BRING YOUR OWN DEVICE AND CORPORATE INFORMATION TECHNOLOGY SECURITY: CASE OF FIRMS LISTED ON THE NAIROBI SECURITIES EXCHANGE LIMITED

MICHAEL ETALE MBALANYA

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF THE DEGREE OF MASTER OF BUSINESS ADMINISTRATION, SCHOOL OF BUSINESS, UNIVERSITY OF NAIROBI

NOVEMBER 2013

DECLARATION

This research project is my original work and has not been submitted for a degree in any other university.

Signature: _____ Date: _____

MICHAEL ETALE MBALANYA

D61/66755/2010

This project has been submitted to the University for Examination with my approval as the University Supervisor

Signature _____ Date: _____

Supervisor

Mr. J.K. LELEI

Department of Management Science

University of Nairobi

DEDICATION

To the tireless pursuit of knowledge

ACKNOWLEDGEMENT

To my Mum, my grandparents, Cucu and Guka, my Aunty Polo, my brothers Ben and Adrian and friends who believed in my abilities and provided constant encouragement in my pursuit of this MBA degree.A special acknowledgement to Mary Nelima, who encouraged, challenged and supported my educational pursuits.

And lastly, a special thanks to my supervisor Mr. J.K. Lelei who reviewed multiple times, thoroughly critiqued and brutally commented on the report and progress. Without your consideration, input and encouragement, this study would not have been completed.

Thank you.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

BYOD	Bring Your Own Device
IT	Information Technology
NSE	Nairobi Securities Exchange Limited

ABSTRACT

Recent years have seen an explosion in consumer mobile computing devices and this has been accompanied by falling prices that make these mobile devices within easy reach of the common man. As a result, organizations that traditionally allowed access to corporate systems through fixed company owned computers are seeing increased numbers of employees purchasing their own mobile devices and demanding to have them enabled to access corporate resources. This is what Bring your own device (BYOD) is. The adoption of BYOD has raised concerns which organizations have to address. This study sought to find out the extent to which BYOD has been adopted in organizations, the accompanying benefits, the threats associated with BYOD, and the counter-measures that organizations have put in place.The study focused on all 61 organizations as listed on the Nairobi Securities Exchange Limited (NSE). A structured questionnaire was used to collect data from respondents within the selected organizations in charge of Information Technology. These respondents included IT managers, IT security managers and IT officers. The data collected was analyzed using frequency, percentages, means, standard deviation and factor analysis.The results were presented using tables and charts. The study revealed that over ninety percent of organizations in the NSE have allowed BYOD in one form or the other. It was also revealed that over half of all the companies studied allowed over 50% of the staff to use their own personal devices for work-related tasks. It was also found that most of the organizations were not ready for BYOD. Most did not have BYOD specific counter-measures in place and instead relied on old security infrastructures that may not be suitable for mobile devices. The top benefit that organizations experienced from adopting BYOD was that of having their employees work flexible hours. The study recommended that organization should address BYOD threats by developing proper policy and procedures, investing in training employees and adopting mobile device management solutions.

CHAPTER ONE: INTRODUCTION

1.1 Background of the Study

The increased sophistication of phones and computing devices coupled with their falling prices has made mobile devices highly accessible and affordable to the common man. Unlike in the past, it is now very easy to obtain a smart-phone, tablet, laptop or net-book at an affordable price. As the prices of components used to build computing devices dropped so have the prices of the consumer devices dropped as well. Sales of laptops and smart-phones on the other hand have shot up rapidly within a very short period. In fact, according to a research done by NPD Group (2003), in May of 2003, 54% of all computers sold in stores were laptops. This was the first time ever that laptop computer sales exceeded desktop computers sales. This trend continues to grow with smart-phones and tablets being introduced into the market and taking off significantly in terms of sales over the years. This has led to a new phenomenon known as "Bring you own Device" (BYOD), where company employees and executives prefer to purchase and use their own smart-phones, laptops or tablets for corporate work with some companies even purchasing these devices on behalf of employees and allowing them to use them for both work related and personal tasks.

Information Technology involves the use of computer applications and equipment to develop, design, manipulate and implement the storing and the transmission of data. Information Technology has revolutionized how companies do business and has brought with it so many advantages that today virtually every corporate firm relies on Information Technology in one way or another. Some of these advantages include globalization. Firms can now communicate across borders easily and efficiently. Communication has

been made cheaper, easier, quicker and more efficient. Business processes have been streamlined and computerized thus making firms extremely cost effective. This in turn has increased productivity which ultimately gives rise to profits (Pieterson 2009). Information systems need people to provide data for processing. Traditionally, to use the corporate information system the employees had to connect via computer terminals. However BYOD has provided a more flexible and efficient interface to the corporate information technology systems (Drury & Absalom 2012).

Employees, including senior level management want the convenience of using just one smart-phone or one tablet for both work and personal use. They have found that owning two separate devices, one for work and another for personal use is cumbersome and inefficient. Consequently employees are bringing in their personal devices and demanding that IT departments allow them access to corporate resources through these devices. A survey done by Citrix (2013) found that 92% of companies have some employees who are already using non-company issued computing devices for work related tasks. In these companies, it was found that 28% of the employees are already using non-company issued computing devices for work-related tasks and this percentage is expected to increase to 35% by mid-2013. Only 44 percent of the companies surveyed had a BYOD policy in place.

When it comes to the employee device of choice, 38 percent of employees brought in personal laptops, 28 percent of employees brought smart-phones to the organization, 7 percent of the employees brought to work tablets, and 6 percent brought in net-books to use for work-related tasks (Citrix 2013). In the companies surveyed, it was found that the uptake of BYOD is not equal amongst the different levels of staff across the organization.

Of the workers that used personal devices for work-related tasks, 62 percent are mobile workers, 48 percent are professional office workers, 43 percent are remote or home based workers, 37 percent are senior executives, 32 percent are third parties and temporary staff, 23 percent are customer service or call center staff, and 9 percent is the rest of the organization (Citrix, 2013).

Many have argued that allowing BYOD in the corporate environment makes sense from a business and IT perspective because it increases employee productivity, improves employee morale, and reduces the cost of IT capital expenditure as well as on-going support costs. However, prematurely allowing BYOD into a corporate environment does introduce security risks that must be addressed otherwise the very assets that a company needs to protect can have their security compromised (Oliver 2012). Some of the security risks associated with BYOD include malicious software infection, loss of confidential corporate information, intrusion, lack of insight into the network, and theft of mobile devices. With companies facing these risks, the statistics show that organizations are still not ready to deal with the issue of BYOD security risks. Security professionals have recommended a number of security measures to minimize BYOD risks. Some of these measures include having a BYOD security policy in place, implementing a mobile device management system and user training. However, only 44 percent of companies have implemented a BYOD security policy, less than 10 percent of organizations are fully aware of the devices that are accessing their network and 80 percent of BYOD activity is going unmanaged (Eschelbeck & Schwartzberg, 2012). Here in Kenya the situation is no different than in the developed countries. Smart-phones and tablets are the fastest selling consumer electronics. The Kenyan middle-class across all business sectors has acquired

these devices in large numbers with most employees having at least two devices i.e. a smart-phone and a tablet. In every meeting or every seminar in Nairobi one cannot miss to see at least more than half of all participants carrying a smart-phone and/ or tablet with them. This research studied a cross section of the Kenyan corporate scene by analyzing the BYOD environment of companies listed in the NSE.

The Nairobi Securities Exchange Limited (NSE) was constituted in 1954 as a voluntary association of stockbrokers. Its major objective was to provide a formal market for buyers and sellers to deal in shares and stocks. The NSE has a total of 61 listed companies from various economic sectors which are: Agricultural, automobiles and accessories, banking, commercial and services, construction and allied, energy and petroleum, insurance, investment, manufacturing and allied, telecommunication and technology and growth enterprise market segment (Nairobi Securities Exchange Limited, 2013). The diverse nature of the firms listed in the NSE provided a more complete picture of the technological situation of the Kenyan corporate workplace as it related to this study on BYOD.

1.2 Statement of the Problem

BYOD is a phenomenon that is rapidly spreading across firms in Kenya and the world at large. The major reason for this trend is that personal computing devices are now very affordable for employees to purchase on their own. Firms have also come to realize the importance of BYOD in increasing employee productivity, increasing work flexibility, reducing the cost of IT expenditure and in retaining the best talent. Whereas most of the studies on BYOD has been geared towards corporates in the developed world, the Kenyan corporate scene is among those that have seen a rapid increase in the

consumerization of IT and the resulting BYOD phenomenon. All around the office space employees can be seen bringing to work all sorts of mobile computing devices including Android smart-phones, tablets, laptops, ultra books, net-books etc. This has left IT departments with challenges of how to go about managing, let alone securing these devices and the corporate assets that these devices have access to.

BYOD brings several security concerns and risks with it. A study by Citrix (2013), shows that 55% of companies are concerned about potential security issues of BYOD. These issues range from theft of mobile devices, leakage of confidential corporate information, system intrusion, malware infection and lack of insight into as to what is accessing the corporate network (WatchGuard 2013). When it comes to countermeasures that have been implemented to address BYOD security concerns, a study by the Sans Institute (2012), revealed that only 41% of companies had a policy supporting BYOD in place however 61% of the companies allowed BYOD use for work-related tasks. These findings show that less than 41% of companies actually have security measures in place to counter BYOD threats.

With all the risks that BYOD brings along with it, it is clear that in order for corporates to protect their assets and remain secure, a change of strategy is required. A number of articles and journals have been written on how best to secure corporations against the backdrop of BYOD however to the best of the knowledge of the researcher, no research has been done in Kenya to find out how much of a threat BYOD is, what strategies and countermeasures have been put in place, what technologies have been adopted to secure BYOD, and what incidents corporations have experienced that were caused by BYOD. Additionally even though all studies have indicated that BYOD does come with potential

risks, no study seems to have been done to find out how big a risk BYOD is and what incidents have organizations faced relating to its adoption. Therefore, there is a gap between the stated security risks and what the actual security risk of BYOD is in companies. This study sought to answer these questions and establish whether BYOD is a real security threat.

1.3 Research Objectives

The objectives of the study were to:

a) Determine the extent to which BYOD is used in firms listed in the NSE.
b) Determine the benefits that BYOD has brought to firms listed in the NSE.
c) Determine the extent to which BYOD causes threats to corporate IT systems of the organizations listed in the NSE.
d) Determine measures that are in place to counter the threats brought about by BYOD that have been adopted by firms listed in the NSE.

1.4 Value of the Study

This study was the first of its kind to analyze they BYOD phenomenon in Kenya. The study identified the threats BYOD brings with it especially in the Kenyan context. Security professionals have claimed that in theory BYOD brings with it many security issues and opens up corporate systems to attacks. However there have been no studies conducted that can offer statistics to confirm whether the threats are real or whether they are just perceived threats that have been publicized by security professionals. By studying the companies listed on the Nairobi Securities Exchange Limited, this study provided a true picture of the extent of BYOD and how the corporates are managing these devices in the Kenyan corporate scene. Most importantly through this study, recommendation of the

best IT security strategies, specially adapted to the Kenyan environment could be made. This will assist corporate management to best manage the BYOD phenomenon and minimize any risks that BYOD brings with it. The study provides business owners and IT managers with valuable insight into the BYOD situation, determining whether the threats are real, and recommending effective countermeasures. The research contributes valuable information and statistics to IT security professionals and researchers by providing information on security incidents that have affected organizations. This information will help security professionals analyze the most common threats against mobile devices and subsequently help them better secure these systems. This helps answer the question on whether BYOD is indeed a real security threat. Lastly, the study reinforces the Unified Theory of Acceptance and Use of Technology.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

The focus of this chapter is on the review of literature related to this study. The literature presented in this chapter focuses on the BYOD concept, the use of BYOD, security threats emerging from BYOD, and IT security measures to counter threats from BYOD.

2.2 BYOD and the Extent of Use in Organizations

According to Apperion (2011), the consumerization of IT has come about because the popularity of smart-phones and tablets is growing exponentially as more and more people realize the benefits of having instant access to email, social media and the general internet wherever they may be. Due to the ease of access and the fun factor provided by these devices, consumers now want to bring these devices to the workplace and have them configured to access the business applications. This has forced many corporates to consider and accept a BYOD environment. Businesses should therefore create a BYOD environment that addresses the demands of end users and properly secures the environment.

BYOD has been used in several organizations across all industries however it is most prevalent in service oriented organizations such as Banks, advertising firms and public relations firms (Oliver 2012). Technology based companies such as Telecoms and Internet Service providers have also seen increasing tendencies of employees choosing to bring their own devices to the workplace. Indeed some telecommunication companies actually purchase these devices for their staff (Gessner et al 2013). Functions within organizations that have seen the biggest rise in the use of BYOD include marketing,

advertising, sales, customer management departments and executive management (Citrix 2013).

Singh (2012) describes BYOD as a business policy that is adopted by management and allows employees to use their own personally owned devices such as Ipads, smart-phones and laptops to access company resources such as email, databases, and documents. In support of this, Singh (2012) quotes Bernnat, Acker, Bieber & Johnson who wrote that "Work is no longer a place you go to, and then leave, but an ongoing activity." Thus the devices used at home would be expected to be used in the corporate environment. The reason companies have chosen to implement this BYOD approach is because of the demand from tech savvy employees who are well leveraged in the technologies of smart phones, tablets, and the internet. Employees demand flexibility and availability of systems so as to be able to work anytime and from anywhere. Consequently, according to Good Technology (2012), "it is a given that employees will either bring their own smart-phones and tablets into the workplace or will want to work on these devices when away from the office." The mass adoption of smart-phones, tablets and mobile computing devices has set expectations resulting in every employee wanting to have their own personal devices, and to bring them into the workplace.

Miller, Voas, and Hurlburt (2012), noted that BYOD is already very common in businesses. They noted according to a Cisco survey carried out in the US, that 95 percent of the respondents said that "their organizations permit employee-owned devices in some way, shape or form in the workplace. The same survey revealed that the average "knowledge worker" uses 2.8 connected devices at work and that the number of devices

used is expected to increase in coming years. Many respondents saw this as a positive for the business but there were security concerns.

The benefits of a BYOD enabled environment as stated by Apperion (2011) are several. Among these is that the total cost of ownership incurred by the business will reduce. Having employees bring their own computing devices reduces device capital expenditure since fewer devices need to be purchased. Ongoing costs for mobile phone usage and data access are also reduced as employees opt to pay for themselves. Technical support from a corporate's IT department shall also be reduced because the employees know how their smart-phones and tablets work and thus require little help from the IT department.

The other benefit is that of improved employee morale. By giving employees the freedom to bring their own devices, they gain more control over their computing environment thus making them happy. They can also work from home and have the option of working flexible hours instead of the traditional nine to five hours. This approach helps a company to recruit and retain the best and brightest professionals in the industry (Miller-Merrel, 2012).

The final benefit is improved productivity. The ability for employees to easily switch from personal applications such as music, photos, social media and email, to corporate applications and systems, allows employees to work away from home on weekends and late into the night. Employees also become more productive and efficient because corporate data and information is readily available to them on their mobile devices. Efficiency is further advanced because the employees are more familiar and comfortable using the functionality of the devices they own (Gajar, Ghosh and Rai, 2013).

UBM Techweb (2012), also states that a BYOD environment brings with it many benefits. The focus of their white-paper was on the Healthcare sector where they state that healthcare professionals such as doctors and nurses frequently need to be on the go, moving to and fro from patient hospital rooms, exam rooms, labs and offices, and because of this high level of movements, mobile devices are very ideal for them. Mobility is one of the most transformational technologies in the healthcare industries and this is facilitated by the BYOD phenomenon which allows the healthcare professionals to be highly productive and efficient while on the go.

2.3 Security Threats Emerging From BYOD

According to Watchguard (2013), BYOD does present its own risks that must be addressed if security is to remain intact in the corporate environment. The first and foremost is the risk of data loss from mobile devices. Data loss can happen in many ways and the damage can range from zero to extreme. By virtue of being mobile, the devices can easily be stolen and the data saved on them can be easily accessed if not encrypted. This information may expose customer data and privacy data that may damage the reputation and trust of the company. Intellectual secrets and trade secrets may also be exposed thus compromising the competitive edge of a company. Additional costs to a company include the cost of lost business, legal fees, consultation fees, and remediation expenses.

Another risk of BYOD is that of malware infecting corporate systems via the mobile devices. Many if not all off the shelf mobile devices lack some form of anti-malware installed. Such malicious software (malware) may include viruses, Trojan horses and key loggers which can capture user passwords, steal information, crash computers or delete

important and sensitive information. Malware can cause widespread damage to an organization by interrupting business processes, stealing corporate information or providing an entry point for hackers (Watchguard 2013).

A third risk associated with BYOD according to Watchguard (2013), is the risk of an intrusion attack. There have so far been no documented intrusion attacks that have been perpetrated through mobile devices however security professionals expect that it is only a matter of time before hackers will be able to compromise a mobile device and use it as a launching pad into the corporate environment.

Apart from intrusion and malware attacks, another challenge to IT departments is that of lacking sufficient insight as to what is going on in the corporate networks they manage. By virtue of not being prepared to manage the devices that access the network and the information stored and transmitted, IT departments have no visibility into the operations of these devices. They lack log files and reports concerning the devices. This makes them more or less powerless when it comes to managing and securing these devices because one cannot protect what they do not know (Watchguard 2013). According to UBM Techweb (2012), there are a number of challenges and issues that must be addressed when it comes to the management of a BYOD environment. Securing the devices themselves and the corporate environment that these devices connect to is one of the biggest challenges any organization will face.

Miller et al (2012) notes that the security concerns for BYOD are largely a replay of the concerns that came about when laptops became common. But with tablets the risk is higher than laptops because tablets and smart-phones are much smaller than laptops. A

laptop is harder to lose and when lost is more easily noticed compared to the tablets and smart-phones. Another concern is that the BYOD devices are not owned by the company therefore the company is unlikely to implement its security policies on these devices. As soon as data is stored and transmitted using a device that the company does not own or have control over, the data stored therein is likewise beyond the control of the company even though it belongs to the company. Another issue is privacy concerns. Mobile devices contain a wealth of information that is private and personal to the user. This data gets mixed up with the corporate data stored on the device especially where there are no clear partitions between the two sets of data (Miller et al., 2012).

According to Perakovic et al (2012), modern mobile devices represent a good target for potential attackers because of the very nature of the operating systems that run on them. Attackers are motivated to attack such devices due to financial, personal or political reasons and the prevalence of such attacks is only likely to increase due to the popularity of these mobile devices. Additionally, user awareness of vulnerabilities and exposures that may lie within these devices is very low. Most users assume that their devices are safe and very few take the extra step of installing security software. Various threats can be identified that have an impact on BYOD and the systems surrounding it. The impact of such threats can be determined by the assets or property that is affected by the threat. Examples of such assets include: personal data, corporate intellectual property, classified information, financial assets, service availability, and reputation. The threats themselves can be classified as physical threats, application-based threats, network based threats, social engineering and web-based threats (Perakovic et al., 2012).

The biggest threat facing mobile devices is that of device loss or theft. The fact that mobile devices are so small and people carry them with them all the time means that the chance of losing them is very high. The impact of a lost device includes financial loss, data breach, loss of intellectual property and trade secrets, and loss of personal information (Perakovic et al., 2012). The second threat is that of attack on devices that are to be disposed. Companies may have sanitization procedures for computers, laptops and hard disks in place, however, these procedures may not currently extend to mobile devices. More and more mobile devices are recycled and disposed because these devices usually have a lifespan of about two years. As these devices are disposed they are disposed with the data on them completely intact and which can then fall into the wrong hands (Osteraman Research Inc., 2012).

The third threat is that of malware attacks. Malware, short for malicious software, is software that is designed to harm a computer, take control over it, spy on user activities or steal information from a it. The majority of malware targeting mobile devices aims to steal personal data or make money fraudulently through the SMS service (Lyne 2012). Inadvertent disclosure of information is yet another attack that can affect mobile devices. Most users are not aware of the functionality and capabilities of the apps they install. Mobile applications usually request certain permissions during installation. Such permissions include requesting access to phone book contents, wireless transmissions, SMS, and much more. Users rarely review the permissions an app is requesting and simply want to have the application running on their devices as quickly as possible. Some applications collect and publish personal data and location information which is often used on social networks. The apps may have privacy settings that allow setting

restrictions on the type of information collected but many users are unaware that such options even exist. Therefore such data collected by apps can be inadvertently published online without the user's consent or awareness (Lyne 2012).

Smart mobile devices can also be used to keep a person under surveillance. These devices contain sensors such as GPS, cameras, microphones and accelerometers that can be used to spy on individuals. The sensors can be activated remotely by third party software without the owner of the device being aware (Sabnis et al, 2012). Phishing attacks are also quite prevalent on mobile devices. Phishing attacks work by trying to lure the device owner to give up information on their own. It is an illegitimate way of extracting confidential information from a device by tricking the user to give it up willingly. The most common types of information targeted in phishing attacks is bank account numbers, online transaction passwords, and social network credentials (Assing and Cale, 2013). Web browser exploits is a category of attacks that take advantage of vulnerabilities present in web browsers used in mobile devices. Simply visiting an infected website using the mobile device can result in the installation of malware on the device or the triggering of other malicious actions on the device (Assing and Cale, 2013).

Network spoofing attacks are one of the easiest to use against mobile devices. This happens when a malicious individual pretends to be someone else in order to gain access to restricted information. An attacker in this case can setup a rogue (fake) access point which creates a Wi-Fi network. Since users are quick to connect to and use free Wi-Fi to connect to the internet, they will connect to this rogue access point thus allowing the attacker to see all the information sent by the mobile device (Gajar et al, 2009). The last category of attack is social engineering. These kinds of attacks on mobile devices are

primarily carried out in two ways. The first is through apps repackaging where a malicious individual takes a legitimate application, modifies it to include malicious code, and then puts it up for download. The second method is slightly similar but in this case the attacker creates a newer version of a legitimate app and puts it up for download (Perakovic et al, 2012).

2.4 BYOD Security and Control Measures

In order for companies to successfully and securely manage the introduction of mobile devices into the corporate workplace, it is crucial that proper policy and procedures be in place. These policies should be endorsed by executive level management for the security program to have any chance of success (Sabnis, Verbruggen, Hickey, and McBride, 2012).

A company should begin with improving the end user experience and satisfaction. The device certification process should be fast and efficient to provide timely access to state of the art technology which is also developing at an extraordinary pace. This requires that IT departments abandon their traditional rigid posture and become more agile and responsive to new technological developments. Guidelines should be documented on the devices allowed and how they are evaluated, the evaluation criteria used, and how to inform employees on those devices that are allowed on the corporate network. Communication must be clear on how the mobile devices shall be configured and how they shall be managed by both the user and the company (Apperion 2011).

Secondly, a tightly coordinated suite of technical and policy based solutions should be developed and applied consistently across a number or critical areas. These areas include:

device access controls; the ability to remotely wipe data from the device; proper configuration of the device; procedures for patching and updating the mobile device; methods for identifying and authenticating users on the device; network access control to detect and prevent unauthorized and unrecognized devices from connecting to the network; device partitioning to separate personal data from corporate data stored on the device; security controls on the device; and proper methods of monitoring activities taking place on the mobile devices (Amando et al., 2009).

Thirdly, to reduce business risk and legal liabilities, user agreements should be developed and training provided to employees. Employees should be made to understand mobile security risks, their individual responsibilities, the acceptable user policy, prerequisites for connecting any device to the network and what is considered to be inappropriate usage. A process for notifying users when they are out of compliance should be developed and should provide steps that must be taken to become compliant (Amando et al., 2009).

Fourth, application development and distribution should be simplified. Application development best practices should be used to develop software for mobile devices. These applications should be developed to be be cross platform i.e. to work across different mobile devices that are running different computing platforms. The company should also consider having an enterprise mobile application store from which employees can have a single, trusted place to download the latest mobile applications (Gajar et al., 2009).

Finally, when implementing a BYOD program, a company should seek to reduce mobile device support. This can be achieved by implementing a centralized device management

solution, registering devices with a central management application to monitor every device for health status, configuration settings, push applications, and software patches across a broad array of mobile devices (Apperion (2011). Employees should be required to sign the mobile device policy. This implies a certain level of compromise between the employee and the company. The company allows the employee to use the device of their choice, while the employee recognizes their responsibilities in regard to corporate data protection and allows a certain level of monitoring on their personal device. Eligibility is yet another aspect of the mobile device policy that must be addressed. It must be determined to whom the mobile device policy shall apply. Will it apply to only certain departments, certain job roles, or the whole organization? Will different policies be required for different departments or employees? Will some employees be restricted completely from using mobile devices on the corporate network? (Absalom, 2012).

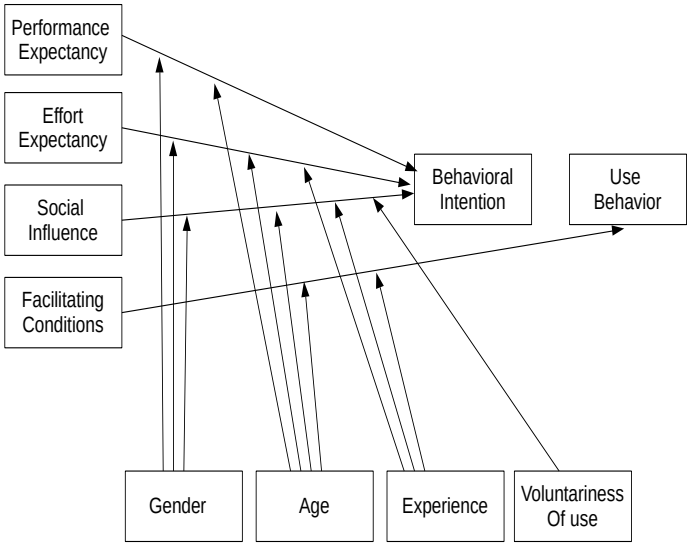
2.5 Theoretical Framework

Several theories exist that support and help to explain the BYOD phenomenon. The most comprehensive is the Unified Theory of Acceptance and Use of Technology. This theory aims to explain user intentions to use an information system and subsequent usage behavior. The theory holds that four key constructs i.e. performance expectancy, effort expectancy, social influence, and facilitating conditions are direct determinants of usage intention and behavior. Gender, age, experience, and voluntariness of use are posited to moderate the impact of the four key constructs on usage intention and behavior. The theory was developed through a review and consolidation of the constructs of eight models that earlier research had employed to explain Information System usage behavior. These models are: the theory of reasoned action, technology acceptance model,

motivational model, theory of planned behavior, model of PC utilization, innovation diffusion theory, and social cognitive theory (Venkatesh et al., 2003).

When it comes to BYOD, increased productivity (performance expectancy), ease of use (effort expectancy), status symbol (social influence), and low cost of mobile devices (facilitating conditions) have led to the BYOD phenomenon of employees bringing in their devices for work-related tasks.

Figure 2.1: Theoretical Framework



Source: Venkatesh et al. (2003)

CHAPTER THREE:RESEARCH METHODOLOGY

3.1 Introduction

This chapter presents the methodology that was used in the study. It describes the research design, population of the study, sample size, sample design, data collection method, and the data analysis techniques that were used.

3.2 Research Design

The study used the descriptive survey method. This method allowed for the collection of quantitative data which was key to this study. This method was the best method for collecting information that brought out the BYOD phenomenon and IT security, threats and countermeasures in the chosen firms. The method was suitable for describing the BYOD situation within corporate firms.

3.3 Population of study

The population of the study was all the 61 firms as listed in the Kenya Nairobi Securities Exchange Limited. A census of the entire population was conducted. A Census was the most appropriate due to small number of firms in the NSE and the nature of the data collected. Another factor that supports a census having been done was that only one IT manager or the individual in charge of IT, from each firm was chosen as a respondent and thus only a total of 61 respondents were used.

3.4 Data Collection

Primary data was collected in this study using a structured questionnaire. The questionnaire was divided into five sections. The first section collected data about the firm and respondent and the second section covered BYOD extent of use and helped

collect data that answered the first objective of the study which was to determine the extent to which BYOD is used in organizations. The third section covered benefits that motivated organizations to adopt BYOD. The fourth section covered BYOD threats and the fifth section covered countermeasures that are in place to manage BYOD**.** Two methods were used to administer the questionnaire, the first was the drop and pick later method. This method was used for firms within the vicinity of Nairobi. The second method made use of Google forms and email. This method was used for firms that are out of Nairobi. The questionnaires were delivered to the IT managers or individuals in charge of IT in each firm. These individuals were in the best position to provide data concerning the use and management of mobile devices in their respective firms.

3.5 Data Analysis

Data analysis involved a process of cleaning up the data and explanations. The data was coded and checked for possible errors and any omissions. Data were subjected to various analyses. Data in section A were analyzed using frequencies and percentages. Data in section B to section D were analyzed using frequencies, percentages, mean and standard deviation. Data in section E were analyzed using frequencies, mean, standard deviation and factor analysis. Responses from the physical and electronic questionnaire were tabulated, coded and processed to analyze the data gathered. The results were presented using tables, charts and graphs.

CHAPTER FOUR: DATA ANALYSIS, RESULTS AND DISCUSSION

4.1 Introduction

This chapter presents the analysis and findings of the study as set out in the research methodology. The research data was gathered exclusively through questionnaires. The questionnaires were designed in line with the objectives of the study. The data that was analyzed focused on the current situation of BYOD in the organization, how BYOD is managed, what advantages the firms has experienced out of adopting BYOD, what threats they have experienced and finally what counter-measures, if any, the firms have put in place to deal with BYOD threats.

4.2 Demographic Characteristics

4.2.1 Response Rate

The study targeted 61 respondents in collecting data of which 43 filled in and returned the questionnaire resulting in a 70.5% response rate. These are shown in Table 4.1.

Table 4.1:Response Rate

Response Rate	Frequency	Percentage
Responded	43	70.5
Not responded	18	29.5
Total	61	100.0

The response rate was satisfactory to make conclusions for the study. According to Mugenda and Mugenda (1999), a response rate of 50% is adequate for analysis and reporting; a rate of 60% is good and a response rate of 70% and over is excellent. Based on the assertion, the response rate was considered to be excellent.

4.2.2 Respondent Information

The respondents chosen for the study all held positions that gave them intimate knowledge about the Information Technologies that the organization had adopted. The chosen respondents were all members of the IT department and were responsible for the day to day running of the IT departments.

4.2.3 Firm Ownership

The study sought to find out the firm ownership of the firms listed on the NSE. The responses were captured using fixed-alternative questions. Percentages were used to interpret the results. The results are shown in Table 4.2.

Table 4.2:Firm Ownership

Ownership	Frequency	Percent
Local	19	44.19%
Foreign	0	0.00%
Both Local and Foreign	24	44.19%
Total	43	100.0

The findings indicate that 44.19% of the firms were locally owned, 0% were fully foreign owned and 55.81% were both local and foreign owned. By nature of being listed on the NSE, firms must have some local ownership. Thus there was an almost even split between those that were fully locally owned and those that were both local and foreign owned.

4.2.4 Number of Employees

The study sought to find out the number of employees in the firms. The responses were captured using fixed-alternative questions. Percentages were used to interpret the results. The findings are shown in Table 4.3.

Table 4.3:Number of Employees

Employees	Frequency	Percent
0 - 500	13	30.23%
501 – 1000	12	27.91%
1001 – 1500	4	9.30%
1501 – 2000	1	2.33%
2501 – 3000	2	4.65%
3001 – 3500	2	4.65%
3501 – 4000	2	4.65%
4001 – 4500	1	2.33%
4501 – 5000	2	4.65%
5000+	4	9.30%
TOTAL	43	100.00%

The findings in Table 4.3 indicate that when it comes to number of employees, 30.23% of the organizations had five hundred or less employees and 27.91% had between five hundred and one thousand employees. The majority of organizations, 32.56%, had between one thousand five hundred and five thousand employees. Only 9.3% had over five thousand employees.

4.2.5 Organization Category

The study sought to find out the organizations category. The responses were captured using fixed-alternative questions. Percentages were used to interpret the results. The findings are shown in Table 4.4.

Table 4.4:Organization Category

Category	Frequency	Percent
Agricultural	5	11.63%
Automobiles & Accessories	2	4.65%
Banking	11	25.58%
Commercial & services	9	20.93%
Manufactured & allied	3	6.98%
Energy & petroleum	2	4.65%
Insurance	2	4.65%
Investment	2	4.65%
Manufacturing & allied	5	11.63%
Telecom & Technology	2	4.65%
Growth Enterprise Market Segment	0	0.00%
TOTAL	43	100.00%

The findings in Table 4.4 indicate that the largest number of respondents were from the categories of Banking and Commercial/Services with 25.58% and 20.93% respectively.

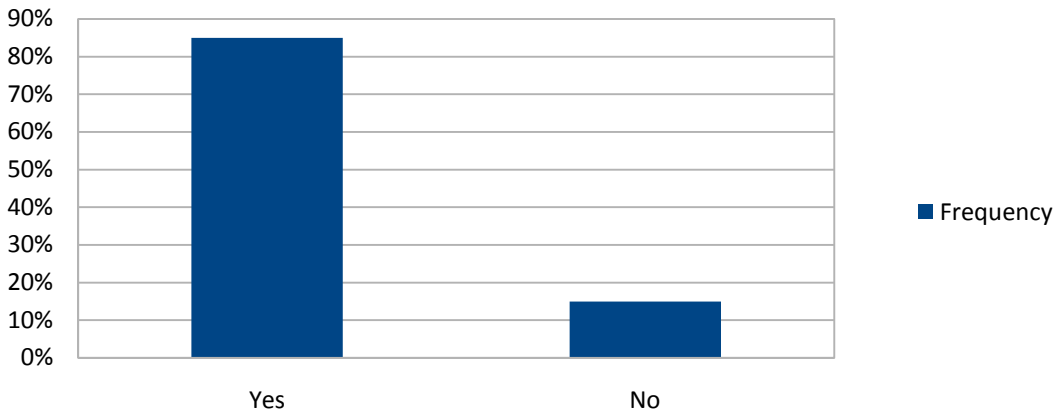
4.3 Extent to Which BYOD is Used in Firms Listed in the NSE

The study sought to find out the extent to which BYOD is used in firms listed on the NSE. The findings are elaborated in the following sections.

4.3.1 Presence of an Information Technology Security Policy

The study sought to find out the information security policy in the respective firms. The responses were captured using fixed-alternative questions. Percentages were used to interpret the results. The findings are shown in Figure 4.1.

Figure 4.1: Information Technology Security Policy

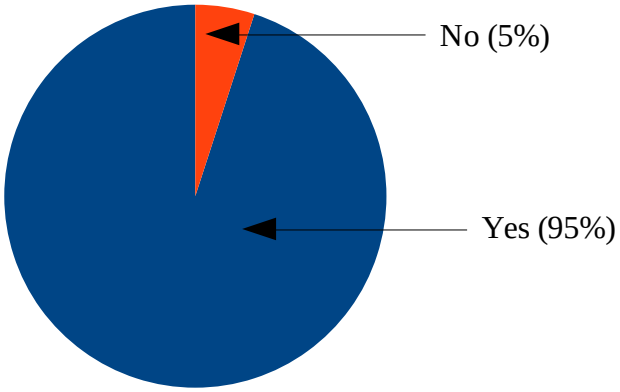


The findings indicate that out of the forty three organizations that responded, 85% had an Information Technology security policy while 15% of them did not.

4.3.2 Use of Personal Mobile Devices in Organizations

The study sought to find out the level of use of personal mobile devices in the organizations. The responses were captured using fixed-alternative questions. Percentages were used to interpret the results. The findings are shown in Figure 4.2.

Figure 4.2: Level of Staff Allowed to Use Personal Mobile Devices



The findings indicate that when it comes to allowing the use of personal mobile devices in the organization, 95% of the organizations interviewed allow their employees to use personal mobile devices for work related tasks. Only 5% of organizations do not allow the use of personal mobile devices.

4.3.3 Grade of Staff Allowed to Use Personal Mobile Devices

The study sought to find out the grade of staff allowed to use personal mobile devices. The findings are shown in Table 4.5.

Table 4.5:Grade of Staff Allowed to Use Personal Mobile Devices

Grade of Staff	Android	Apple	BlackBerry	Symbian	Windows Smartphone	Android Tablet	Apple Ipad	Windows Tablet	Laptops	Netbooks	Mean
All staff	61%	61%	53%	59%	61%	53%	53%	56%	44%	41%	**54%**
Executive Management	11%	17%	21%	12%	17%	18%	24%	22%	28%	35%	**21%**
Heads of Dept.	6%	11%	16%	6%	11%	18%	12%	11%	17%	12%	**12%**
Middle Management	22%	11%	11%	18%	11%	12%	12%	11%	6%	6%	**12%**
Mobile Workers	0%	0%	0%	0%	0%	0%	0%	0%	6%	6%	**1%**
Lower Management	0%	0%	0%	6%	0%	0%	0%	0%	0%	0%	**1%**

The findings indicate that from the information gathered and analyzed, on average, 54% of the organizations studied allowed all staff to use personal mobile devices for work

related tasks, 21% of the organizations only allowed device use amongst executive management, 12% allowed only Heads of Departments and higher grades, another 12% allowed only middle management and above, 1% allowed lower management and above, and finally another 1% allowed mobile workers and above to use personal mobile devices for work related tasks.

4.3.4 Organizational Resources Allowed on Personal Mobile Devices

The study sought to find out the organizational resources allowed on personal mobile devices. The responses were captured using Likert Scale: 1 – no extent; 2 – small extent; 3 – moderate extent; 4 – large extent; and 5 – very large extent. The mean and standard deviations of the responses were calculated. The mean values were interpreted using the Likert Scale. The results are shown in Table 4.5 below.

Table 4.5:Extent to Which Resources are Allowed on Personal Mobile Devices

Resources Allowed On Personal Mobile Devices	No Extent	Small Extent	Moderate Extent	Large Extent	Very Large Extent	Mean Score	Std. Deviation
	1	2	3	4	5		
	Frequency						
Email Resources	2	0	2	9	30	**4.51**	**0.96**
Voice Calls	4	4	5	5	25	**4.00**	**1.40**
Corporate Files And Documents	2	7	7	22	5	**3.49**	**1.05**
Customer Information	7	7	5	19	5	**3.19**	**1.31**
Instant Messaging	6	8	13	8	8	**3.09**	**1.30**
Accounting and Financial Information	12	12	9	5	5	**2.51**	**1.33**
IT Support	17	9	5	7	5	**2.40**	**1.45**
Video Conference	20	9	5	0	9	**2.28**	**1.56**

The findings of the study indicatedthat Email resources had the highest mean of 4.51 and thus were the most accessed corporate resource via personal mobile devices. Email access via personal mobile devices was allowed to a very large extent. Instant messages

were allowed to a moderate extent with a mean of 3.09.Video conferencing had the lowest mean of 2.28 revealing that access to this resource was allowed to a small extent.

4.3.5 Corporate Operations Allowed on Personal Mobile Devices

The study sought to find out the corporate operations allowed on personal mobile devices.The responses were captured using Likert Scale: 1 – no extent; 2 – small extent; 3 – moderate extent; 4 – large extent; and 5 – very large extent. The mean and standard deviations of the responses were calculated. The mean values were interpreted using the Likert Scale. The results are shown in Table 4.6.

Table 4.6:Extent to Which Corporate Operations are Allowed on Personal Mobile Devices

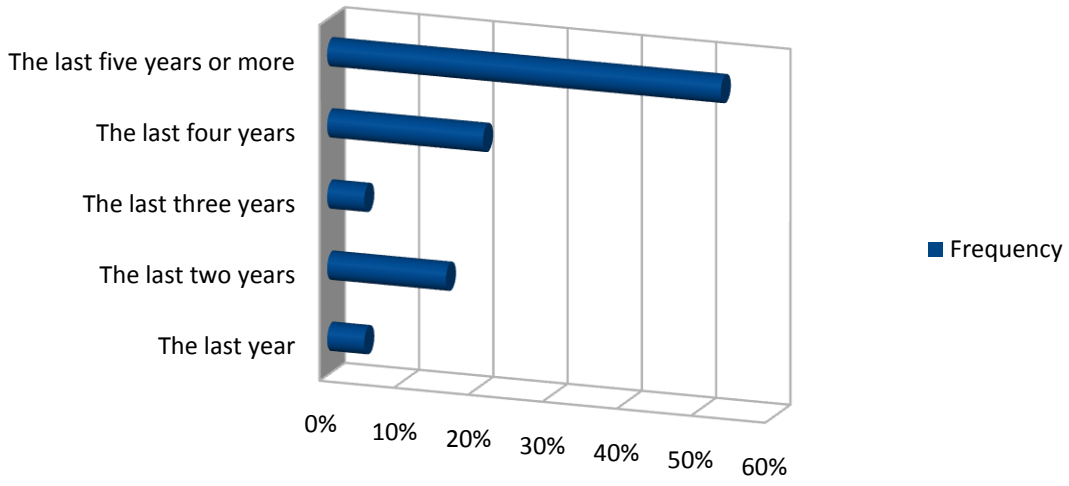
Corporate Operations Allowed On Personal Mobile Devices	No Extent	Small Extent	Moderate Extent	Large Extent	Very Large Extent	Mean Score	Std. Deviation
	1	2	3	4	5		
	Frequency						
Marketing Operations	2	2	5	16	18	**4.07**	**1.08**
IT Management Operations	18	2	7	14	2	**2.53**	**1.44**
Security Operations	19	3	13	5	3	**2.30**	**1.34**
Procurement Operations	18	7	12	3	3	**2.21**	**1.26**
Human Resource Operations	15	13	10	5	0	**2.12**	**1.03**
Accounting Operations	20	5	12	3	3	**2.16**	**1.29**
Transport Operations	21	6	10	6	0	**2.02**	**1.14**
Manufacturing Operations	24	10	6	0	3	**1.79**	**1.15**

The findings provided by the research indicated that organizations in the NSE allowed marketing operations on personal mobile devices to a large extent. Marketing operations had the highest mean of 4.07. IT management operations such as remote monitoring of corporate systems were allowed to a moderate extent. Transport operations had the lowest mean of 2.02 thus revealing that access to this resource via mobile devices was not allowed.

4.3.6 Number of Years BYOD Has Been Allowed in the Organization

The study sought to find out the number of years BYOD has been allowed in the organization. The responses were captured using fixed-alternative questions. Percentages were used to interpret the results. The results are shown in Figure 4.3.

Figure 4.3: Number of Years BYOD Has Been allowed in the Organization



Findings provided by the research revealed that 53% of the organizations in the NSE begun allowing the use of personal mobile devices in the organization five or more years ago, 21% of the organizations begun four years ago, 5% within the last three years, 16% within the last two years and 5% within the last year.

4.4 Drivers that Led to the Adoption of BYOD

The study sought to find out the drivers that led to the adoption of BYOD. The responses were captured using Likert Scale: 1 – no extent; 2 – small extent; 3 – moderate extent; 4 – large extent; and 5 – very large extent. The mean and standard deviations of the responses

were calculated. The mean values were interpreted using the Likert Scale. The results are shown in Table 4.7.

Table 4.7:Drivers that Led to the Adoption of BYOD

Drivers That Led To The Adoption of BYOD	No Extent	Small Extent	Moderate Extent	Large Extent	Very Large Extent	Mean Score	Std. Deviation
	1	2	3	4	5		
	Frequency						
Improved employee working mobility	5	5	2	18	13	**3.67**	**1.34**
Improved employee productivity and efficiency	4	4	4	16	15	**3.79**	**1.28**
Demand for flexible working hours	5	6	2	16	14	**3.65**	**1.38**
End user demand	5	7	7	7	17	**3.56**	**1.45**
Management pressure	3	14	6	10	10	**3.23**	**1.32**
Employee morale boost	8	5	14	11	5	**3.00**	**1.27**
Reduced total cost of IT infrastructure ownership	8	9	7	14	5	**2.98**	**1.34**
Reduced capital expenditure on IT equipment	9	11	5	14	4	**2.84**	**1.34**
Project a professional image towards clients and other third parties	11	11	7	14	0	**2.56**	**1.20**
Reduction of IT technical support costs	12	17	5	5	4	**2.35**	**1.27**

The study sought to find out what were the drivers that led organizations to adopt BYOD in the workplace. According to the data collected, the biggest driver that led to organizations adopting BYOD was improved employee productivity and efficiency which had the highest mean of 3.79. Reduction of IT technical support had the lowest mean of 2.35 and therefore had the least influence on the adoption of BYOD in organizations listed in the NSE.

4.5 Benefits that Have Been Realized as a Result of BYOD Adoption

The study sought to find out the benefits that have been realized as a result of BYOD adoption. The responses were captured using Likert Scale: 1 – no extent; 2 – small extent; 3 – moderate extent; 4 – large extent; and 5 – very large extent. The mean and standard

deviations of the responses were calculated. The mean values were interpreted using the Likert Scale. The results are shown in Table 4.8.

Table 4.8:Benefits Realized From Adopting BYOD

Benefits Realized From Adopting BYOD	No Extent	Small Extent	Moderate Extent	Large Extent	Very Large Extent	Mean Score	Std. Deviation
	1	2	3	4	5		
	Frequency						
Flexible working hours	4	3	14	10	12	**3.53**	**1.24**
Improved Employee morale	3	12	19	7	2	**2.84**	**0.95**
Improved employee productivity and efficiency	3	21	10	7	2	**2.63**	**1.00**
Project a professional image towards clients and other third parties	14	3	17	9	0	**2.49**	**1.16**
Reduced total cost of IT infrastructure ownership	17	12	5	9	0	**2.14**	**1.17**
Reduced capital expenditure on IT equipment	17	12	7	7	0	**2.09**	**1.11**
Improved employee working mobility	5	13	0	3	22	**3.56**	**1.62**
Reduced operational costs	26	3	6	5	3	**1.98**	**1.37**
Increase in sales and revenue	23	10	7	0	3	**1.84**	**1.15**
Reduction of IT technical support costs	24	6	11	2	0	**1.79**	**0.99**

The study sought to find out the actual benefits that organizations had realized as a result of allowing the use of personal mobile devices for work related tasks. Improved employee working mobility had the highest mean of 3.56 indicating organizations realized this benefit to a large extent. Reduction of IT technical support costs had the lowest mean of 1.79 indicating that this benefit was realized to a small extent by organizations.

4.6 Threats Experienced as a Result of BYOD Adoption

The study sought to find out the threats that organizations have experienced as a result of BYOD adoption. The responses were captured using Likert Scale: 1 – no extent; 2 – small extent; 3 – moderate extent; 4 – large extent; and 5 – very large extent. The mean

and standard deviations of the responses were calculated. The mean values were interpreted using the Likert Scale. The results are shown in Table 4.9

Table 4.9:BYOD Threats

BYOD Threats	No Extent	Small Extent	Moderate Extent	Large Extent	Very Large Extent	Mean Score	Std. Deviation
	1	2	3	4	5		
	Frequency						
Theft of mobile device	2	9	7	14	11	**3.53**	**1.22**
Misplacing of mobile device	5	9	9	16	4	**3.12**	**1.20**
Unauthorized tethering	20	2	5	16	0	**2.40**	**1.40**
Virus infection	7	20	14	0	2	**2.30**	**0.91**
Unauthorized WI-FI access point	21	0	15	7	0	**2.19**	**1.22**
Device Rooting	22	9	9	3	0	**1.84**	**1.00**
Theft of company proprietary information	25	9	5	2	2	**1.77**	**1.13**
Spy-ware infection	23	13	5	2	0	**1.67**	**0.87**
Identity theft	27	9	7	0	0	**1.53**	**0.77**
Corporate espionage	29	7	7	0	0	**1.49**	**0.77**
Data leakage to public online websites	25	18	0	0	0	**1.42**	**0.50**
Rogue Access Point	36	0	5	2	0	**1.37**	**0.87**
System intrusion/attack	36	2	5	0	0	**1.28**	**0.67**
Financial fraud	34	7	2	0	0	**1.26**	**0.54**

The study sought to find out actual threats that have been brought about by BYOD adoption and to what extent these threats have affected organizations in the NSE. Theft of mobile device had the highest mean of 3.53 having been experienced to a large extent.Financial fraud using mobile devices had the lowest mean of 1.26 indicating that this threat was experienced to no extent.

4.7 Countermeasures Adopted to Mitigate BYOD Threats

4.7.1 BYOD Countermeasures Mean and Standard Deviation

The study sought to identify the counter-measures that organizations had implemented to mitigate threats that have arisen from the adoption of BYOD. The responses were

captured using Likert Scale: 1 – no extent; 2 – small extent; 3 – moderate extent; 4 – large extent; and 5 – very large extent. The mean and standard deviations of the responses were calculated. The mean values were interpreted using the Likert Scale. The results are presented in Table 4.10.

Table 4.10:BYOD Threat Counter-measures

BYOD Threat Countermeasures	No Extent	Small Extent	Moderate Extent	Large Extent	Very Large Extent	Mean Score	Std. Deviation
	1	2	3	4	5		
	Frequency						
Firewalls	5	2	2	9	25	**4.09**	**1.38**
User awareness, training and/or education	6	7	9	14	7	**3.21**	**1.30**
Mobile Device security policy	11	9	0	14	9	**3.02**	**1.57**
Intrusion detection/ Intrusion prevention system	13	2	7	16	5	**2.95**	**1.46**
Signing of user agreements (terms of usage)	7	16	5	9	6	**2.79**	**1.34**
Network access control	9	9	11	9	5	**2.81**	**1.31**
Installation of security software such as anti-virus / anti-malware on the device	14	11	5	2	11	**2.65**	**1.60**
Software Patching / Software updates	23	2	5	2	11	**2.44**	**1.74**
Data leakage prevention system	20	5	5	11	2	**2.30**	**1.41**
Data classification to control / monitor flow of information out of the organization	25	5	4	9	0	**1.93**	**1.24**
Data watermarking to control / monitor flow of information out of the organization	25	5	4	9	0	**1.93**	**1.24**
Minimum security baseline for mobile devices	18	11	11	3	0	**1.98**	**0.99**
Mobile device encryption	27	7	2	5	2	**1.79**	**1.24**
Mobile device management system	27	10	2	2	2	**1.65**	**1.09**
Remote wiping of mobile device	30	7	2	2	2	**1.58**	**1.10**
Remote tracking of mobile device	32	5	4	0	2	**1.49**	**1.01**
Enterprise mobile application store	34	5	2	2	0	**1.35**	**0.78**
Partitioning to separate corporate data from personal data on the mobile device	34	7	2	0	0	**1.26**	**0.54**
Complete ban on mobile device usage	36	5	2	0	0	**1.21**	**0.51**

The results show that when it comes to implementing technical counter-measures, most organizations had implemented the traditional firewall to a large extent though the primary focus of a firewall is not in securing mobile devices but in securing server farms and system perimeters. Implementation of firewalls had the highest mean of 4.09. Non-

technical counter-measures such as user awareness or training and mobile device security policy had been implemented to a moderate extent. Intrusion detection systems had also been implemented to a moderate extent though similar to firewalls, this counter-measure is not specific to mobile devices. Counter-measures that are specifically designed for mobile devices such as security baselines, mobile device encryption, mobile device management systems, remote wiping of mobile device data, and remote tracking of mobile devices was found to have been implemented to a small extent. A complete ban on mobile device use had the lowest mean of 1.21 indicating that almost all organizations in the NSE did not consider this as a countermeasure for BYOD threats.

4.7.2 Factor Analysis

Responses collected on the BYOD counter-measures were subjected to further factor analysis. Communality is the proportion of variance that each item has with other items. The proportion of variance that is unique to each item is then the respective items total variance minus the communality. Table 4.11 shows the communalities. The extraction method was the principal component analysis.

Table 4.11Factor Analysis (Communalities)

Communalities		
	Initial	**Extraction**
Mobile Device security policy	1.000	.835
User awareness, training and/or education	1.000	.881
Signing of user agreements (terms of usage)	1.000	.821
Mobile device management system	1.000	.911
Complete ban on mobile device usage	1.000	.717
Network access control	1.000	.682
Remote tracking of mobile device	1.000	.838
Remote wiping of mobile device	1.000	.809
Mobile device encryption	1.000	.925
Partitioning to separate corporate data from personal data on the mobile device	1.000	.958

Data classification to control / monitor flow of information out of the organization	1.000	.883
Data watermarking to control / monitor flow of information out of the organization	1.000	.892
Data leakage prevention system	1.000	.941
Enterprise mobile application store	1.000	.831
Minimum security baseline for mobile devices	1.000	.911
Intrusion detection/ Intrusion prevention system	1.000	.859
Firewalls	1.000	.796
Installation of security software such as anti-virus / anti-malware on the device	1.000	.854
Software Patching / Software updates	1.000	.870
Extraction Method: Principal Component Analysis.		

4.7.3 Factor Extraction

Table 4.12 presents the total variance of all the factors. Principal component analysis was used to extract factors which totaled 19. Eigen values indicate the relative importance of each factor accounting for a particular set and hence those with small Eigen values were left out. According to Table 4.12 only 5 factors were significant for analysis.

Table 4. 12Factor Extraction (Total Variance)

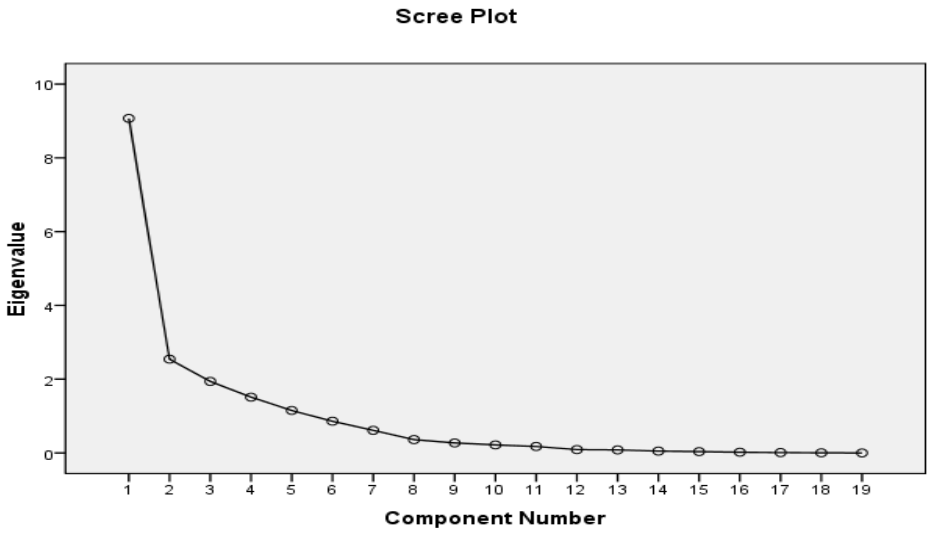
Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	9.070	47.737		5.284	27.811	27.811
2	2.542	13.379		3.553	18.699	46.511
3	1.939	10.204		3.019	15.887	62.398
4	1.513	7.961		2.713	14.277	76.675
5	1.151	6.057		1.646	8.663	85.338
6	.860	4.524	89.862			
7	.611	3.218	93.080			
8	.362	1.903	94.983			
9	.271	1.428	96.412			
10	.217	1.145	97.556			
11	.175	.920	98.476			

12	.091	.478	98.955			
13	.082	.430	99.385			
14	.050	.262	99.646			
15	.035	.187	99.833			
16	.020	.106	99.939			
17	.009	.046	99.985			
18	.002	.013	99.998			
19	.000	.002	100.000			
Extraction Method: Principal Component Analysis.						

4.7.4 Scree Plot

This is a plot of the factor Eigen values against the component numbers. According to scree plot in Figure 4.4, the study could only consider 5 factors because the curve tends to flatten from the fifth components onwards, due to relatively low factor Eigen values.

Figure 4.4Scree Plot



4.7.5 Component Matrix

Component Matrix contains the relative Eigen values in respect of each factor. Each factor belongs to one of the sets of factors extracted and is determined by the Eigen values of the factors relative to each set. Table 4.13 shows which set of factors falls into.

Table 4. 13Factor Analysis (Component Matrix)

Component Matrix[a]					
	Component				
	1	2	3	4	5
Mobile Device security policy	.669	.140			.454
User awareness, training and/or education	.682	.484			.166
Signing of user agreements (terms of usage)	.592	.132		.128	
Mobile device management system	.836		.093	.432	
Complete ban on mobile device usage		.257	.515	.388	.470
Network access control	.742	.018		.092	
Remote tracking of mobile device	.616	.257		.427	
Remote wiping of mobile device	.678		.063	.026	
Mobile device encryption	.744		.118		.081
Partitioning to separate corporate data from personal data on the mobile device	.875		.264	.323	
Data classification to control / monitor flow of information out of the organization	.704	.562	.139		
Data watermarking to control / monitor flow of information out of the organization	.645	.585	.270		.064
Data leakage prevention system	.686	.605	.235		
Enterprise mobile application store]	.584	.085	.505	.384	.285
Minimum security baseline for mobile devices	.713				.535
Intrusion detection/ Intrusion prevention system	.792		.101		.032
Firewalls	.463		.420		
Installation of security software such as anti-virus / anti-malware on the device	.789		.004	.019	
Software Patching / Software updates	.830		.140		
Extraction Method: Principal Component Analysis.					
a. 5 components extracted.					

Table 4.13 presents factor analysis of BYOD countermeasures using extraction method: principal component analysis with 5 components extracted. Each number represents the correlation between the item and the un-rotated factor. These correlations help formulate an interpretation of the factors or components. This is done by looking for a common

thread among the variables that have large loadings for a particular factor or component. The Table shows that the majority of the critical success factors had high loadings.

From Table 4.13 we can see that all variables that measure BYOD countermeasures in one way or another are highly correlated with this factor.

Table 4. 14Factor Analysis (Rotated Component Matrix)

	Component				
	1	**2**	**3**	**4**	**5**
Mobile Device security policy			.852		
User awareness, training and/or education			.726		
Signing of user agreements (terms of usage)				.597	
Mobile device management system				.631	
Complete ban on mobile device usage					.814
Network access control			.508		
Remote tracking of mobile device				.860	
Remote wiping of mobile device	.878				
Mobile device encryption	.934				
Partitioning to separate corporate data from personal data on the mobile device	.691				
Data classification to control / monitor flow of information out of the organization		.835			
Data watermarking to control / monitor flow of information out of the organization		.858			
Data leakage prevention system		.827			
Enterprise mobile application store	.400				.735
Minimum security baseline for mobile devices			.812		
Intrusion detection/ Intrusion prevention system	.658				
Firewalls		.701			
Installation of security software such as anti-virus / anti-malware on the device	.857				
Software Patching / Software updates	.856				
Extraction Method: Principal Component Analysis. *Rotation Method: Varimax with Kaiser Normalization*.					

4.7.6 Factor Isolation

Factor isolation involves isolating each of the variable factors and grouping them by these 5 extracted factors based on their factor loadings on each set. Table 4.15 shows the factors grouped with a minimum correlation of 0.4.

Table 4. 15Isolation of Factors

Factor Group	Variables
Factor 1 – Data & Anti-Malware Security	• Remote wiping of mobile device • Mobile device encryption • Partitioning to separate corporate data from personal data on the mobile device • Enterprise mobile application store • Intrusion detection/ Intrusion prevention system • Installation of security software such as anti-virus / anti-malware on the device • Software Patching / Software updates
Factor 2 – Information flow Controls	• Data classification to control / monitor flow of information out of the organization • Data watermarking to control / monitor flow of information out of the organization • Data leakage prevention system • Firewalls
Factor 3 – Policies and Training	• Mobile Device security policy • User awareness, training and/or education • Network access control • Minimum security baseline for mobile devices
Factor 4 – Usage Control and Monitoring	• Signing of user agreements (terms of usage) • Mobile device management system • Remote tracking of mobile device
Factor 5 – Usage Banning	• Complete ban on mobile device usage • Enterprise mobile application store

Table 4.15 shows there are 5 extracted group factors. Extracted group factors 1,2,3contain the most number of variable components which determine BYOD countermeasures. Factors 1, data and anti-malware security isolates the majority of the factors representing BYOD countermeasures in Table 4.14 and includes the following Factors (i) Remote wiping of mobile device; (ii) Mobile device encryption; (iii) Partitioning to separate corporate data from personal data on the mobile device; (iv)

Enterprise mobile application store; (v) Intrusion detection/ Intrusion prevention system; (vi) Installation of security software such as anti-virus / anti-malware on the device and (vii) Software Patching / Software updates

Factor 2, information flow controls, comprises of (i) Mobile Device security policy; (ii) User awareness, training and/or education; (iii) Network access control and (iv) Minimum security baseline for mobile devices

Factor 3, policies and training, comprises of (i) Mobile Device security policy; (ii) User awareness, training and/or education; (iii) Network access control and (iv) Minimum security baseline for mobile devices

Factor 4, usage control and monitoring, comprises of (i) Signing of user agreements (terms of usage); (ii) Mobile device management system and (iii) Remote tracking of mobile device

Factor 5, usage banning, comprises (i) Complete ban on mobile device usage and (ii) Enterprise mobile application store

It is clear that most of the 19 factors listed in the questionnaires were grouped together by their correlation with each other and brought down a total of 5 main group factors. The most number of factors were in group 1 while few elements fell in factor group 3, 4 and 5.

CHAPTER FIVE: SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

From the analysis and data collected, the following discussions, conclusion and recommendations were made. The responses were based on the objectives of the study which sought to determine the extent to which BYOD is used in firms listed in the NSE, determine the accompanying benefits that BYOD has brought to firms listed in the NSE, to determine the extent to which BYOD causes threats to corporate IT systems belonging to organizations listed in the NSE and to determine measures that are in place to counter the threats brought about by BYOD that have been adopted by firms in the NSE.

5.2 Summary

The study found out that the respondents chosen for the study all held positions that gave them intimate knowledge about the Information Technologies that the organization had adopted. The chosen respondents were all members of the IT department and were responsible for the day to day running of the IT departments. The findings also indicate that 44.19% of the firms were locally owned, 0% were fully foreign owned and 55.81% were both local and foreign owned. By nature of being listed on the NSE, firms must have some local ownership. Thus there was an almost even split between those that were fully locally owned and those that were both local and foreign owned.

The study also found out that when it comes to the number of employees, 30.23% of the organizations had five hundred or less employees and 27.91% had between five hundred and one thousand employees. The majority of organizations, 32.56%, had between one thousand five hundred and five thousand employees. Only 9.3% had over five thousand

employees. In addition the study found out that the largest number of respondents were from the categories of Banking and Commercial/Services with 25.58% and 20.93% respectively.

On the companies that had an information security policy, the study found out that out of the forty three organizations that responded, 85% had an Information Technology security policy while 15% of them did not. In addition when it comes to allowing the use of personal mobile devices in the organization, 95% of the organizations interviewed allow their employees to use personal mobile devices for work related tasks. Only 5% of organizations do not allow the use of personal mobile devices.

The study also found out that on average, 54% of the organizations studied allowed all staff to use personal mobile devices for work related tasks, 21% of the organizations only allowed device use amongst executive management, 12% allowed only Heads of Departments and higher grades, another 12% allowed only middle management and above, 1% allowed lower management and above, and finally another 1% allowed mobile workers and above to use personal mobile devices for work related tasks.

On the BYOD devices used in the organizations the study found out that the information collected indicated that the most accessed corporate resources via personal mobile devices were Email, voice calls and corporate files and documents. Email access via personal mobile devices was allowed to a very large extent, voice calls were allowed to a large extent and access to corporate files and documents was allowed to a moderate extent. The least allowed corporate resources were video conference, IT support and customer information which were allowed to a small extent.

The study also found out that organizations in the NSE allow marketing operations on personal mobile devices to a large extent. IT management operations such as remote monitoring of corporate systems are allowed to a moderate extent, and all other operations are allowed to a small extent. In addition the findings provided by the research revealed that 53% of the organizations in the NSE begun allowing the use of personal mobile devices in the organization five or more years ago, 21% of the organizations begun four years ago, 5% within the last three years, 16% within the last two years and 5% within the last year.

The study sought to find out what were the drivers that led organizations to adopt BYOD in the workplace. According to the data collected, the biggest drivers that led to organizations adopting BYOD were improved employee working mobility, improved employee productivity and efficiency, demand for flexible working hours and end user demand. These four drivers contributed to BYOD adoption to a large extent. The study also found out that the actual benefits that organizations had realized as a result of allowing the use of personal mobile devices for work related tasks. The benefit of flexible working hours was realized to a large extent. Improved employee morale, improved employee productivity and efficiency and projection of a professional image towards clients and third parties was realized to a moderate extent.

On the threats brought out by BYOD adoption, the study found out that theft of mobile device had been experienced to a large extent, and misplacing of mobile devices by employees had been experienced to a moderate extent. The more advanced threats such as unauthorized tethering, virus infection, unauthorized Wi-Fi, device rooting, theft of proprietary information, spyware infection and identity theft were experienced to a small

extent. The results show that when it comes to implementing technical counter-measures, most organizations had implemented the traditional firewall to a large extent though the primary focus of a firewall is not in securing mobile devices but in securing server farms and system perimeters. Non-technical counter-measures such as user awareness or training and mobile device security policy had been implemented to a moderate extent. Intrusion detection systems had also been implemented to a moderate extent though similar to firewalls, this counter-measure is not specific to mobile devices. Counter-measures that are specifically designed for mobile devices such as security baselines, mobile device encryption, mobile device management systems, remote wiping of mobile device data, and remote tracking of mobile devices was found to have been implemented to a small extent.

Finally factor analysis was carried out on the BYOD countermeasures to extract the most effective and significant countermeasures for BYOD. The analysis revealed that implementing remote wiping of mobile devices, mobile device encryption, mobile device data partitioning, a mobile application store, intrusion preventions systems, mobile security software, and system patching are the best countermeasures for a BYOD enabled organization.

5.3 Conclusion

The survey revealed that 95% of the organizations interviewed allowed employees to use a large range of personal mobile devices for work related tasks. The devices allowed included laptops, smart-phones, net-books and tablets. Just over half of all the organizations interviewed allowed all staff to use their own personal mobile devices to access corporate resources. The most accessed corporate resource was email which was

accessed to a very large extent. Of key note is that only 85% of the companies had an IT security policy in place. This means that 10% of the organizations interviewed are allowing BYOD use yet they have no IT security policy in place. Having an IT policy in place does not necessarily mean that the policy addresses BYOD concerns. This is reflected in the fact that a mobile device security policy had been implemented only to a moderate extent as a counter-measure to BYOD threats by the organizations surveyed.

They survey also revealed that the main benefits that organizations have realized from adopting BYOD include flexible working hours, morale boost amongst employees, increase in productivity and efficiency, and projection of a professional corporate image. Surprisingly increase in sales and revenue and reduced operational costs were experienced to a small extent. This shows that the benefits organizations derive from adopting BYOD are non-financial.

The largest threat that came about by adopting BYOD was the unsophisticated theft and misplacement of mobile devices. The sophistication of attacks in the organizations surveyed was found to be very low. Advanced attacks such as system intrusion, financial fraud via mobile device, corporate espionage and identity theft are rarely if ever seen however as mobile device proliferation in organizations continues, this vector of attack may become irresistible to attackers. Most organizations had a low implementation rate of mobile device security and countermeasures. Non-technical counter-measures such as training, policies and user agreements had been implemented to a moderate extent and the technical countermeasures such as device encryption, data partitioning and mobile device management systems had been implemented to a small extent. This shows that most organizations are not prepared for BYOD management.

5.4 Recommendations

It may only be a matter of time before attackers take notice of the prevalence of the mobile device and begin devising ways of exploiting corporate resources through them. Organizations should take a top down approach. Top level management should be sensitized on BYOD trends and threats so as to get management support. IT security policies should be reviewed to ensure they also cater for and include BYOD control and management. Training and awareness programs should be developed to enlighten employees. Technical measures that organizations should implement to protect their assets include:

- Remote wiping of mobile device
- Mobile device encryption
- Partitioning to separate corporate data from personal data on the mobile device
- Enterprise mobile application store
- Intrusion detection/ Intrusion prevention system
- Installation of security software such as anti-virus / anti-malware on the device
- Software Patching / Software updates

5.5 Limitations of the Study

Time was a major limiting factor. The time to collect data was very short given the deadlines required of this paper. In some organizations it was impossible to get the most senior official in charge of information systems to answer the questionnaire however the next in charge or officers within the department were cooperative. Getting responses within the stipulated time frame for data collection was also a challenge.

5.6 Suggestions for Further Research

Following the discussions presented in this study, the research suggests further research be carried out on the rate and extent of cannibalization of traditional computers and laptops by the adoption of mobile devices and how this cannibalization and proliferation affects the working dynamics in the corporate workplace.

REFERENCES

Aberdeen Group (2012). Endpoint Security and Endpoint Management in the Era of Enterprise Mobility and BYOD: Still Better Together. *An Aberdeen Group Whitepaper*, 4, 6, 9.

Absalom R. (2012). International Data Privacy Legislation Review: A Guide for BYOD Policies. *Ovum Consulting, IT006-000234,* 3-5.

Apperian (2011). Protecting Corporate Data in the "BYOD" Environment. *Apperian, Inc. byod.wp.v110803,* 4-6.

Armando A. Costa G., Merlo A., and Verderame L., (2009). Securing the "Bring Your Own Device" Policy. *Journal of Internet Services and Information Security (JISIS) volume: 2, 5-16.*

Assing D. and Cale S. (2013). Mobile Access Safety: Beyond BYOD. *ISTE Ltd and John Wiley & Sons Inc, 978-1-84821-435-4,* 7, 65, 157, 173.

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/BYODGuide,* 1,4,8.

Drury A. and Absalom R. (2012). BYOD: an emerging market trend in more ways than one. *Logicalis Group Whitepaper,* 4-5.

Eschelbeck G. and Schwartzberg D. (2012). BYOD risks and rewards. *A Sophos Whitepaper 06.12v1.dNA,* 1-7.

Forrester Research (2010). Share of US Consumer PC sales by form factor, 2008 to 2015. *Forrester Research Incorporated.*

Gajar K.P., Ghosh A. and Rai S. (2013). Bring your own device (BYOD): security risks and mitigating strategies. *Journal of Global Research in Computer Science, Volume 4 No. 4,* 1-3, 7.

Gessner D., Girao J., Karame G. and Li W. (2013). Towards a User-Friendly Security Enhancing BYOD Solution. *NEC Technical Journal Vol.7 No.3/2013,* 1-4.

Good Technology (2012). Bring your own device: Individual liable user policyconsiderations. A *VISTO corporation and Good Technology whitepaper, IL_Policy_Jan2012_US, 6,8.*

Lyne, J. (2012). Eight trends that are changing network security. *A Sophos article, 04.12v1.dNA,* 2.

Miller K.W., Voas J., and Hurlburt G.F. (2012). BYOD: Security and Privacy Considerations. *IEEE Computer Society, 1520-9202/12,* 1-3.

Miller-Merrel J. (2012). The Workplace Engagement Economy Where HR, Social, Mobile, and Tech Collide. *Wiley Periodicals Inc, DOI 10.1002/ert.21359,* 1, 7.

Nairobi Securities Exchange Limited (2013). Listed Companies. Retrieved August 25th 2013 from https://www.nse.co.ke/listed-companies/list.html

NPD Group (2003). Canadians spent more than $4.66 billion on technology products. Retrieved May 26th 2013 from https://www.npd.com/wps/portal/npd/us/news/press-releases/pr_100209a...

Oliver R. (2012). Why the byod boom is changing how we think about business IT. *E and T Magazine, November 2012 Issue.*

Osterman Research Inc. (2012). Putting IT Back in Control of BYOD. *An Osterman Research Whitepaper,* 3, 5-6, 8.

Perakovic D., Husnjak S. and Remenar V. (2012). Research of security threats in the use of modern terminal devices. *DAAAM International,* 1-4.

Pieterson M.N.B. (2009). Benefits of IT (Information Technology) in Modern Day Business. Retrieved July 20th 2013 from http://www.modernghana.com/news/242392/1/benefits-of-it-information-technology-in-modern-da.html

Sabnis S., Verbruggen M., Hickey J., and McBride J. (2012). Intrinsically Secure Next Generation Networks. *Bell Labs Technical Journal 17(3),* 19.

Sans Institute (2012). Mobility / BYOD Security Survey. *A Sans Institute Research Paper*, 21.

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

UBM Techweb (2012). How Technology Executives are Managing the Shift to BYOD: An analysis of the benefits and hurdles of enabling employees to use their own consumer devices in the workplace. *A UBM Techweb whitepaper, september 2012,* 2-3.

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

WatchGuard (2013). Ten Tips for Establishing a Secure Foundation for BYOD. *WatchGuard Technologies Whitepaper,* 2-7.

Zikmund W., Babin B., Carr J., and Griffin M. (2009). Business Research Methods. *Cengage Learning, eighth edition,* 68.

APPENDICES

APPENDIX I: QUESTIONNAIRE

I am undertaking a research on "Bring your own device" (BYOD) and IT Security as part of the requirements of the MBA degree. It is for this reason that I am requesting you to spare a few minutes to fill in the following questionnaire.

This is a study into the "Bring your own device" (BYOD) phenomenon and its impact on IT Security in the Kenyan corporate environment. Please respond by ticking or filling the appropriate spaces on the following questionnaire.

SECTION A

RESPONDENT INFORMATION

1. Your Name
   ….....
2. Your Position within the organization
   .....
3. Your Department
   ….....

FIRM INFORMATION

1. Name of organization
   ….....
2. Ownership:
   Local..... ( )
   Foreign..... ( )
   Both (local and foreign).. ( )
3. Date of incorporation
   ….....
4. Number of employees:
   0 - 500 ( )
   501 – 1000 ( )
   1001 – 1500 ( )

1501 – 2000 ( )

2001 – 2500 ( )

2501 – 3000 ( )

3001 – 3500 ( )

3501 – 4000 ( )

4001 – 4500 ( )

4501 – 5000 ( )

5000 + ( )

5. Number of branches.....

6. Organization category:

Agricultural..... ( )

Automobiles & Accessories..... ( )

Banking..... ( )

Commercial & services..... ( )

Construction & allied..... ( )

Energy & petroleum..... ( )

Insurance..... ( )

Investment..... ( )

Manufacturing & allied..... ( )

Telecommunication & Technology..... ( )

7. Does your organization have an IT security policy in place?

Yes ( ) No ( )

SECTION B: BYOD EXTENT OF USE

1. Does your organization allow the use of personal mobile devices for organizational work including accessing corporate resources in the workplace?

Yes ( ) No ( )

2. Which grade of staff is allowed to bring in their own personal mobile devices and use them for organizational work including accessing corporate resources in the workplace and which devices are allowed? (Tick the appropriate box)

	STAFF							
		Executive management	Heads of Department	Middle Management	Lower management	Mobile Workers (Those who are not stationed at a desk)	All staff	Other, specify
DEVICES	Android Smartphones							
	Apple Iphones							
	Blackberry							
	Symbian smartphones							
	Windows Smartphones							
	Android tablets							
	Apple Ipads							
	Windows Tablets							
	Laptops							
	Net-books							

	Other, specify ….....							

3. To what extent are employees allowed to access each of the following organization's resources using their own personal mobile devices? (Tick the appropriate box)

Resource	No extent	Small extent	Moderate Extent	Large Extent	Very Large Extent
Corporate files and documents					
Customer information					
IT support					
Accounting & Financial information					
Email Resources					
Instant Messaging					
Video Conference					
Voice Calls					
Others, specify ….....					

4. To what extent are employees allowed to perform each of the following operations using their own personal mobile devices? (Tick the appropriate box)

Operations	No extent	Small extent	Moderate Extent	Large Extent	Very Large Extent
Marketing Operations					
Human Resource Operations					
Procurement Operations					
Accounting Operations					
Manufacturing Operations					
Transport Operations					
IT Management Operations					
Security Operations					
Others, specify ….....					

5. For how long has your organization allowed the use of employees' own personal mobile computing devices for work-related tasks?

The last year.....…..... ( )

The last two years..... ( )

The last three years.....…..... ( )

The last four years..... ( )

The last five years or more..... ( )

SECTION C: BYOD BENEFITS

1. To what extent did each of the following drivers lead to the adoption of Bring Your Own Device (BYOD) for work-related tasks in your organization? (Tick the appropriate box)

Factors that led to the Adoption of BYOD	No extent	Small extent	Moderate Extent	Large Extent	Very Large Extent
Reduced total cost of IT infrastructure ownership					
Reduced capital expenditure on IT equipment					
Reduction of IT technical support costs					
Employee morale boost					
Demand for flexible working hours					
Improved employee productivity and efficiency					
Improved employee working mobility					
Project a professional image towards clients and other third parties					
End user demand					
Management pressure					
Other, please specify ….....					

2. To what extent has the organization realized each of the following benefits as a result of adopting Bring Your Own Device (BYOD) for work related tasks? (Tick the appropriate box)

Realized Benefits of Adopting BYOD	No extent	Small extent	Moderate Extent	Large Extent	Very Large Extent
Reduced total cost of IT infrastructure ownership					
Reduced capital expenditure					
Reduced IT technical support					
Improved employee morale					
Flexible working hours					
Improved employee productivity and efficiency					
Improved employee working mobility					
Improved professional image towards clients and other third parties					
Increase in sales and revenue					
Reduced operational costs					
Other, please specify ….....					

SECTION D: BYOD THREATS

To what extent has each of the following threats been experienced as a result of adopting Bring Your Own Device (BYOD) in the organization? (Tick the appropriate box)

BYOD Threats	No extent	Small extent	Moderate Extent	Large Extent	Very Large Extent
Theft of mobile device (device is stolen from the office, a car, robbery etc)					

Misplacing of mobile device (employee loses device accidentally)					
Virus infection (unwanted programs are installed either unknowingly or knowingly on the device)					
Spy-ware infection (virus designed to steal information)					
Identity theft (username/password are stolen and used to access system illegally)					
Device Rooting (mobile device is modified to allow the user gain super rights thus allowing him to modify any component of the device)					
Rogue Access Point (a fake wireless network is setup and mobile device users connect to it unknowingly and the attacker captures their transmissions)					
Unauthorized tethering (the mobile device is used to connect the organization's PC or laptop to internet thereby bypassing the organization's controlled internet)					
Unauthorized WI-FI access point (The mobile device is used to create a wireless network that can then be used to connect to the internet)					
System intrusion/attack (an attack of corporate systems using the mobile device)					
Data leakage to public online websites (confidential information is leaked to the internet)					
Financial fraud (the mobile device is used to steal money from the organization)					
Corporate espionage (the mobile device is used to steal trade secrets or corporate					

information and delivered to a competitor)					
Theft of company proprietary information (theft of information that gives the company a competitive edge)					
Other, specify and rate ….....					

SECTION E: BYOD COUNTER-MEASURES

To what extent has the organization implemented each of the following security counter-measures to address threats that have arisen through the adoption of Bring Your Own Device (BYOD)? (Tick the appropriate box)

Security Counter - Measures	No extent	Small extent	Moderate Extent	Large Extent	Very Large Extent
Firewalls					
User awareness, training and/or education					
Mobile Device security policy					
Intrusion detection/ Intrusion prevention system					
Signing of user agreements (terms of usage)					
Network access control					
Installation of security software such as anti-virus / anti-malware on the device					
Software Patching / Software updates					
Data leakage prevention system					

Data classification to control / monitor flow of information out of the organization					
Data watermarking to control / monitor flow of information out of the organization					
Minimum security baseline for mobile devices					
Mobile device encryption					
Mobile device management system					
Remote wiping of mobile device					
Remote tracking of mobile device					
Enterprise mobile application store					
Partitioning to separate corporate data from personal data on the mobile device					
Complete ban on mobile device usage					
Other, specify and rate ….....**.....**					

APPENDIX II:SELECTED NSE FIRMS

Below are the sixty one firms that are listed on the NSE that have been selected for data gathering in this study.

CATEGORY	FIRM
Agricultural	1. Williamson Tea Kenya
	2. Sasini ltd
	3. Eaagads ltd
	4. Kapchorua Tea Co.ltd
	5. Kakuzi
	6. Rea Vipingo Plantations ltd
	7. Limuru Tea Co. ltd
Commercial and Services	8. Express Ltd
	9. Kenya Airways Ltd
	10. Nation Media Group
	11. Standard Group Ltd
	12. TPS Eastern Africa (Serena) Ltd
	13. Scangroup Ltd
	14. Uchumi Supermarket Ltd
	15. Hutchings Biemer Ltd
	16. Longhorn Kenya Ltd
Telecommunication and Technology	17. Safaricom ltd
	18. Access Kenya Group ltd
Automobiles and accessories	19. Car and General (K) Ltd
	20. CMC Holdings Ltd
	21. Sameer Africa Ltd
	22. Marshalls (E.A.) Ltd
Banking	23. Barclays Bank ltd
	24. CFC Stanbic Holding ltd
	25. I&M Holdings ltd
	26. Diamond Trust Bank Kenya ltd
	27. Housing Finance Company ltd
	28. Kenya Commercial Bank ltd
	29. National Bank of Kenya ltd

	30.	NIC Bank ltd
	31.	Standard Chartered Bank ltd
	32.	Equity Bank ltd
	33.	The Cooperative Bank of Kenya
Insurance	34.	Jubilee Holdings
	35.	CFC Insurance
	36.	Pan Africa Insurance Holdings
	37.	Kenya Reinsurance Cooperation
	38.	British American Investments ltd
	39.	CIC Insurance Group ltd
Investment	40.	Olympia capital holdings
	41.	Centum Investments Co ltd
	42.	Trans-Century ltd
Manufactured and Allied	43.	East African Breweries
	44.	British American Tobacco Kenya
	45.	Eveready East Africa ltd
	46.	B.O.C Kenya ltd
	47.	Carbacid Investments ltd
	48.	Mumias Sugar Co
	49.	Unga Group ltd
	50.	Kenya Orchards ltd
	51.	A.Baumann co ltd
Construction and Allied	52.	Bamburi Cement ltd
	53.	E.A. Portland Cement ltd
	54.	Crown Berger ltd
	55.	Athi River Mining
	56.	E.A. Cables ltd
Energy and Petroleum	57.	KenolKobil ltd
	58.	Total Kenya ltd
	59.	KenGen ltd
	60.	Kenya Power and lighting
Growth Enterprise Market Segment	61.	Home Afrika Ltd