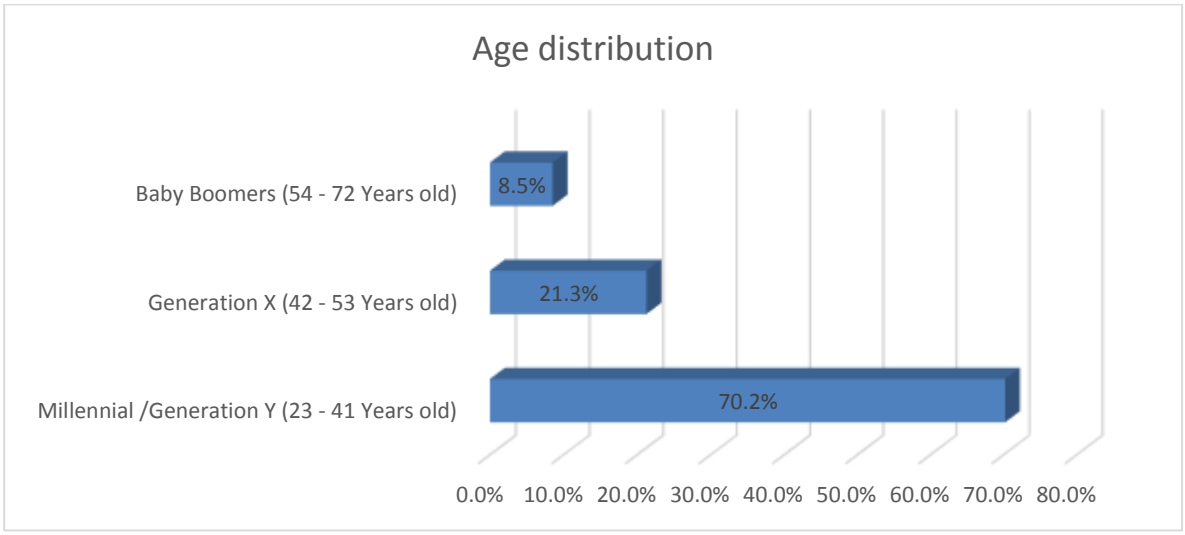


Figure 4.3: age/generational distribution of the respondents

As shown in figure 4.3 above, 70.2% of the respondents were Millennials/Generation Y (Born between the year 1977 and 1995) while 21.3% were Generation X (Born between the year 1965 and 1976). Only 8.5% of the respondents were aged above 54 years.

4.2.4 Level of experience of the respondents

The study also sought to understand the level of experience of the respondents in their current role and in the ICT industry in general. Figure 4.4 and 4.5 below show the summary of the results.

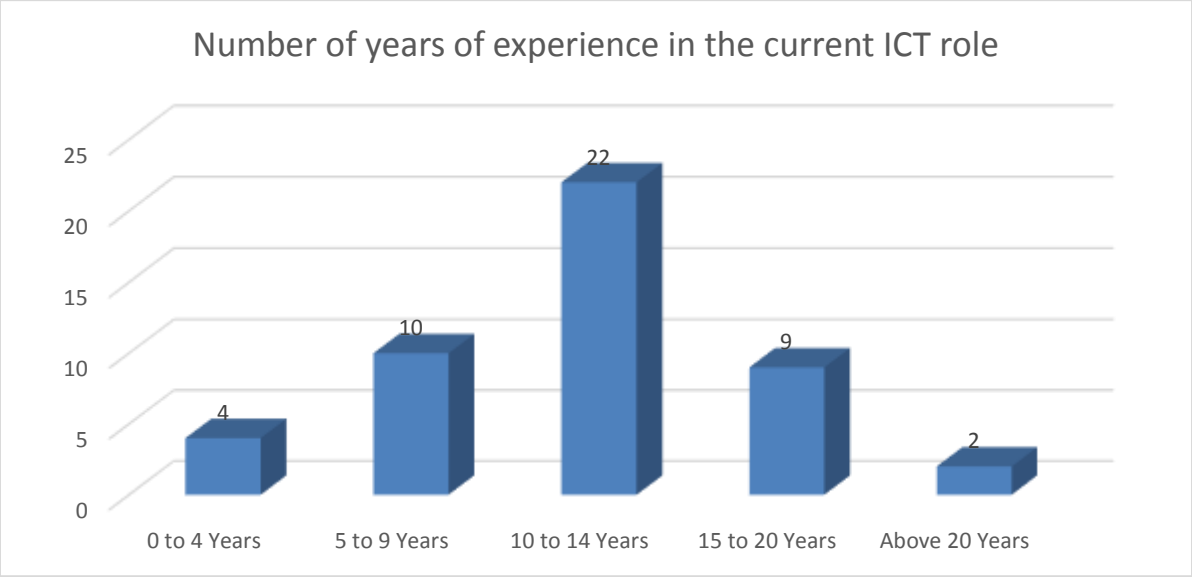


Figure 4.4: Number of years of experience in the current ICT role

The highest number of respondents had 10 to 14 years' experience in their current ICT role while the lowest number had more than 20 years' experience. The mean number of years of experience was 9.4 years with a standard deviation of 7.79.

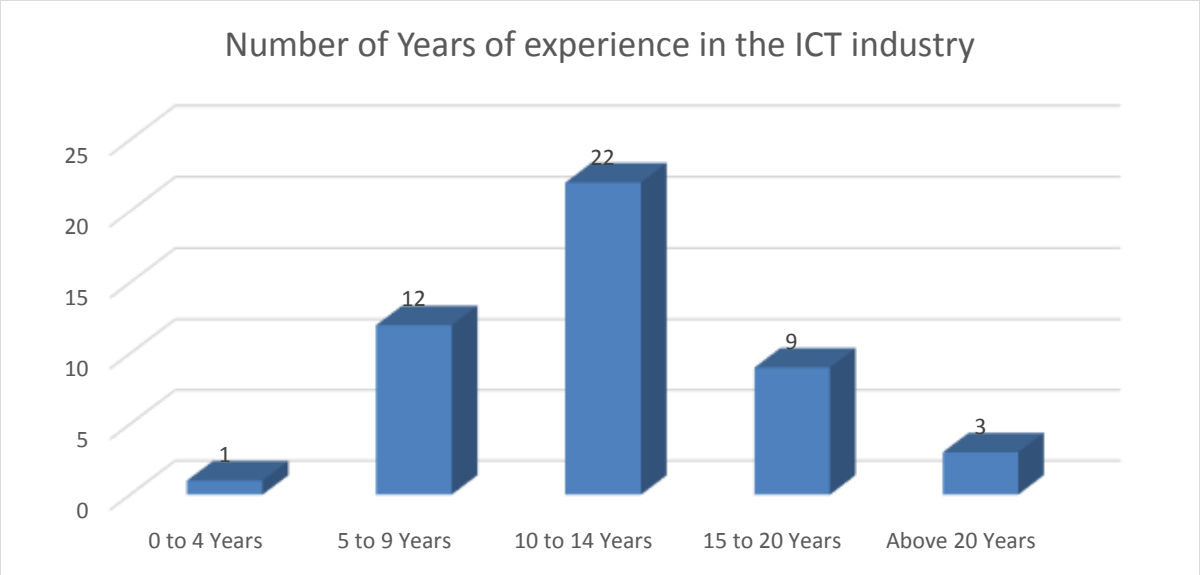


Figure 4.5: Number of Years of experience in the ICT industry

The highest number of respondents had 10 to 14 years' experience in the ICT industry while the lowest number had 0 to 4 years' experience.

4.3 Extent of Bring Your Own Device (BYOD) adoption

The first specific objective of the study was to identify the extent of BYOD adoption in Government agencies in Kenya. In order to achieve this objective, the study sought various responses from the ICT professionals and the results are presented below.

4.3.1 BYOD adoption

The study began by asking the respondents whether their organizations had ever implemented BYOD. Figure 4.6 below shows a summary of the results.

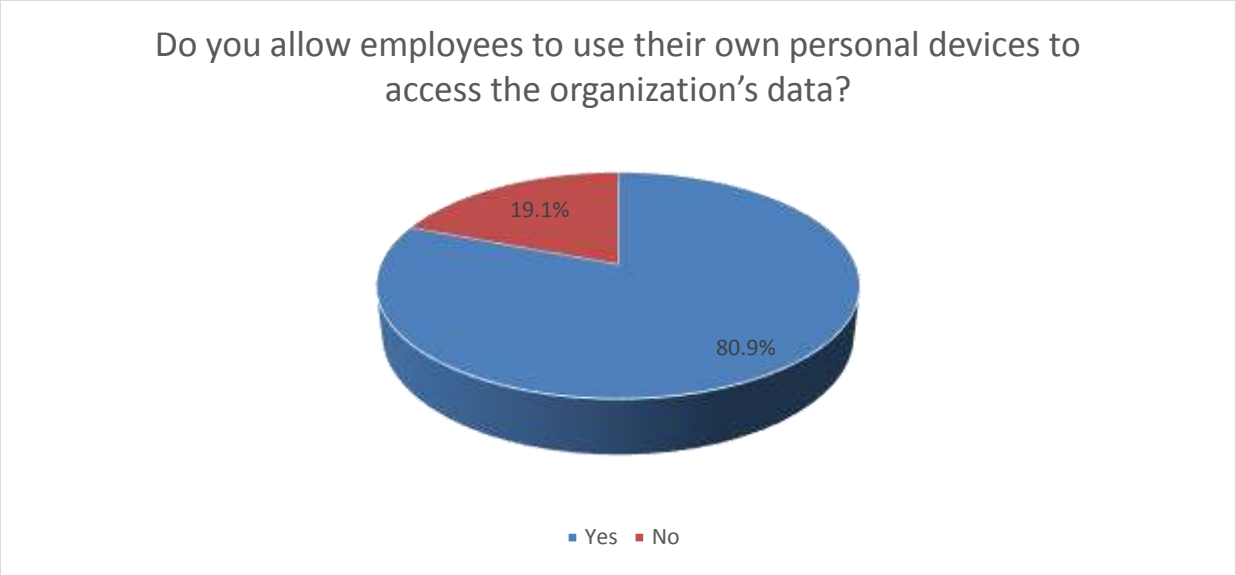


Figure 4.6: BYOD adoption

From the results in figure 4.6 above, 80.9% of the respondents indicated that their organization allows or has ever allowed BYOD in the workplace while only 19.1% had not. This implies that a large number of ministries and parastatals/agencies have allowed their employees to bring their own devices to the workplace and use them to access organizational data or resources.

4.3.2 Reasons for not adopting BYOD

As a follow up on the respondents who had indicated that their organizations had not adopted BYOD, the study sought to establish the reasons why this was the case. Figure 4.7 below shows a summary of the reasons given by the respondents and the extent of each reason.

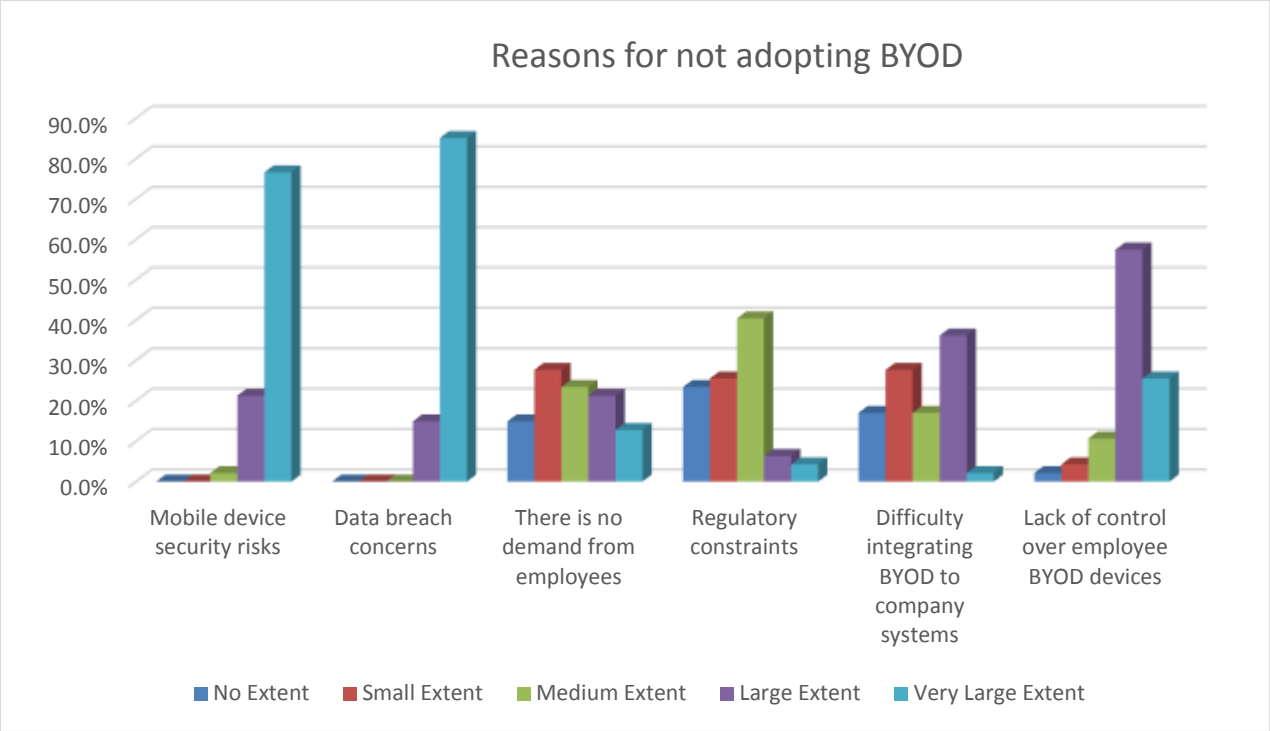


Figure 4.7: Reasons for not adopting BYOD

From the results in figure 4.7 above, mobile device security risks and data breach concerns were identified as the factors hindering the adoption of BYOD to a very large extent. The percentage of respondents who indicated that these reasons hindered BYOD adoption to a very large extent were 76.6% and 85.1% respectively. In addition, 21.3%, 14.9%, 57.4% and 36.2% of the respondents also indicated that mobile device security risks, data breach concerns, lack of control over employee BYOD devices, and difficulty integrating BYOD to company systems respectively, hindered BYOD adoption to a large extent.

4.3.3 Potential benefits of BYOD adoption

The respondents also indicated the potential benefits of successful BYOD adoption in their organizations. Figure 4.8 below shows a summary of the results.

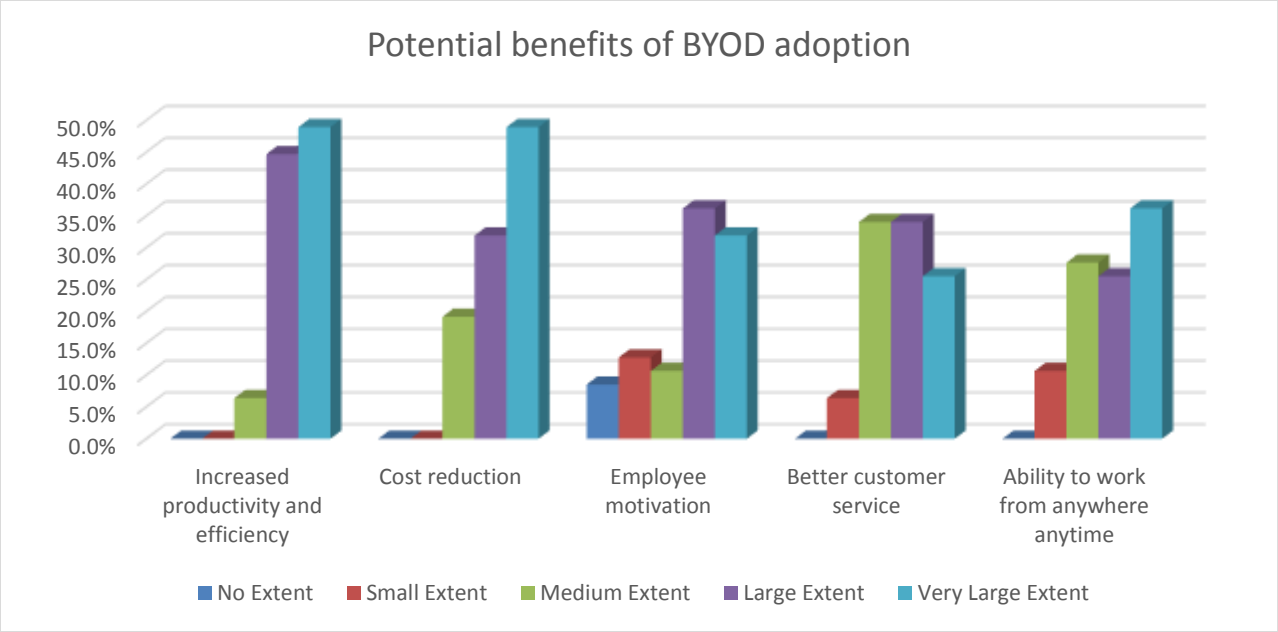


Figure 4.8: Potential benefits of BYOD adoption

From the results in figure 4.8 above, 48.9%, 48.9%, 31.9%, 25.5%, and 36.2% of the respondents indicated that increased productivity and efficiency, cost reduction, employee motivation, better customer service and ability to work from anywhere anytime respectively, were the potential benefits of BYOD adoption a very large extent. The percentage of respondents who indicated that increased productivity and efficiency, cost reduction, employee motivation, better customer service and ability to work from anywhere anytime were the potential benefits of BYOD adoption to a large extent were 44.7%, 31.9%, 36.2%, 34.0% and 25.5% respectively.

4.4 BYOD Benefits, Security frameworks and related security challenges

The second objective of the study was to review the existing BYOD security frameworks and related security challenges in Government agencies/parastatals in Kenya. This section presents the results relating to the security challenges or risks faced by the Government organizations that have implemented BYOD, benefits that these organizations have derived from BYOD adoption so far, and the security frameworks that are currently in place to address BYOD security risks.

4.4.1 Duration since the adoption of BYOD

The respondents indicated the number of years that have elapsed since their organization adopted BYOD. Table 2 shows a summary of the results.

Mean	5.5
Median	6
Mode	3
Standard Deviation	2.97
Range	9
Minimum	1
Maximum	10

Table 2: summary of the results

The maximum duration was 10 years while the minimum was 1 year. The mean duration was 5.5 years while the most common was 3 years.

4.4.2 Group/Level of employees that are allowed to access organizational resources through BYOD and the devices they are allowed to use.

The study also sought to understand the group or level of employees allowed to use various BYOD devices. The objective was to establish whether organizations restrict the use of particular BYOD devices to particular groups or levels of staff. Figure 4.10 below shows a summary of the results obtained.

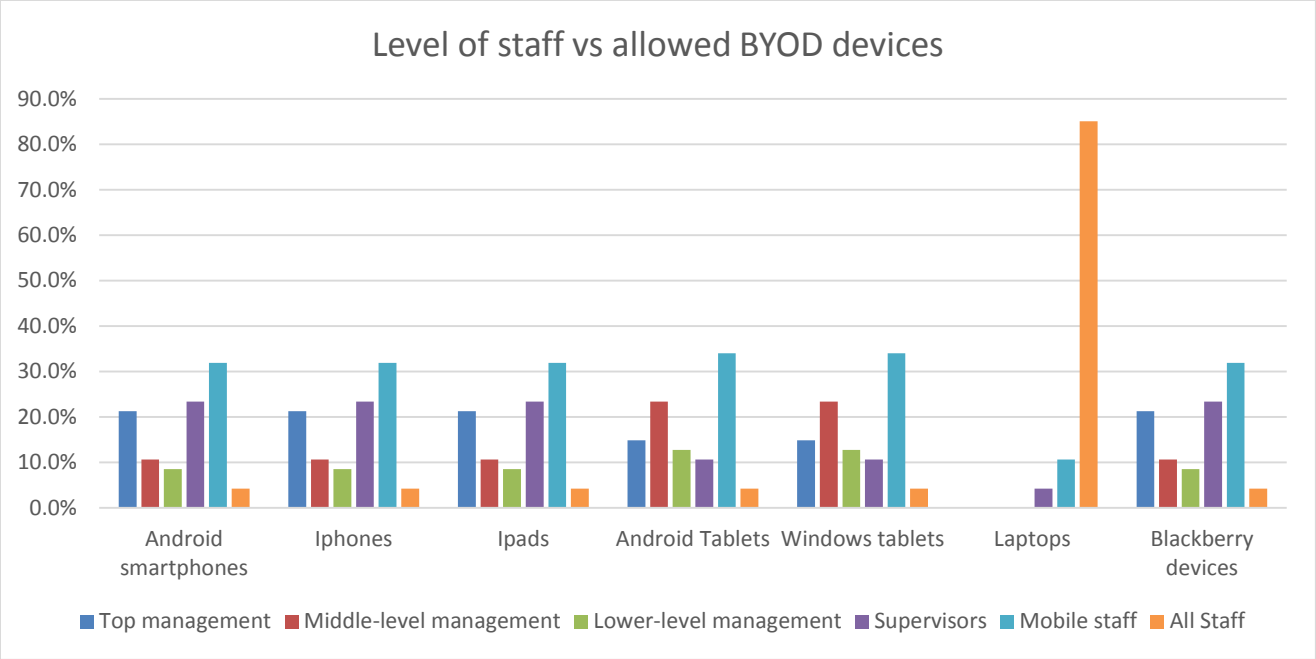


Figure 4.9: Group/Level of employees and the BYOD devices they are allowed to use

Table3 also shows the percentage of respondents per BYOD device and per level of staff

	Top management	Middle-level management	Lower-level management	Supervisors	Mobile staff	All Staff
Android smartphones	21.3%	10.6%	8.5%	23.4%	31.9%	4.3%
Iphones	21.3%	10.6%	8.5%	23.4%	31.9%	4.3%
Ipads	21.3%	10.6%	8.5%	23.4%	31.9%	4.3%
Android Tablets	14.9%	23.4%	12.8%	10.6%	34.0%	4.3%
Windows tablets	14.9%	23.4%	12.8%	10.6%	34.0%	4.3%
Laptops	0.0%	0.0%	0.0%	4.3%	10.6%	85.1%
Blackberry devices	21.3%	10.6%	8.5%	23.4%	31.9%	4.3%

Table3: percentage of respondents per BYOD device and per level of staff

4.4.3 Extent to which employees access organizational resources using BYOD.

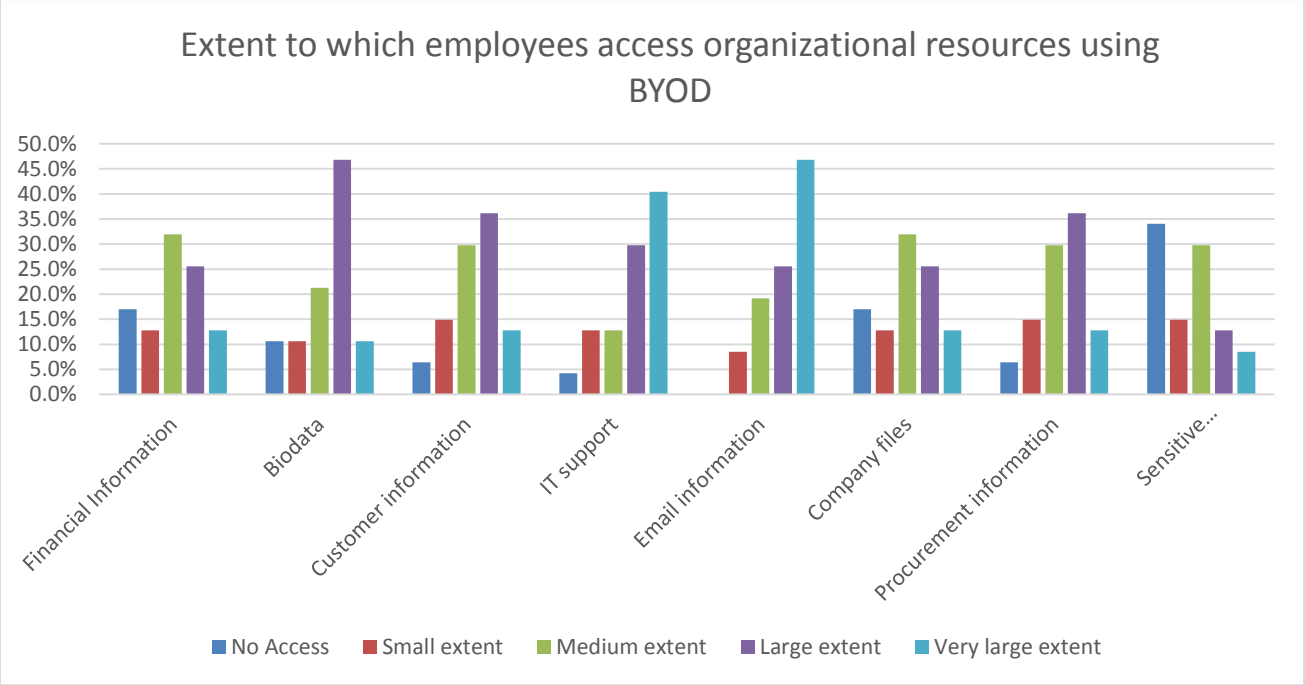
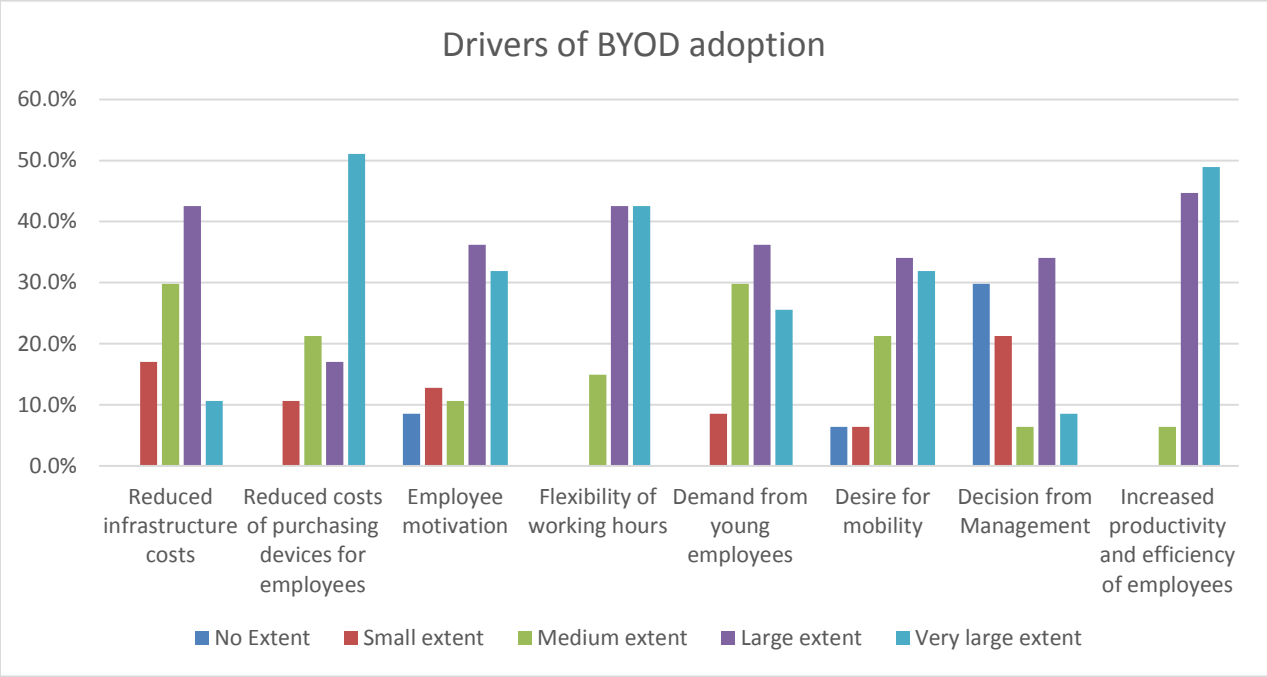


Figure 4.10: Extent to which employees access organizational resources using BYOD

From the results in figure 4.10 above, the largest percentage of respondents indicated that employees use BYOD to access IT support information and email information to a very large extent. Biodata, customer information and procurement information is accessed through BYOD to a large extent while financial information and company files are accessed through BYOD to a medium extent. On sensitive government data, the largest percentage of respondents indicated that employees do not access this information through BYOD. However, this was followed closely by respondents who indicated that employees access the sensitive government data through BYOD to a medium extent.

4.4.4 Key drivers of BYOD adoption

Figure 4.11 Key drivers of BYOD adoption

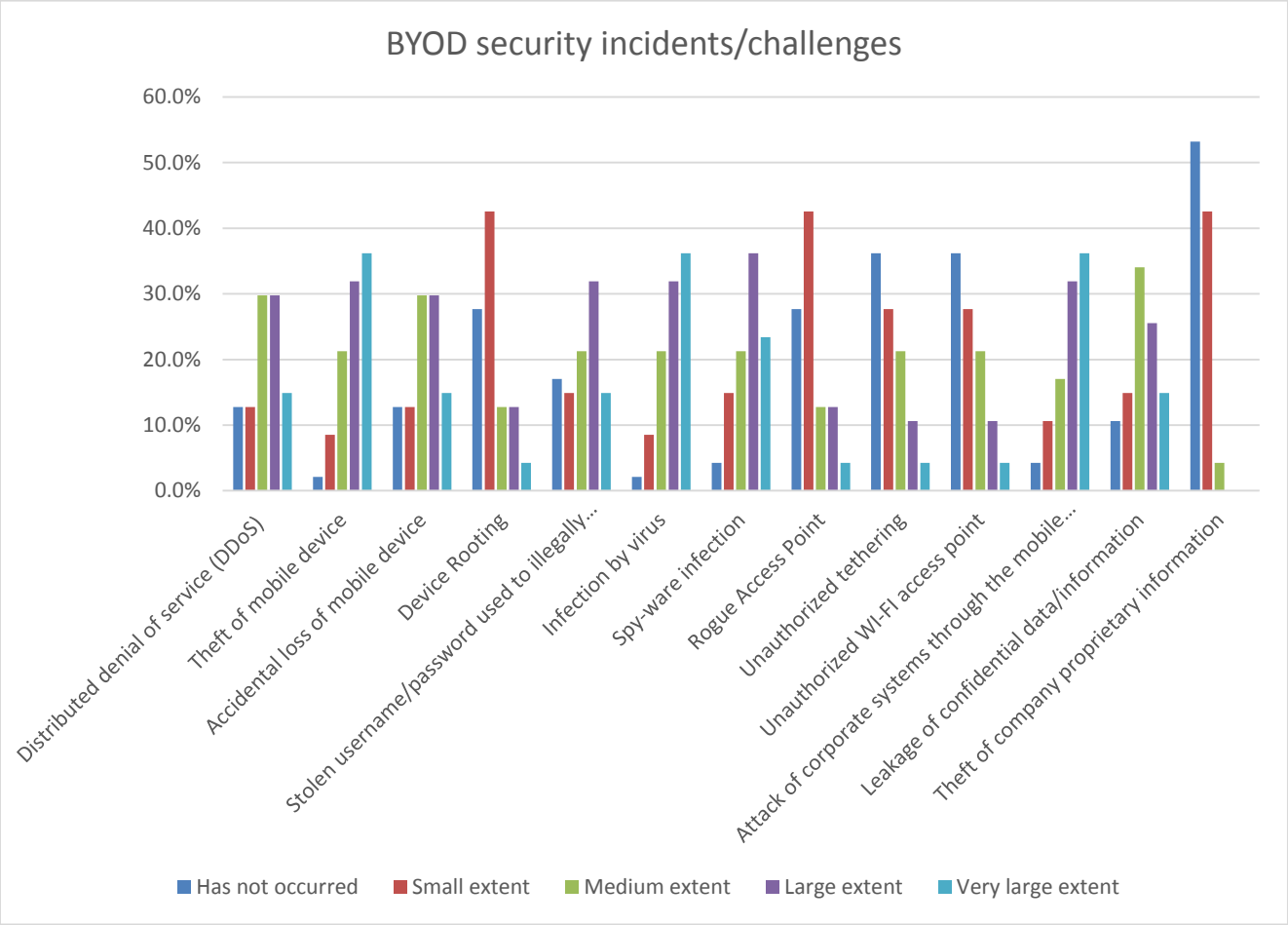


The largest percentage of respondents identified increased productivity and efficiency, flexibility of working hours and reduced cost of purchasing devices for employees as the factors that drive the adoption of BYOD to a very large extent. Reduced infrastructure costs, employee motivation, demand from young employees, desire for mobility, and management decision were identified by the largest percentage of respondents as drivers of BYOD adoption to a large extent.

4.4.5 Security incidents/challenges encountered since the adoption of BYOD.

The study also sought to establish the specific security challenges or incidents that the government organizations have faced since adopting BYOD. This would form a basis upon which the study developed and recommend a holistic framework to address the BYOD-related security risks. The results are presented in figure 4.12 below.

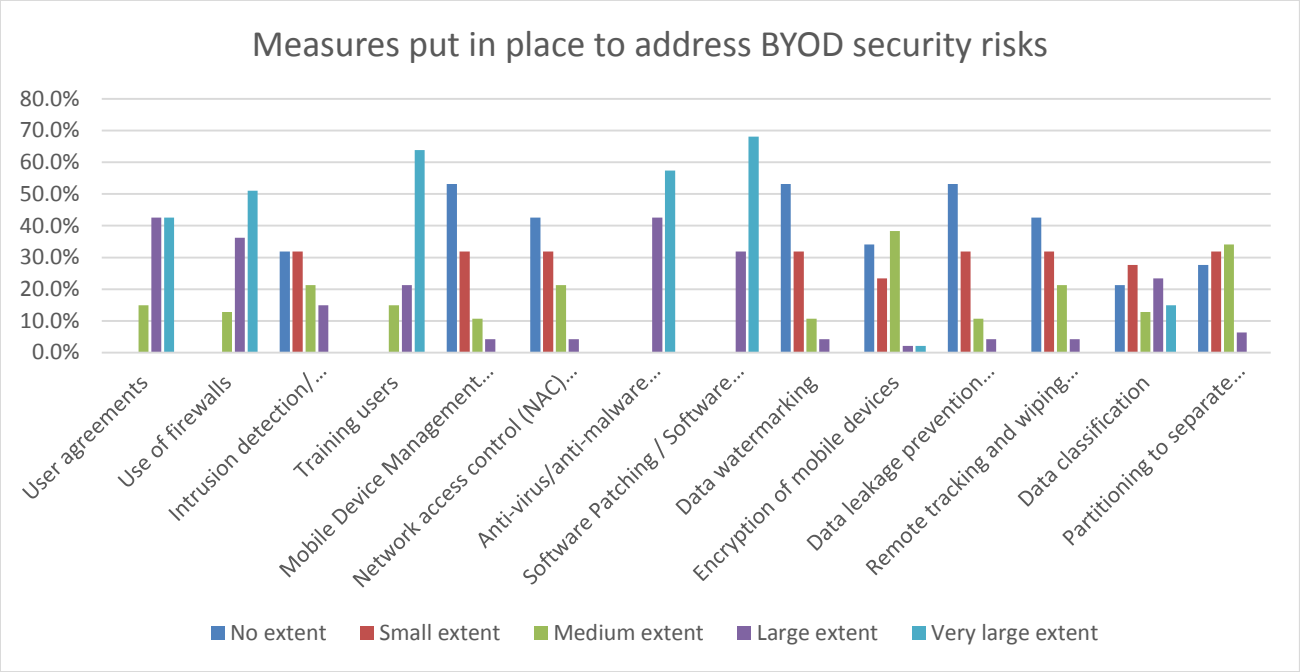
Figure 4.12 BYOD security incidents/challenges



The largest percentage of respondents indicated that theft of mobile devices, infection by virus and attack of the corporate systems through the mobile devices had occurred to a very large extent. Distributed denial of service, accidental loss of mobile devices, illegal access of corporate systems through stolen passwords, and infection by spy-ware had also occurred to a large extent.

4.4.6 Measures put in place to address BYOD security risks

Figure 4.13 Measures put in place to address BYOD security risks

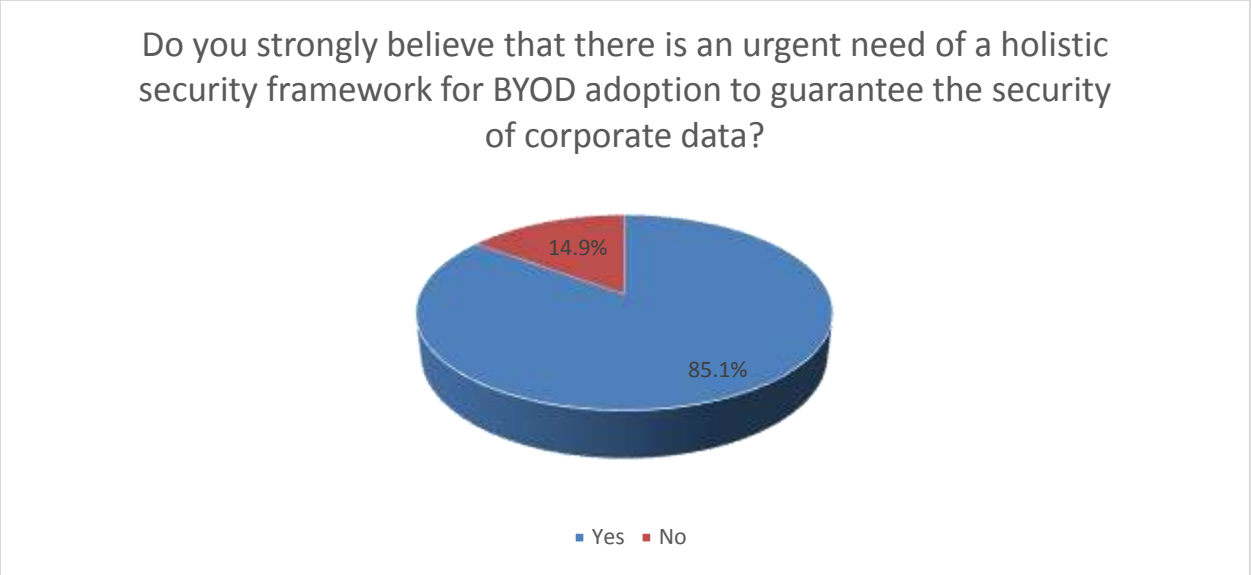


The largest percentage of respondents indicated that the security measures implemented to a very large extent to address BYOD-related security risks include user agreements, firewalls, user training, anti-virus/ anti-malware software, and regular updates on their software.

4.4.7 Need for a holistic security framework for BYOD adoption to guarantee the security of corporate data

The study also asked the respondents whether they believed that there was an urgent need for a holistic security framework to guarantee the security of corporate data in a BYOD environment. Figure 4.14 below shows a summary of the results.

Figure 4.14 Summary results on the need for a BYOD security framework



As shown in figure 4.14 above, it is clear that a large percentage (85.1%) of the ICT professionals strongly believe that a security framework that addresses BYOD-related security risks is urgently required in order to enhance successful BYOD adoption and to guarantee the security of corporate data. Therefore the aspirations of the first objective were clearly achieved.

4.5 Design and development of the Framework

In developing the BYOD security framework, the study considered the existing frameworks and the security challenges facing BYOD adoption in government agencies as presented in section 4.4 above. The objective of the framework is to enhance secure adoption of BYOD in government agencies so that these agencies can enjoy the benefits of BYOD adoption without compromising the security of sensitive data that most of the agencies store.

4.5.1 Design of the Framework

Objective number 2

The second objective of the study was to design a BYOD security framework based on the findings of the first objective.

The design of the framework followed the Control Objectives for Information and Related Technologies (COBIT) 5 process reference model developed by ISACA, 2012. The four key pillars or steps of the COBIT 5 model include Planning, Building, Running, and Monitoring. The COBIT 5 model is illustrated in the figure below

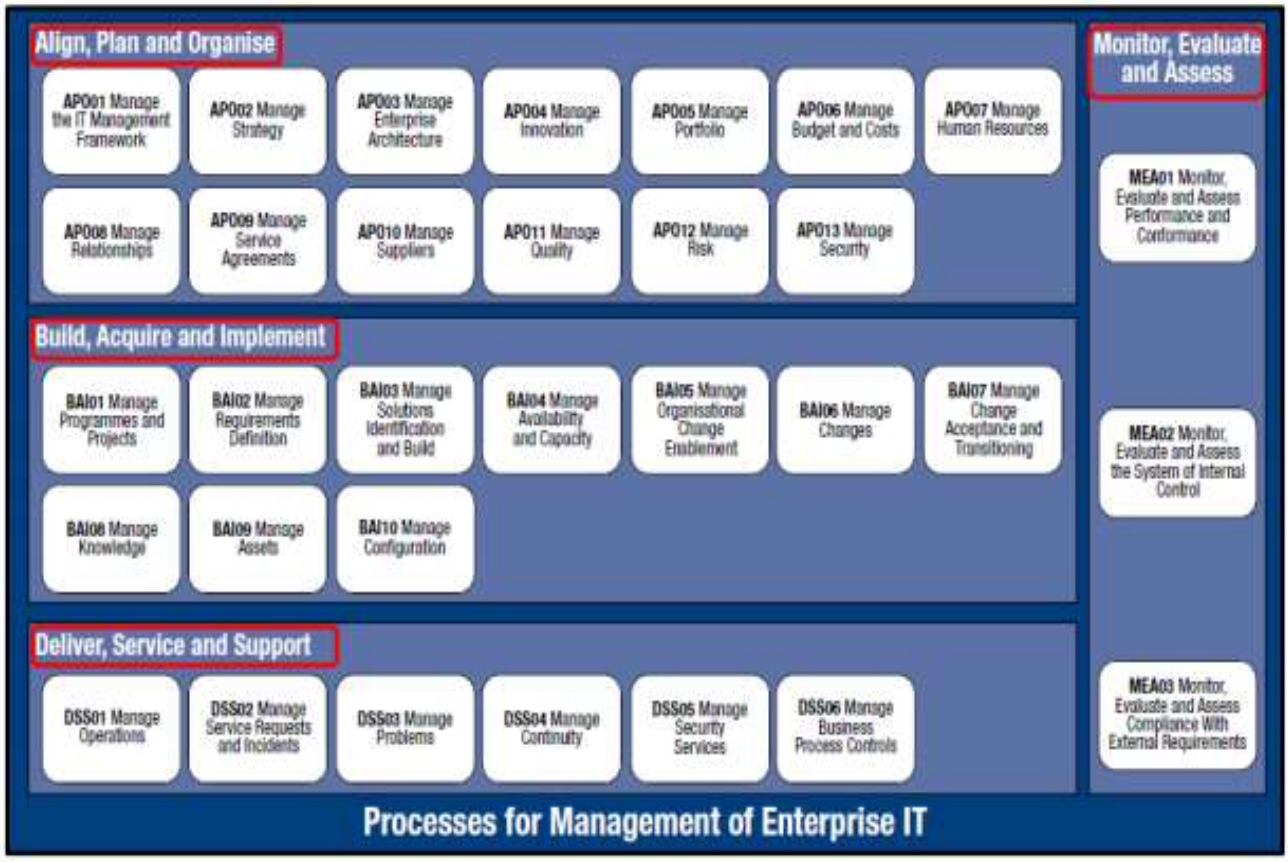


Figure 4.15: The COBIT 5 Process Reference Model Management Domain (ISACA, 2012).

The COBIT 5 Process Model provides a comprehensive coverage of enterprise IT management and incorporates both governance and management processes of IT in an organization (ISACA, 2012). The model is therefore suitable in the implementation and management of key IT activities such as BYOD in an organization. The next section discusses the four phases of the COBIT 5 Process Model in relation to the developed BYOD security framework.

In developing this framework, the study considered the De Kock (2016) security framework as a basis because it was the most current and had already incorporated elements from other frameworks developed earlier. The study also adopted elements from the High Level BYOD Management framework by Fani, von Solms and Gerber (2016), the BYOD Policy Framework for Educational Institutions by Oluranti and Sanjay (2016), the Enterprise and BYOD space BYOD Security Framework by Wang, Wei, and Vangury (2014) and the BYOD framework for a management system by Brodin (2015). The study also incorporated the solutions to the findings on security challenges facing BYOD adoption.

4.5.2 Development of the Framework

Objective number 3

The third objective of the study was to develop a holistic BYOD security framework that would guide government agencies to securely adopt BYOD. To achieve this objective, the development of the framework followed the four phases of the COBIT as illustrated below:

4.5.2.1 Phase 1: Planning

In the planning phase, the factors that need to be considered before implementing BYOD are analyzed. In developing a security framework for BYOD adoption in higher education institutions in South Africa, De Kock (2016) considered development of a BYOD policy, Internet Access Policy and Acceptable Use Policy; Determining devices and platforms to be allowed in BYOD, financial and sustainability plan, Mobile Device Management (MDM) plan, and planning how to address inequality in accessing organizational resources. However, De Kock (2016) did not include critical elements such as analysis of unique security risks and requirements in an organization as in Fani, von Solms and Gerber(2016), employee/user management as in Oluranti and Sanjay (2016) and Fani, von Solms and Gerber (2016), and risk

vs benefit analysis. Figure 4.16 below shows the components of the planning phase in the developed BYOD security framework which took into account the De Kock (2016) framework and included the missing elements. Figure 4.16 below shows the components of the planning phase in the developed BYOD security framework.

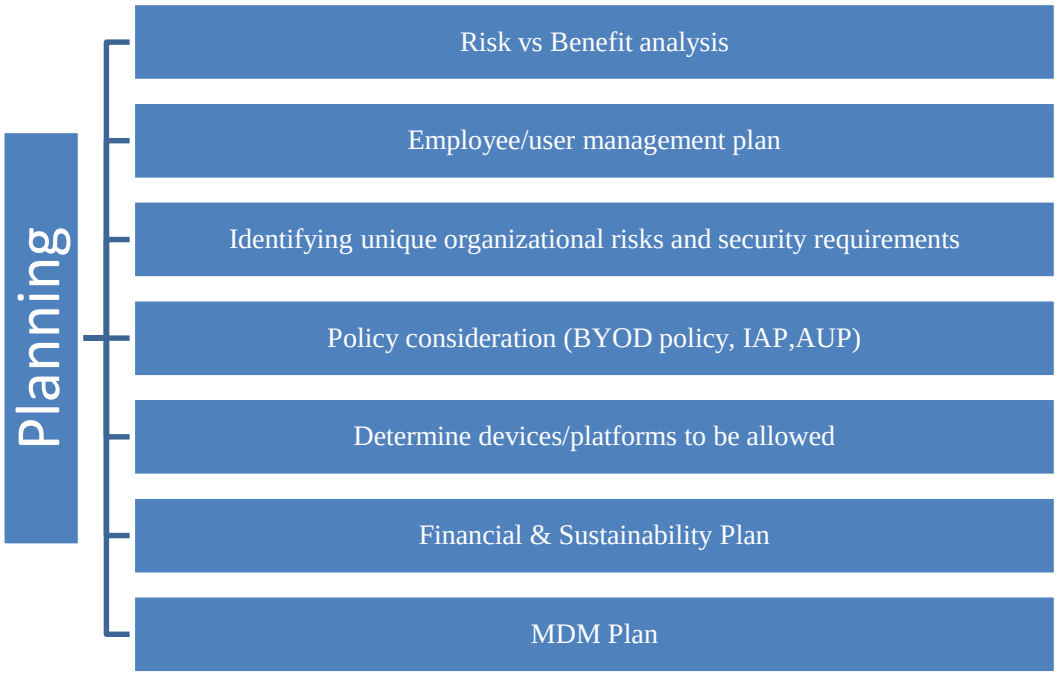


Figure 4.16: Planning Phase of the developed BYOD Security Framework

BYOD Risk vs Benefit Analysis

Before implementing BYOD, government organizations need to carry out a risk versus benefit analysis which involves comparing the possible benefits of adopting BYOD and the magnitude of possible security risks that the organization will be exposed to upon adopting BYOD. This was adopted from the BYOD framework for a management system by Brodin (2015). A cyber security report by Serianu (2015) identified government organizations as the most vulnerable organizations to cyber security risks. Some government organizations possess very sensitive

information that can easily land in the wrong hands. An organization-specific risk versus benefit analysis of BYOD adoption will therefore help a government organization determine whether to avoid BYOD completely, allow specific devices only, allow specific users only, or fully adopt BYOD accompanied with additional security measures to safe guard the security of information.

Employee/User Management

According to the Kenya Cyber Security Report (2016), cyber security risks are higher when a high percentage of employees with personal devices have multiple access to databases, email accounts and applications. Matinde (2015) also noted that employees can bypass company security protocols thus exposing the organization's data to risk. According to Olalere (2015), most data leakages in organizations are caused by employees. The findings of this study also indicated that loss of sensitive information and attack of the corporate systems through the mobile devices had occurred to a large extent. Therefore, an employee/user management plan is a critical element of BYOD security framework. The plan would include determining eligibility of an employee to use BYOD, registration of BYOD users, and user awareness/education plan.

Identifying unique organizational risks and security requirements

The extent of exposure to information security risks is different from one agency to another. Every agency should therefore analyze the specific information security risks that it is most vulnerable to. The analysis should include rating the severity of the risks as high, medium or low. This analysis will determine various aspects of BYOD adoption such as the devices and users to be allowed and security measures to be implemented. In analyzing the security requirements, an organization should consider the risks to the organization's information,

regulatory issues concerning BYOD implementation, and organizational security requirements (Fani, von Solms and Gerber (2016).

Policy consideration

As organizations plan to implement BYOD, it is important to develop various policies to enhance secure adoption (Oluranti& Sanjay, 2016). These policies include an Internet Access Policy, Acceptable Use Policy, and a BYOD policy.

Internet Access Policy (IAP)

In a BYOD environment, an Internet Access Policy (IAP) helps in management and governance of an organization's internet resource. It enhances responsible use of the internet by employees. The policy should clearly state type of websites that employees are allowed to visit, and that the organization has the right to block sites that may pose an information security risk to the organization. Depending on the type of government organization, the IAP may also state that the organization has a right to track employee's activity on the internet while on the organization's network as an additional security measure. The IAP should also describe the controls that may be implemented by the organization to enhance security of its network, procedure for allowing external third parties to access the organization's network, responsibility for managing the organization's internet resource, and consequences for breaching the policy.

Acceptable Use Policy (AUP)

According to Green (2007), AUP guides in the management of information systems by outlining what a user is authorized or prohibited to access, as well as the consequences for violation. Since government information systems contain huge volumes of sensitive information, AUPs should

clearly specify that ICT resources and information that employees are allowed to access are strictly for purposes of executing their duties in the organization and not for any other purpose. All first time users must sign the AUP before being allowed to access the organization's network.

Determining devices/platforms to be allowed

BYOD devices used by employees may come in many open mobile platforms and operating systems hence making them vulnerable to security breaches (Salem et al, 2008). In addition, the technology savvy generation, which accounts for most BYOD users is enthusiastic about the sense of fashion, and greater capability and flexibility of the latest devices and therefore, they are quick to purchase them and bring to the workplace (Trend Micro, 2012). Some of these latest devices lack strong security architecture because they are still new in the market (Leavitt, 2013). Government organizations should therefore determine a range of allowable devices and platforms. In addition, they should come up with guidelines and recommendations to help their employees when purchasing the devices. Minimum security requirements that must be met by any device should also be provided so that employees consider them before purchasing a BYOD device.

Financial and sustainability plan

Like other corporate organizations, government organizations strive to remain agile and up to date in terms of technology. In order to sustainably adopt BYOD, government organizations need to plan for the resources that will be required to achieve the goal. This involves planning for adequate bandwidth, IT infrastructure and the necessary human resources to support additional devices in the organization's network to avoid overstretching the already existing resources and

causing inefficiency (Probert, 2012). The organization should also develop a Business Continuity Plan (BCP) which includes a disaster recovery plan and a contingency plan.

Mobile Device Management (MDM) plan/strategy

A Mobile Device Management (MDM) strategy is very useful in monitoring and managing devices that connect to the organization's network. An MDM solution can be used to control devices remotely through a central management console. Using this solution, government organizations can be able to track lost or stolen devices and lock them or wipe the data therein to avoid sensitive data landing in the wrong hands.

Phase 2: Build

In the build phase, the organization should put in place the necessary software and network infrastructure in order to facilitate the translation of the elements of the planning phase into actual implementation (De Kock2016). Other activities in the build phase should include putting in place the necessary platforms and prerequisites for BYOD education, procuring the required tools/services, and implementing a data security plan.

Network Infrastructure

In addition to a Local Area Network (LAN), an organization should also consider a Wireless Local Area Network (WLAN) to ensure that BYOD devices can connect to the organization's LAN anywhere within the organization. To enhance the security of WLAN, government organizations should also ensure that they deploy a Virtual Private Network (VPN). In order to avoid straining the network as a result of increased number of devices accessing the organization's network, the organization should also ensure that there is sufficient bandwidth.

Controls should also be put in place to manage traffic and ensure fair usage. The organization could also consider segmentation and role-based access controls (RBAC) to control access to the organization's servers based on an employee's role.

Software Infrastructure

Adoption of BYOD presents increased information security risks that traditional security software may not adequately address. The fact that BYOD devices used by employees may come in many open mobile platforms and operating systems and that the devices may still be new in the market and therefore lack strong security architecture, may present additional security challenges (Salem et al, 2008; Leavitt, 2013). Government organizations should consider developing or purchasing additional software applications such as MDM tools, Network Access Control (NAC) tools, Mobile Application Management (MAM) tools, Mobile Information Management (MIM) tools, and Desktop Virtualization models (Downer & Bhattacharya, 2018).

BYOD education platforms and prerequisites

As a prerequisite to BYOD education and awareness creation among employees in government organizations, the ICT department should develop a curriculum that contains a detailed content coverage to educate staff on BYOD security risks, the role of employees in enhancing safety of organization's data, BYOD security measures put in place by the organization, the organization's AUP and IAP, emerging issues as well as guidelines on devices to purchase.

The organization can also consider developing a mandatory training program that all BYOD users have to go through quarterly or half yearly. In addition, the BYOD training material should be made available in organizational portals such as the Intranet where employees can easily

access. Organizations should also ensure that they have adequate operational manuals before implementing BYOD in production.

Procurement

Having identified the required services, tools, hardware, software and other items, the organization should then perform the necessary procurement processes based on the procurement laws or policies.

Data Security

The organization should then implement its integrated data security plan in preparation for the run phase. The data security plan incorporates the elements of the plan phase as well as the software acquired with the aim of securing access to sensitive data in a BYOD environment.

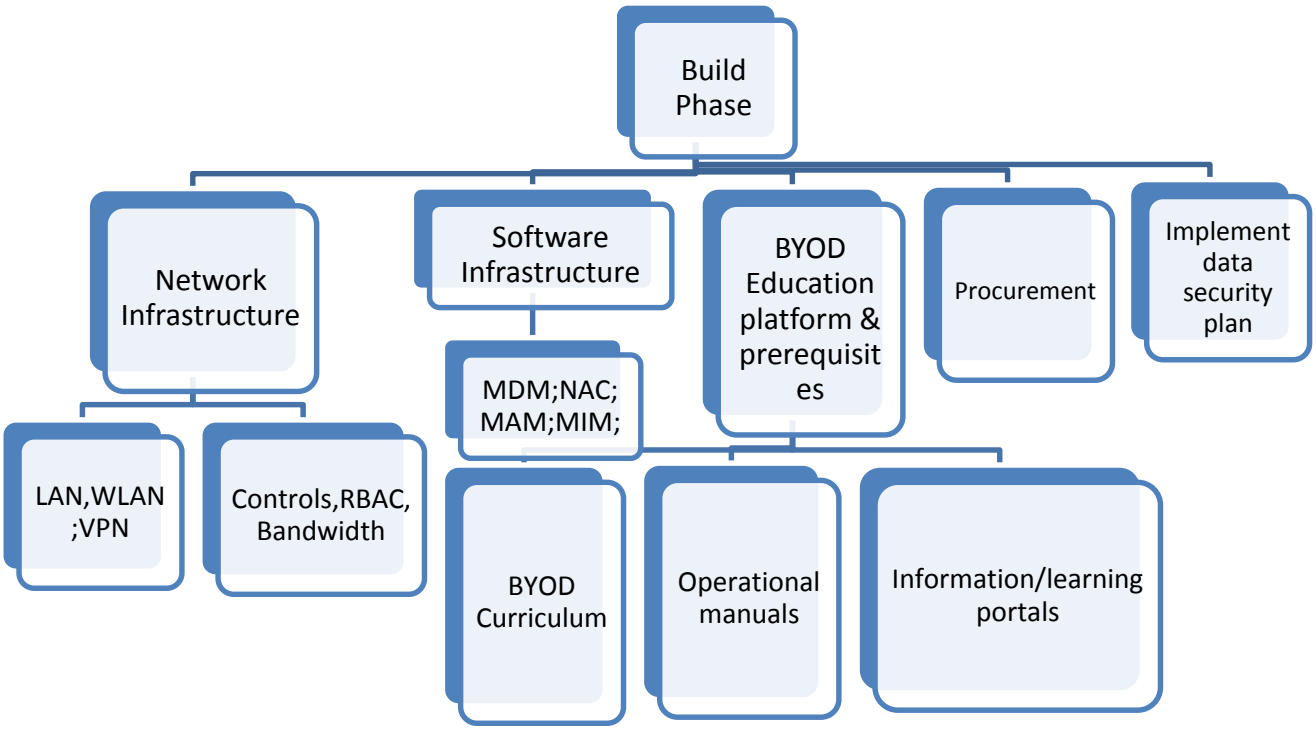


Figure 4.17: Build Phase of the developed BYOD security framework

4.5.2.3 Phase 3: Run Phase

Phase 3: Run Phase

In the run phase, the elements of the planning and the build phase are consolidated and executed in production. This is the stage where employees are now allowed to start accessing organizational resources using their own devices. Each element included in the planning and build phases will serve a specific purpose with a common goal of guaranteeing security of corporate data upon adopting BYOD. For instance, NAC will be responsible for device registration, authentication, and controlling access to the network. MDM will be responsible for monitoring and managing the devices that access the organization's servers, MAM will be

responsible for managing specific applications on the employee's device, while MIM will be responsible for safeguarding data integrity and administering encryptions. Compatibility of the devices is also tested in the run phase before being configured to access the organization's network.

Another important element of the run phase is separating data in a BYOD device into a personal category and corporate category (Wang, Wei, and Vangury, 2014). This allows the ICT administrator to enforce controls and security measures on the corporate category without causing too many restrictions on an employee's personal data. In the run phase, the administrator should also ensure that the organization's network infrastructure is running efficiently and is reliable.

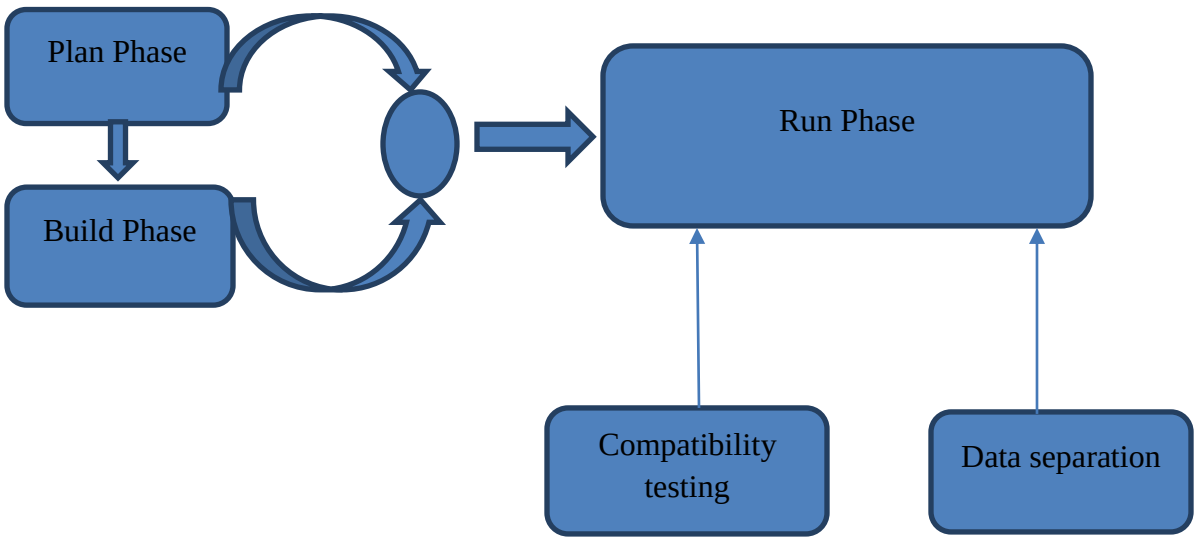


Figure 4.18: Run Phase: Consolidation and execution of the elements of Plan phase and Build phase.

4.5.2.4 Phase 4: Monitoring

The final phase is a continuous phase where each element in production is monitored and evaluated. It also involves ensuring that there is strict compliance to all BYOD-related policies

and procedures, reviewing policies when need arises, continuously improving controls, continuous BYOD education, and being up to date with latest BYOD security measures and tools.

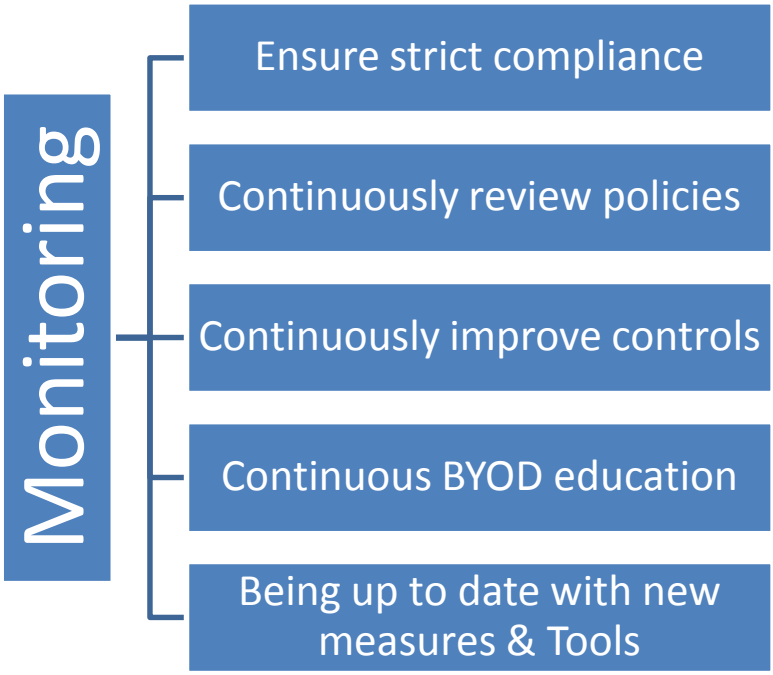


Figure 4.19: The Monitoring Phase of the developed BYOD security framework

The four phases of the developed BYOD security framework are summarized below:

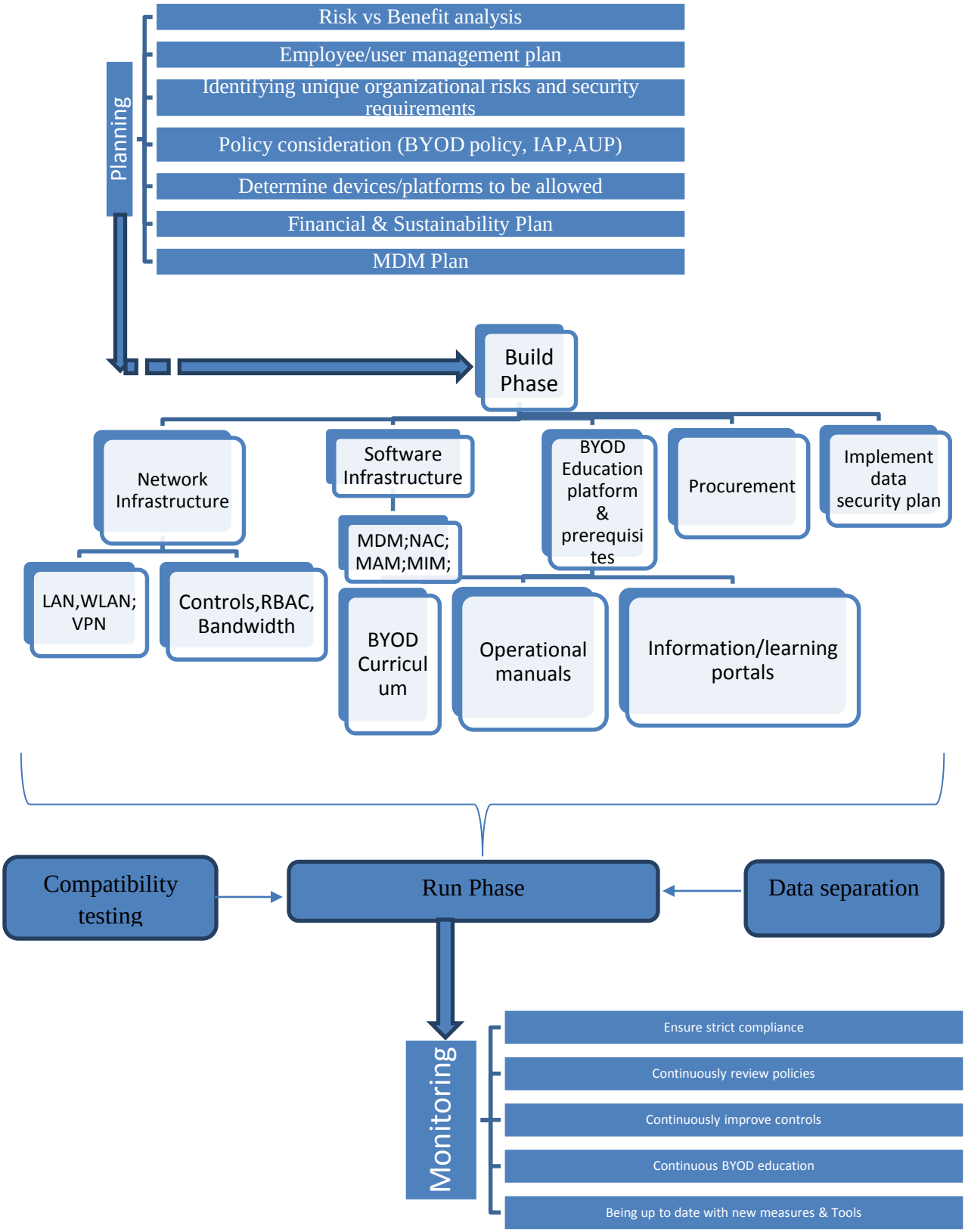


Figure 4.20: The developed BYOD security framework (2018)

4.6 Validation of the framework

Objective number 4

The fourth and last objective of the study was to validate the developed framework.

This section describes the process used to arrive at validation of the developed framework for enhancing security of corporate data in a BYOD Environment. The model was built from the analysis of the primary data and the information gathered from the literature. The primary data was useful in defining the key blocks of the framework.

The primary objective of the validation was to gather feedback from ict expert focus group on the framework for security of corporate data in a BYOD Environment, which is the ultimate aim of this study. The developed framework was designed using design science approach (Henver, 2007) . There are three types of validation methodologies for such kinds of artifacts developed using design science approach: plan, process and product validation (Verschuren & Hartog, 2005). The developed framework is best validated under Product validation since the prototype has been developed and therefore validation will be looking at the final product: the Sowek Framework.

The feedback provided the necessary feedback that helped in validating the framework. The validation was carried out through a workshop involving a focus group of experts in the information security sector.

4.6.2 Experts Focus Group Selection

The ICT focus group was selected from the department of ICT and Department of Computer Science and Mathematics. The total number of staff in these two departments is 21 and out of this number, a total of 7 were selected from the two departments. The selection was based on the

staff role (for administrative) and area of specialization (for Academic). The selection was deemed sufficient since the personnel in these two departments had the requisite expertise as it has the workforce aware of the research area and had experience in the field of Information security.

A cross-functional team consisting of Heads of Departments, Systems and Networks Administrators as Information security officers were involved in the workshop. For the workshop, structured questions approach was used so as to help in comparing and contrasting the responses of participants in the workshop.

Validation Process

The developed framework was presented to the workshop participants after a brief introduction to the topic of BYOD and explanation of the relevant problem. The components of the framework were then explained to the participants.

Results of the validation workshop are summarized below.

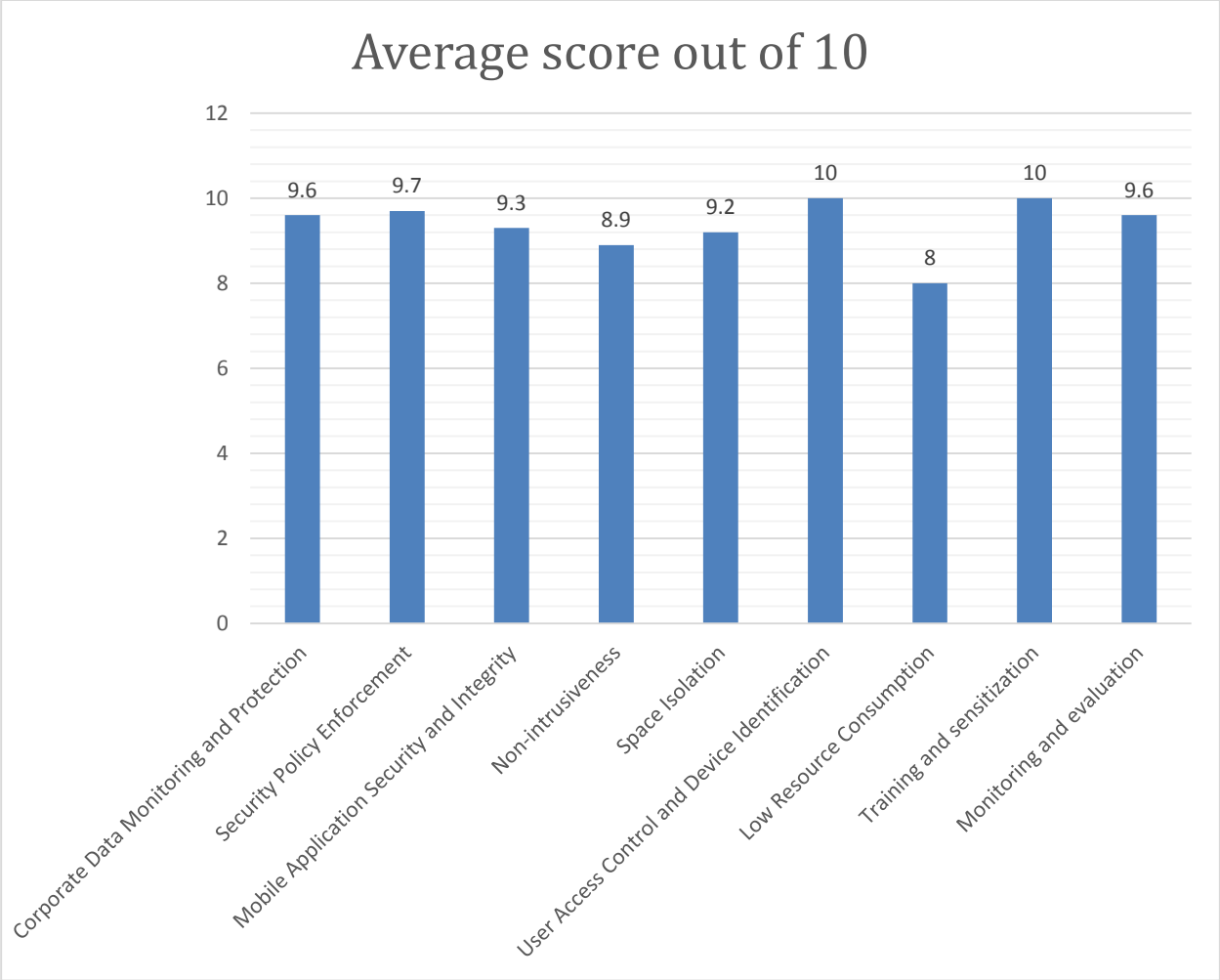


Figure 4.21: Average score out of 10 of the developed framework for each feature.

From the results in the figure above, it can be deduced that the developed framework as validated meets the desired objectives to a large extent. The average score given by the ICT expert panel was above 9 in all the functional areas except non-intrusiveness and low resource consumption whose average scores were 8.9 and 8 respectively.

4.7 Summary of the findings

The main objective of the study was to establish a framework for enhancing security of corporate data in a Bring Your Own Device (BYOD) Environment. In order to achieve this objective, the study reviewed the existing security frameworks in government institutions and the related

security challenges in order to develop a multi-layered BYOD security framework that unites the existing frameworks in the literature and also takes into account the practitioners' views, experiences, awareness as well as the business needs.

The study found that government organizations in Kenya are increasingly allowing their employees to bring their own devices to the workplace and use them to access organizational data or resources. Increased productivity and efficiency, flexibility of working hours and reduced cost of purchasing devices for employees were identified as the key motivations behind this new trend. Reduced infrastructure costs, employee motivation, demand from young employees, desire for mobility, and management decision were also identified as reasons for adopting BYOD. The main organizational resources accessed through BYOD include IT support information, email information, Bio data, customer information, procurement information, financial information and company files. Sensitive government data is also accessed through BYOD although to a smaller extent and by middle-level management and top management.

On security challenges or incidents that government organizations have faced since adopting BYOD, the study found that theft of mobile devices, infection by virus or malware, attack of corporate systems through the mobile devices, distributed denial of service (DDoS), accidental loss of mobile devices, illegal access of corporate systems through stolen passwords, and infection by spy-ware had been experienced. These security risks or challenges were hindering the secure adoption of BYOD to a large extent. Some organizations that had already implemented BYOD had chosen to stop the adoption completely as a result of these security incidences. Others that were mulling the BYOD concept had later chosen to shelve the idea as a result of the security risks that accompany BYOD adoption.

The study also sought to establish the security measures that government organizations had put in place in the BYOD environment. The study found that the existing measures include user agreements, firewalls, user training, anti-virus/ anti-malware software, regular software updates, Virtual Private Networks (VPN), and intrusion detection systems.

CHAPTER 5

5.0 CONCLUSIONS, CONTRIBUTIONS AND RECOMMENDATIONS

5.1 Introduction

In this chapter, the study presents the summary of the findings followed by conclusions based on the findings. It also presents policy recommendations by summarizing the developed BYOD security framework and also presents suggestions for further research on this topic. Lastly, the study will discuss the limitations of the study.

5.2 Conclusion

Based on the findings of this study, it is evident that BYOD is a concept whose time has come. The numerous potential benefits of adopting BYOD are increasingly attracting corporate organizations to this emerging concept. The Government of Kenya for instance, is increasingly moving away from the traditional approach of purchasing devices for employees and instead allowing employees to buy their own devices and use them in the workplace, in order to benefit from reduced costs, increased efficiency and flexibility, and increased employee motivation.

However, this new concept is a double-edge sword. BYOD adoption indeed introduces new security risks that organizations must be prepared to deal with. It was evident that organizations were still implementing the traditional security measures only, despite the new security risks introduced by BYOD. The numerous security incidents and challenges experienced by organizations that had adopted BYOD implied that a security framework that addresses BYOD security risks was extremely necessary. A review of the existing frameworks in the literature pointed out various limitations and loopholes. It was therefore necessary to develop a security framework that unites the existing frameworks in the literature and also takes into account the practitioners' views, experiences, awareness and business needs.

The BYOD security framework developed by this study considered the existing frameworks and the security challenges facing BYOD adoption. The framework followed the pillars of the Control Objectives for Information and Related Technologies (COBIT) 5 process reference model developed by ISACA, 2012, which include Planning, Building, Running, and Monitoring. The components of the planning phase include risk versus benefit analysis, user management plan, identifying unique organizational risks and security requirements, policies, determining devices/platforms to be allowed to access organizational resources, financial and sustainability plan, and a Mobile Device Management (MDM) plan. The Build phase involves putting in place the necessary software and network infrastructure in order to facilitate the translation of the elements of the planning phase into actual implementation, putting in place the necessary platforms and prerequisites for BYOD education, procuring the required tools/services, and implementing a data security plan. In the run phase, the elements of the planning and the build phase are consolidated and executed in production. Testing the compatibility of devices and separation of personal and organizational data are also carried out in this phase. The final phase involves monitoring and evaluation of every element of the framework. It is a continuous process which ensures strict compliance, continuous review of policies and controls, continuous BYOD training as well as being up to date with new measures and tools.

5.3 Contribution to the body of knowledge

The study contributed to the body of knowledge on this topic by providing empirical evidence on challenges facing BYOD adoption in the public sector and the existing security frameworks that have been put in place to address these challenges. Understanding the state-of-the-art provided a basis upon which this study recommended a holistic framework that would effectively guide the implementation of BYOD in the public sector.

5.4 Recommendations

5.4.1 Recommendations for corporate organizations

The study recommends that corporate organizations that have adopted or are considering adoption of BYOD should adopt and implement the developed security framework because it is multi-layered and unites the existing frameworks and solutions. In addition, the framework takes the existing security challenges and risks into consideration. While adopting this framework, the study further recommends that organizations should tailor the components of the four phases of the framework to their specific organizational and business needs in order to increase the effectiveness of the framework.

5.4.2 Recommendations for further research

BYOD security requires continuous research and development. This study recommends that further research should be carried out to refine or expand the developed framework further by considering organizations in other sectors such as banking, higher education, telecommunication, hospitality and healthcare.

5.5 Challenges and Limitations of the study

Access to information in government organizations was a major challenge in this study. The level of bureaucracy in government organizations made it difficult to get the required information from ICT experts/practitioners in these organizations.

The limitation of the study is that it only considered government organizations. Future research should include other sectors as well.

REFERENCES

Baruch, Y. (1999). Response Rate in Academic Studies-A Comparative Analysis. Human Relations, 52(4), 421-438. doi: 10.1177/001872679905200401

Brodin (2015). Combining ISMS with strategic management: The case of BYOD Combining ISMS With Strategic Management: The Case of BYOD

Cisco IBSG Horizon. (2012). BYOD: A Global Perspective. San Jose, CA: Cisco Systems Inc. Retrieved from http://www.cisco.com/web/about/ac79/docs/re/BYOD_Horizons-Global.pdf

Citrix systems (2013). Best practices to make BYOD simple and secure: A guide to selecting technologies and developing policies for BYOD programs. A Citrix Whitepaper, 0312/BYOD Guide, 1,4,8

Communications Authority of Kenya. (2016). *Annual Report 2016/2017* (pp. 16-20). Nairobi: Communications Authority of Kenya.

Dahlstrom, E., &Difilipo, S. (2013). *The Consumerization of Technology and the Bringing your Own Everything (BYOD) Era of Higher Education.*

De Vos, A.S., Strydom, H., Fouche, C.B., &Delport, C.S.L. (2005). *Research at Grass roots: For the social sciences and human service professions.* Pretoria: Van Schaik Publishers.

Dell Inc (2015) Dell Offers Top Five Best practices for Overcoming BYOD and Mobile Security Challenges. *ENP Newswire Publishing*, UK, 1-3.

Dongwan, K., Changmin, J., Taeeum, K., Hwankuk, K. (2015) A Study on Security framework for BYOD environment (Pp. 89-92) USA. Institute of Research Engineers and Doctors.

Downer, K., & Bhattacharya, M. (2018). BYOD Security: A New Business Challenge.

Downer, K., & Bhattacharya, M. (2018). BYOD Security: A New Business Challenge.

Elbanna, S. (2010). Strategic planning in the United Arab Emirates. *International Journal of Commerce And Management, 20*(1), 26-40. doi: 10.1108/10569211011025934

Ernest and Young (2013). Bring Your Own Device, Security and risk considerations for your mobile device program, Insights on governance, risk amd compliance.

Espiner, T, (2015). One in five hacked logins match Microsoft accounts. ZDNet. [Online]. Available: http://www.zdnet.com/article/one-in-five-hacked-loginsmatch-microsoft-accounts/

Forrester Consulting (2012). Key Strategies To Capture And Measure The Value OfConsumerization Of IT.

Gheorghe, G. &Neuhaus, S. (2013). Poster: preserving privacy and accountability for personal devices. Presented at the Proceedings of the 2013 ACM SIGSAC conference on Computer & Communications Security (CCS' 13), Berlin, Germany.

Gheorghe, G., &Neuhaus, S. (2013). Poster: Preserving privacy and accountability for personal devices (pp. 1359-1362). Berlin, Germany: Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. Retrieved from http://doi>10.1145/2508859.2512500

Ghosh, A., Gajar, P., & Rai, S. (2013). Bring Your Own Device (BYOD): Security Risks and Mitigating Strategies. *Journal of Global Research in Computer Science*, *4*(4). Retrieved from http://www.jgrcs.info

Hernandez, A., & Choi, Y. (2014). Securing BYOD Networks: Inherent Vulnerabilities and Emerging Feasible Technologies. *IT Professional*, 16(5), 9-11. doi: 10.1109/mitp.2014.76.

Henver, A. R. (2007). Three cycle view of deisgn science research. Scandanavian Journal of Information systems.

Hormazd, R. (2014). Best practices for BYOD security. *Computer Fraud & Security*, *2014*(1), 13-15. doi: 10.1016/s1361-3723(14)70007-7

ISACA. (2012). A Business Framework for the Governance and Management of Enterprise

IT. Retrieved July 26, 2014, from COBIT 5: www.isaca.org/cobit

Knight, K. (2010). Study/Experimental/Research Design: Much More Than Statistics. *Journal of Athletic Training*, *45*(1), 98-100. doi: 10.4085/1062-6050-45.1.98

Koh, E., Oh, J., &Im, C. (2014). A study of the Security threats and dynamic access control technology for BYOD, smart environment. Hong Kong: International Multi-Conference of Engineers and Computer Scientists.

Leavitt, N. (2013). Today's Mobile Security Requires a New Approach. *Computer*, *46*(11), 16-19. doi: 10.1109/mc.2013.400

Lee, N & Lings, Ian (2008) Doing Business Research: A Guide to Theory and Practice. SAGE Publications.

Li, F., Peng, W., Zou, X., & Huang, C. (2013). Smartphone strategic sampling in defending enterprise network security. Budapest, Hungary: IEEE International Conference on Communications.

Lookout. (2015). *Feds: You have a BYOD program whether you like it or not* (pp. 3-5). Washington, CA: Market Cube.

Mahesh, S., & Hooter, A. (2013). Managing and securing business networks in the smartphone era. *Annual General Business Conference*, 1-17. Retrieved from http://scholarworks.uno.edu/mgmt_facpubs/5

Mathiyazhagan, T., &Nandan, D. (2010). Survey research method. Media Mimansa (pp–34-45)

Matinde, V. (2015). Africa: The rise of BYOD & corporate data threats. *IDG Connect*. Retrieved from https://www.idgconnect.com/abstract/9313/africa-the-rise-byod-corporate-threats

Millard, A. (2013). Ensuring mobility is not at the expense of security. *Computer Fraud & Security*, *2013*(9), 11-13. doi: 10.1016/s1361-3723(13)70080-0

Mooi, E. A., &Sarstedt, M. (2011). *A concise guide to market research: the process, data, and methods using IBM SPSS Statistics*. Heilderberg (DE): Springer.

Morrow, B. (2012). BYOD security challenges: control and protect your most sensitive data. *Network Security*, *2012*(12), 5-8. doi: 10.1016/s1353-4858(12)70111-3

Mugenda, O., &Mugenda, A. (2003). *Research methods: Quantitative and qualitative Approaches*. Nairobi: African Centre for Technology Studies.

Mwenja, J.M. (2013) Framework for Securing Wireless Local Area Network

Ndeng'ere, D.K (2017). A BYOD framework for secure use of mobile devices in universities: The case of Universities in Kenya

NIST, "Guidelines for Managing the Security of Mobile Devices in the Enterprise", 2011. NIST SP-800-124 Rev1

Olalere, M., Abdullah, M., Mahmod, R., & Abdullah, A. (2015). A Review of Bring Your Own Device on Security Issues. *SAGE Open*, *5*(2), 4. doi: 10.1177/2158244015580372

Oluranti, J., Sanjay, M. (2016). Policy framework for adoption of bring your own device (BYOD) by institutions in Nigeria.

Pell, L. (2013) BYOD Implementing the Right Policy. *University of Derby*, UK, 95-98.

Rhee, K., Jeon, W., & Won, D. (2018). Security requirements of a Mobile Device Management System. *International Journal of Security and Its Applications*, *6*(2).

Selviandro N., Wisudiawan G., Puspitasari S., and Adrian M. (2015). Preliminary study for determining bring your own device implementation framework based on organizational culture analysis enhanced by cloud management control (pp. 113-118): In 2015 3rd International Conference on Information and Communication Technology (ICoICT).

Serianu Ltd. (2015). *Kenya Cyber Security Report* (pp. 19-25). Nairobi: Serianu Limited

Serianu Ltd. (2016). *Kenya Cyber Security Report* (pp. 21-25). Nairobi: Serianu Limited.

Thielens, J. (2013). Why APIs are central to a BYOD security strategy. *Network Security*, *2013*(8), 5-6. doi: 10.1016/s1353-4858(13)70091-6

Thomson, G. (2012). BYOD: enabling the chaos. Network Security, 2012(2), 5-8. doi: 10.1016/s1353-4858(12)70013-2

Titze, D., Stephanow, P., &Schutte, J. (2013). A configurable and extensible security service architecture for smartphones. Barcelona, Spain: 27th International Conference on Advance Information Networking and Applications Workshops.

Verschuren, & Hartog. (2005). Evaluation in design oriented research. Quality and Quantitiy.

Wang, Y., Wei, J. and Vangury, K., (2014) Bring your own device security issues and challenges, IEEE 11th Consum. Commun. Netw. Conf., pp. 80–85, 2014.

WatchGuard. (2013). *Ten Tips for Establishing a Secure Foundation for BYOD* (pp. 2-7). Washington DC: WatchGuard Technologies Whitepaper.

Werthmann, T., Hund, R., Davi, L., &Holz, T. (2013). PSiOS: Bring your own privacy & security to iOS devices. Berlin, Germany: In Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security.

Zahadat, N., Blessner, P., Blackburn, T., & Olson, B. (2015). BYOD security engineering: A framework and its analysis. *Computers & Security*, *55*, 81-99. doi: 10.1016/j.cose.2015.06.011