THE BRING YOUR OWN DEVICE PHENOMENA: BALANCING PRODUCTIVITY AND CORPORATE DATA SECURITY

BY

WILLIAM TURI KAMAU

REG NO. D61/67685/2011

A MANAGEMENT RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF MASTER OF BUSINESS ADMINISTRATION (MBA) DEGREE, SCHOOL OF BUSINESS, UNIVERSITY OF NAIROBI.

OCTOBER, 2013

DECLARATION

This is to certify that this research project is a product of my original research investigation and has not been presented for a degree award in any other university or institution of higher learning. Information from other sources has been acknowledged.

WILLIAM TURI

Reg No: D61/67685/2011 **Date……**

Sign…….

SUPERVISOR

This management project has been submitted for examination with my approval as the university supervisor.

Dr. MURANGA NJIHIA **Date……**

Sign……

ACKNOWLEDGEMENT

First is to thank the almighty God who has seen me through this post graduate journey and through whose grace I have managed to complete my studies on time. I would also wish to acknowledge the selfless assistance and guidance from my supervisor, Dr. Muranga Njihia. Indeed much credit goes to him especially in guiding me shape up this research study and for the endless hours and effort he put in assisting me. Many thanks also go out to my parents who have always encouraged and cheered me on and also for their financial assistance.

To you all, Thank you very much and may God bless you abundantly.

DEDICATION

To my dear parents, Thomas Kamau and Jane Wangui. I shall live the dream.

God Bless you

ABSTRACT

In a world where technology changes faster than organizations can cope with, it has become common practice for most employees to acquire the latest of these technologies and use them for work related activities. This has seen an influx of personally owned devices into the corporate offices and networks thus creating a host of security challenges on one hand and improving overall employee productivity on the other.

The main objective of this research study was to find out how organizations can strike a balance between BYOD productivity and corporate data security. The study primarily focused on the insurance industry in Kenya due to the high sensitive nature of data and information they handle. This study made use of exploratory case design. It also utilized primary data only which was collected through questionnaires and in-depth interviews. The respondents' were from two insurance firms, herein referred to as Company A and Company B.

From analysis of data collected, it has come out clearly that as much as the term BYOD seems all too new to most employees it is a practice that has been going on for quite a while. It is also very clear that management does understand the concept very well, and they are aware of BYOD impact on productivity. However, adoption of BYOD has not been embraced as much as in the western countries and industries. This is as a result of a host of challenges that come from own device usage key been security challenges. However this is set to change as organizations continue to realize the full potential of BYOD and especially its impact on employee productivity and as such they have started embracing it amid a lot of infrastructure upgrades and security solutions to ensure safe onboarding.

LIST OF ABBREVIATIONS

BYOD – Bring Your Own Device

CCK – Communications Commission of Kenya

CIO – Chief Information Officer

Cisco IBSG – Cisco Internet Business Solutions Group

IBM – International Business Machines

ICT – Information Communication Technology

IRA - Insurance Regulatory Authority

IT – Information Technology

ITU – International Telecommunication Union

MDM - Mobile Device Management

MIPs - medical insurance providers

PwC – Pricewaterhousecoopers

PC – Personal Computer

Wi-Fi – Wireless Fidelity Network

URL – Uniform Resource Locator

VM – Virtual Machines

VPNs – Virtual Private Networks

3G – Third Generation

TABLE OF CONTENTS

CHAPTER ONE: INTRODUCTION

1.1 Background

People today own or are using more than one computing device, it has become common practice for an employee to on top of the workstation provided for by the company to also own a smart phone, a tablet and a personal laptop; they also happen to use all this gadgets in a complimentary fashion (Trend Micro, 2012). Conventional desktops and laptops are being mainly used to produce information; tablets to consume and smart phones to communicate that information. BYOD (Bring your own device) is a term which refers to when employees use their personal computing devices (typically smart phones, tablets and laptops) in the workplace (Trend Micro, 2012). This new ICT phenomena is here to stay and the challenge is that it is a double edged sword pitting user satisfaction and productivity on one end and organizations data security on the other (Madden, 2013).

A research by Cisco (Weldon, 2012) on Bring Your Own Device (BYOD) showed that nearly half of all respondents prefer own devices over corporate ones and this BYOD-ers are willing to back up their mindsets with cash, spending on average $965 purchasing devices for work, and an additional $734 annually on mobile voice and data plans. Though the research was conducted within the US market, a survey of some Kenyan firms shows a similar trend with workers spending tens of thousands on BYOD (PwC, 2012).

BYOD cannot be ignored because most organizations have generation Y forming a bulk of its workforce, these are technology hungry and savvy personalities, willing to explore and try out new technologies as they come out. According to Red Hat's CIO Lee Congdon these young users have more control over IT than ever before (The CIO, 2013). Similarly technology is changing at a very fast rate. Kolb and Kolb (2013) note that a few years back it used to be that IT departments drove technology, but that has changed dramatically in recent years. With consumerization of IT revolution there has been a cultural shift such that the users are the ones getting the latest, cutting edge technologies first, and they want to bring those devices to work. This is something that most organizations would want to wish away while others are eager to embrace all for differing reasons.

BYOD without doubt brings with it increased productivity by allowing employees to use their own equipment for work. This is so because employees are familiar with their own device(s) and without any training can use them to maximum effect. This is a big win for both employers and workers. Another major benefit that BYOD brings is worker satisfaction. Users have the laptops and smartphones they have for a reason, those are the devices they prefer in contrary to being stuck with company procured devices which more often than not have less features, difficult to use, outdated and have to be used under strict company guidelines.

However, allowing workers to simply walk in with their own set of devices and connect to the corporate network in itself poses a hidden danger for corporations such as risks of data loss or spillage, introducing a host of security vulnerabilities such as a weak point of entry for hackers and other data protection concerns key been what happens when that gadget is lost while still holding critical corporate data (Current Analysis, 2012). This is compounded by client end applications fondly referred to as "consumer apps" such as Google Apps, Box, Dropbox, Evernote and social media sites that workers find so easy and convenient to work with especially on their personally owned gadgets (Forrester, 2012). The use of consumer apps, social networks and other mobile apps may result in either intentional or accidental file sharing loops holes for malicious software getting into the corporate network, and possibilities of industrial espionage (Kerravala, 2012).

1.2 BYOD and Knowledge workers

Though BYOD cuts across different organizations and sectors of the economy, this study aims to focus on organizations or sector(s) of the economy where the concept has taken off at jet speed. These are organizations where the bulk of the workforce is composed of Tech savvy generation Y and where most employees are knowledge workers. Knowledge workers are employees whose main asset is knowledge; they tend to perform non-routine problem solving that requires a combination of convergent, divergent, and creative thinking (Reinhardt et al., 2011). According to Mcdermott (2005), Knowledge workers spend 38% of their time searching for information and are often very mobile and prefer working from anywhere. It is for this and other reasons that this

special group of users prefer to use their own gadgets due to convenience, ease of use, highly innovative devices among other reasons.

According to management guru, Peter Drucker who coined the term “knowledge worker” (Drucker, 1966), he insists that new industries will employ mostly knowledge workers and as such emphasize on the need to expand the role of knowledge in an information-based economy. Drucker insists that the most valuable asset of a 21st-century institution, whether business or non-business, will be its knowledge workers and their productivity. He says "making knowledge workers productive requires changes in attitude, not only on the part of the individual knowledge worker, but on the part of the whole organization” and as such BYOD with its proven impact on productivity will have to be adopted.

1.3 Insurance Industry in Kenya and BYOD

Many users are now acquiring these devices in the backdrop of an intense demand that has mostly been driven by mobile operators in Kenya in a bid to increase data uptake in their 3G networks. Safaricom for instance with about 1.9 million subscribers on the 3G platform is already partnering with smart phone makers and has already rolled out a plan to abandon feature phones in favour of affordable smartphones. This has seen it partner with Electronic giants like Samsung and Intel in a move that has seen it sell smartphones at prices 20cert lower than the market average.

This among other efforts from the Telco’s and even the industry regulator, the Communication Commission of Kenya has seen internet usage in Kenya surge to over 17 million users. Safaricom and Orange also have embarked on multibillion fiber rollout projects that will see them rollout fiber networks across the major towns in the country. This is informed by the fact that data is the next frontier to rake in billions in revenues. This coupled with the intentions of some players to role out an even faster 4G network will see the demand for smart data enabled gadgets continue to soar.

A report by the Communications Commission of Kenya (CCK) stamps this in a report that shows the dominance of the smartphone and other mobile devices over traditional PCs in connecting to

the Internet is likely to increase with operators collaborating with phone manufacturers to roll out low-cost devices in in East Africa.

This study aims to look at Kenya firms domineered by Tech savvy generation Y and where most employees are knowledge workers. This is so because studies have shown that these special groups of employees (Reinhardt et al., 2011) are the first ones to adopt and embrace BYOD. Still within this group the study will specifically look at Kenyan Insurance firms where client and most business data are held within user devices.

The insurance industry is governed by the Insurance Act and regulated by the Insurance Regulatory Authority (IRA). As at 2013, there are 45 licensed insurance service providers (IRA, 2013). Of the licensed insurance companies, 20 were general insurers, 7 long term insurers and 15 were composite (both life and general) insurers. In addition, there are 201 licensed brokers, 21 medical insurance providers (MIPS), 2,665 insurance agents, 23 loss adjusters, 1 claims settling agent, 8 risk managers, 213 loss assessors/investigators and 8 risk managers (PWC, 2007).

1.4 Statement of the Problem

According to Forrester Research more than half of information workers own the devices they use for work, this came out in a survey of almost 10 000 people in 17 countries, and that proportion is likely to increase Forrester (2012). Research in BYOD and mobile computing (Nicol, 2013) shows that technology changes today faster than organizations IT departments can keep up with it, allowing the user to choose their device benefits the Organizations by putting the newest devices in employees' hands much more quickly. This however does pose serious challenge for the organizations especially with regard to data security, ability to demarcate between the use of these devices for personal and business use, cost implications, dealing with challenges of device and data theft. Most authors like Sheninger (2011) and Lee (2012) however agree that BYOD is not something an organization can wish away and as such coming up with policies to regulate onboarding and usage of personal devices at the work place is the way to go (Kerravala, 2012).

Locally this concept is still very new and most users and organizations still aren't aware of the potentials and risks associated with own devices. PwC (2012) highlights most of the benefits and challenges of BYOD, in this article it notes that most organizations are experiencing bandwidth and productivity drains. This is because many employees have found that mobile devices often do not have the same strict policy enforcement capabilities as desktop devices. This policy gap enables many employees to use their mobile devices to access video streaming and other applications that are denied by standard corporate policy. With mobile devices offering a way to bypass the limits normally imposed on these applications and behaviors, users are putting a strain on the corporate network bandwidth and being less productive.

It is this gap that informs this research study and the researcher aims to address. It includes how own devices can safely be brought onboard and how this will impact the organizations productivity. The study aims to answer the questions: What is the relationship between organizational Productivity and BYOD? and What challenges BYOD pose and how we can overcome them?

1.5 Research objectives

Specific research objectives:

1. To establish BYOD usage patterns and the security challenges posed to the organization
2. To explore the relationship between BYOD and organizational productivity in Kenyan insurance firms.
3. To determine how and to what extent the organization and its workers can benefit from BYOD
4. To find out how Kenya insurance firms are dealing with BYOD

1.6 Value of the Study

This research study aims to benefit organizations domineered by knowledge workers and where information/data is the key asset. Organizations under this category include financial institutions, insurance firms, brokerage firms, Telco's among others. This study will show the working of a knowledge worker, their preferences and the kind of technological working environment they prefer. Likewise, employees are at the center of this BYOD study and this document aims to clearly show just how they stand to benefit even more, how their privacy can be assured, how costs can be shared as well as train them on the potential ways they are likely to expose their organizations to security risks and how this can be mitigated.

Solution providers also stand to benefit from this study as it unearths immense opportunities where they can lake in millions of dollars by providing secure platforms that would seamlessly yet securely integrate the personal devices to the organization ICT infrastructure. This could be fronted in terms of applications, storage solutions, unified communication or data security solutions. The study will explore the available solutions to BYOD challenges, expose their shortcomings and highlight possible areas of improvement. According to a research done by Cisco Corporation, BYOD presents a multi-billion dollar frontier for solution providers especially secure platform providers.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

This chapter looks at the BYOD concept in more details giving a brief history into its origin and how it has become a phenomena. It also looks at other research work on BYOD with a keen focus on productivity and security. Finally the chapter shows the relationship between BYOD usage and employee/organizational productivity with security policies moderating the two.

2.2 BYOD as a concept

In recent years, there has been an explosion of technology that has led to the "consumerization of IT" (CIO, 2011). Devices and services historically available only in the workplace and provided by IT departments are now widely available to and affordable by consumers. The introduction of devices such as the Apple iPhone and iPad, Google Android smartphones and tablets, and lower cost laptops has increased consumers' appetite for the latest technology, and they crave that same technology at the workplace (Slottow, 2012). IT departments typically lag behind the technology curve due to the effort to test new technologies, cost of procurement, and the depreciation of assets which leads to staff members taking it upon themselves to bring in their own equipment. This has resulted in the Bring Your Own Device (BYOD) trend seen across most industries today (PWC, 2012).

Though smart phones have actually been around in one form or another since 1993, the year 2007 remains the revolutionary year when Apple brought the smartphone to a mass consumer market (Weldon, 2012). Initially early smartphones were primarily used as enterprise devices and were prohibitively expensive for most consumers; these devices were also used by mobile workers principally for voice, SMS, and email, and were locked down in terms of what corporate data they could access (Weldon, 2012). However, this is not the case anymore as these devices are now considered more business centric and are being used for a lot of corporate business processing. This has led to the development of corporate mobile applications giving workers ability to access corporate databases and do real-time queries making business processes highly

productive by eliminating paper-based, manual, or on-site requirements for dispatch, inventory management, field sales, and technical support, attend real-time company videoconferences etc.

With the influx of data enabled devices top been smart phones, Macintosh iPhones and iPad (tablet computer), IBM's Palm tops (a battery-powered microcomputer small enough to fit in the palm) and portable laptops. Advances in technology have seen the development of Smart phones with storage and processing capabilities that could rival any decent PC out there, this phones have 3G (3G is an ITU specification for the third generation analog cellular was the first generation, digital PCS the second) of mobile communications technology. 3G promises increased bandwidth, up to 384 Kbps when a device is stationary or moving at pedestrian speed, 128 Kbps in a car, and 2 Mbps in fixed applications (GMSARENA, 2012) and wi-fi (wireless network) capabilities, meaning that you can connect them to the corporate network when within range and still continue to access internet and other services at high speeds away from work.

According to a research paper by PWC (2012) Users' demands that they be allowed to use technologies of their own choosing isn't a fad that will fade. CIOs can't squelch these demands—nor should they. The consumerization of IT is a symptom of a shift in workplace expectations that has been brewing for years and is now reaching an inflection point.

2.3 BYOD and Productivity

Cisco through its Internet Business Solutions Group (Cisco IBSG) recently conducted a research on the financial impact of BYOD to companies (Loucks et al., 2013). The findings show that, on average, BYOD is saving companies money and helping their employees become more productive. But the value companies currently derive from BYOD is dwarfed by the gains that would be possible if they were to implement BYOD more strategically. According to cisco IBSG the true value BYOD largely depends on the model an organization decides to use (Loucks et al., 2013). In the study, Cisco identifies two scenarios of BYOD usage:

- "Basic BYOD" is the way BYOD is typically implemented in companies today, with an incomplete patchwork of capabilities and policies. This scenario could also be viewed as the median level of BYOD capabilities across companies.

- "Comprehensive BYOD" refers to a more strategic approach to BYOD, and features eight core capabilities companies need to harness BYOD effectively.

Using this approach Cisco was able to look at the full BYOD journey, and to examine the benefits at each stage: from no BYOD at all, to Basic BYOD, and then to Comprehensive BYOD. Cisco goes further to use the survey findings and internal data to estimate the productivity impact of these different transitions across seven categories — availability, collaboration, efficiency, new ways of working, avoided distractions, reduced downtime, and reduced administration , as well as the potential cost savings in hardware and telecommunications.

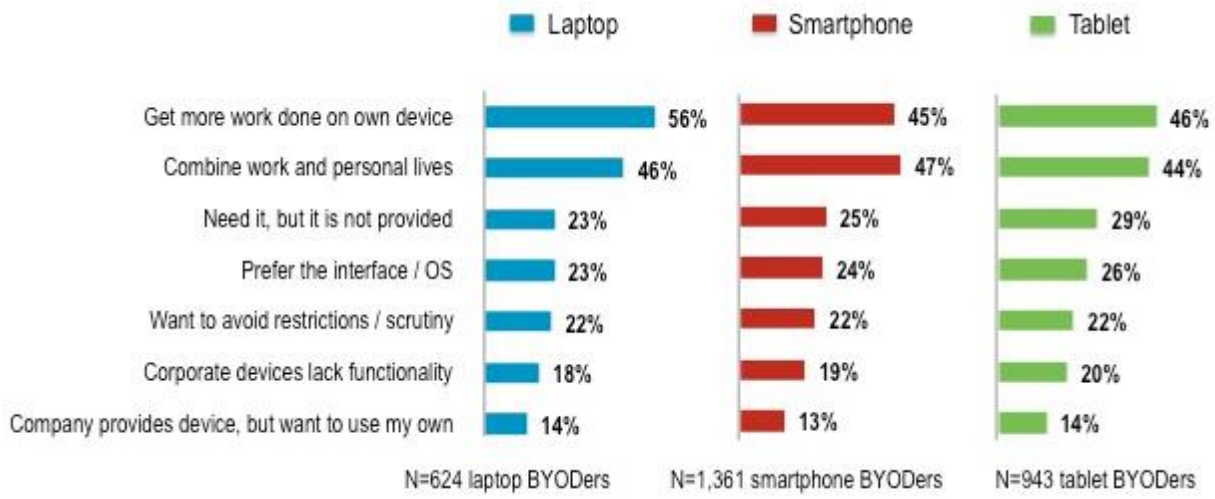
Cisco discovered that companies in all countries surveyed had been reactive in developing their BYOD capabilities and policies, yielding to demands for a wider variety of devices and applications rather than executing a vision for greater flexibility and cost savings. Some have been more successful than others in garnering value from this patchwork of capabilities (Basic BYOD). For companies in all countries Surveyed, however, the lion's share of the value of BYOD comes from a more strategic approach to the way they provision devices, provide IT support, and develop mobile policies (Comprehensive BYOD). With Comprehensive BYOD, companies that are already successful in reducing costs and increasing employee productivity will see their gains increase substantially. Those that have struggled to generate significant value can use Comprehensive BYOD to approach, and even surpass, the gains made by firms in the most successful countries to date.

Further insights derived from the study showed that, even with basic BYOD, companies around the globe are making productivity gains and making employees more productive. The average BYOD user across countries saves 37 minutes per week thanks to using his or her own device, with a high of 81 minutes per week in the United States and a low of 4 minutes per week in Germany. On average, Basic BYOD generates $350 of value annually per mobile user (including both BYOD and corporate device users). Further, companies can gain an additional $1,300 annually per mobile user with Comprehensive BYOD and that goes to show just why an organization should be strategic rather than reactive with BYOD.

The study (Cisco IBSG, 2013) goes further to show just how BYOD impacts on productivity. In a question posed to respondents, it emerged that BYOD-ers accomplish more by using their own

devices (see Figure 2). This was the top reason by far that BYOD-ers use their own laptops for work, and likely accounts for the surprisingly high rate of BYOD laptops. The study noted that the laptop is the main work productivity device for most mobile users, at least when they are working from a desk or fixed location. (Loucks et al., 2013) note that "BYO-laptop" should be an important strategy for companies looking to expand the benefits of BYOD. It is important to note that productivity improvements come from the device and the software, mobile apps, and cloud services used on these devices. BYOD-ers highly value the ability to use the applications and services of their choice, rather than being limited to what their companies offer.

Figure 3. Top Reasons BYOD-ers Use Their Own Devices for Work



Source: Cisco IBSG 2013

The study further shows that these employees are taking the initiative to increase their productivity — and spending their own money to do so. BYOD users spend an average of $965 (U.S. dollars) purchasing their own devices for work. They spend an additional $734 per year on mobile voice and data plans for their BYOD devices. The cost of these plans varies widely across countries, from more than $1,200 in the United States to under $400 in India.

A significant share of BYOD users — 36 percent overall — were found to be "hyperproductive," saving at least two hours per week by using their own devices for work. Twenty-one percent save at least four hours per week and these highly productive employees were found in every country in the study (Loucks et al., 2013). Another significant productivity findings was that employees using their own mobile devices, software, apps, and cloud services did end up finding

new ways of working and an astounding 53 percent of these BYOD workers have increased their productivity through employee-led innovation.

In yet another Study the strategic importance of BYOD is emphasized and the authors insist more on strategy and planning for BYOD (Dimensional Research, 2011).
Apart from Productivity there were other reasons as to why BYOD use is growing in organizations. Convenience was cited as another common reason why most workers prefer their own personal devices at work. Convenience comes in the ability of the users to work from home, after hours and from anywhere, leading to increased productivity. Research has shown that about 93% of staff who use personally-owned devices for work performs work outside of their normal working hours. According to an iPass survey (2012) of 1,100 mobile workers, employees who use mobile devices for both work and personal issues put in 240 more hours per year than those who don't.

It is also important to note that these devices form or are a significant part of employees' lives. Many authors point out to this fact (Sheninger, 2011) (Lee, 2012) (Sweeney, 2012) (Walling, 2012). Some of these authors argue that as these devices are integral to the world in which these employees live they should be integral to their working lives. The authors tend to agree that instead of restricting use, the company should teach the employees on how to use them properly. Employee satisfaction increases due to ability to choose their own device, they enjoy using it more and are more likely to spend time exploring it and understanding it and are less likely to require technical support iPass survey (2012).

The organizations also stand to benefit due to financial pressures. Most companies embrace it as a cost saving programs as it shifts costs to the user, with employees paying for mobile devices and data services and also incurring insurance risks/costs (CIO, 2012). BYOD also means fewer headaches to the company in that due to device familiarity most users can and will be able to maintain and even upgrade the devices they use. This leaves ICT department with more time to focus on more strategic initiatives, rather than spending majority of their time dealing with helpdesk tickets.

2.4 BYOD and Corporate Data Security

Security does remain the biggest BYOD Challenge (Cisco IBSG, 2013) and it brings yet another battle in the war between security and usability. Employees want the ability to use personal devices for work purposes, their belief being that personal devices are more powerful, flexible, and usable than those offered by corporate. Organizations also look to capitalize on this trend by shifting maintenance costs to the employee, eliminating the standard-setting role of IT. Workers have discovered the power of constant connectivity and have come to expect secure access to their corporate network regardless of location. The promises of increased productivity and worker satisfaction have brought BYOD to the forefront of most IT discussions today.

Mixing personal and business applications and data has the potential to introduce malware such as viruses that can infect devices and potentially lead to the compromise of corporate data (Current Analysis, 2012). More mundanely (and much more commonly), devices with corporate data on them may be lost or stolen. These facts make it difficult to comply with corporate security requirements without the use of extra management and security protections. Enterprises can deploy mechanisms such as device lock, device wipe, application blacklisting, centralized configuration and inventory management, software updating and troubleshooting, and private enterprise app stores, as well as mobile VPNs, url and content filtering, device/transport encryption, and anti-malware solutions (Weldon, 2012).

The security concern is centered around the security of data, since that is the institutional asset at risk. Other security concerns revolve around; inadequate security safeguards implemented on personally-owned devices, employees retaining sensitive institutional data on personally-owned devices after they have changed roles or left the company, lost, stolen, misused, or hacked devices not reported as a security incident. A report from Trendmicro (2012) shows that 93% of personal tablets connecting to corporate data have no security software installed; the report also notes that 84% of smart phones connecting to corporate data do not have any form of security installed on them.

2.5 Managing BYOD in Organizations

BYOD does raise other concerns including cost and though seen as a potential cost costing venture for most businesses, there are financial risks that should be considered when implementing a BYOD program. These include an increase in infrastructure, support, and security costs. Privacy is also a major and valid concern especially for employees. More often than not the company would require for purposes' of ensuring security to their data require that they have access and control to the employees' device. This same devices they are using for company work are the very same they use for personal things, as such employees are wary about organizations being able to "spy" on them and have access to their personal passwords, websites, and information. This may also happen in the form of a discovery request in the context of a litigation involving the company and where the employees may be asked to surrender their personal devices.

There is also the question of what happens when the employee leaves employment. What happens to the company data held in their gadgets? There is a genuine concern about retrieving all company data and information if the employee were to quit or get fired. One commonality among organizations is educating employees and having them sign official BYOD policy forms outlining what employees can and can't do on their own devices. It is common sense that the company will want its data and as such there should be a policy in place that governs how that data will be retrieved from the personal laptop and/or smartphone.

Defining the boundary between personal and official work on BYOD devices also remains a challenge. The use of personal devices for work purposes may blur the line between work and personal activity. This does raise concerns for organizations willing to embrace BYOD. Organizations struggle with implementing the right balance of technologies and policies to ensure that BYOD is both secure and effective and that these devices aren't being used to push or do personal work to the detriment or at the cost of organization. Mobile workers also experience some unique threats and risks including the risk of malware infection, inadvertent or malicious sharing of critical business data or even the devices being lost or stolen. Additionally, the users may decide to use their personal devices at public places with rogue wireless networks

which are prone to stealing of unprotected data. The use of the devices in places such as cyber cafes also puts the devices at risk of malware infection.

According to a report done by PwC (2012) the organizations are also experiencing Bandwidth and Productivity Drains. This is because many employees have found that mobile devices often do not have the same strict policy enforcement capabilities as desktop devices. This policy gap enables many employees to use their mobile devices to access video streaming and other applications that are denied by standard corporate policy. With mobile devices offering a way to bypass the limits normally imposed on these applications and behaviors, users are putting a strain on the corporate network bandwidth and being less productive.

In order to address the balance between usability and security, organizations are taking a variety of steps. Some choose extreme approaches such as denying all personal devices on the corporate network which may be warranted for extremely secure organizations, while a majority of the organizations want to adopt a BYOD policy that offers some flexibility for users while enforcing corporate policies and adopting best practices. It is however important to note that these listed measures are solutions from various vendors and not academic research. This is because, BYOD still is and remains a new concept and hasn't been widely written about.

Explicit Policies on BYOD usage must be put in place as this is the first line of defense. According to Fortinet (Enabling secure BYOD), organizations must first address the BYOD challenges through explicit policies. This starts by first deciding the extent of any BYOD program i.e. scoping. Some organizations will still choose to limit access to certain data or applications. Others may choose to require employees to have specific software installed on their device in order to use a personal device on the network. The organization determines what devices they will allow on the network and generates policies stating appropriate devices and acceptable behaviors. (Fortinet is a USA company manufacturing firewalls and other security applicances)

Creating the corporate policy is a necessary first step for creating a secure mobile environment but ultimately organizations need technical solutions in place to enforce policy. Technical

controls can vary from network-based to device-based and no single solution is appropriate for all organizations. Some of the most common technical controls associated with enforcing BYOD policies are discussed here. (Source, Cisco)

The organization may also choose to use "Containerization" or dual-persona devices. Containerization refers to the ability to setup an encrypted storage space on a mobile device and manage access to that space. The technology offers a seamless and intuitive dual-persona platform for situations where a single mobile device is used for both work and play. As it allows IT to do what they want on the business side while leaving the personal side alone so that the employee can have free reign. This works by separation a corporate-managed container and its associated apps and settings, and the unmanaged personal space, such that a user is effectively using two different platforms or environments on a single device. (Source, VMware)

Mobile Device Management (MDM) is another approach and refers to a software platform that secures monitors, manages and supports mobile devices deployed across an enterprise. Its functionality includes over-the-air distribution of applications, data and configuration settings for all types of mobile devices, including mobile phones, smartphones, tablet computers and other device utilizing wireless technology. This applies to both company-owned and employee-owned devices across the enterprise or mobile devices owned by consumers. (Source, Apple)

The organization could also implement secure mobile VPNs. A virtual private network (VPN) is a network designed to secure remote network access. It extends the reach of LANs by using a public telecommunication infrastructure, such as the Internet, and does not require any owned or leased private lines. Companies use VPNs to provide telecommuting employees and branch offices with secure access to the corporate network and applications on internal servers. (Source, Cisco)

Cloud computing and storage technology is also offering solutions to these challenges. The popularity of Dropbox simply highlights the rising demand for a simple, accessible, user-friendly storage and collaboration product that enterprises and their users should embrace. The cloud offers the most cost-effective and least resource intensive way to secure data in the era of BYOD and "work anywhere" computing. We are moving to a scenario where corporate data and

applications no longer need to be stored on the device but instead can be hosted on the cloud and employees can access it from virtually anywhere as long as they have internet access. (Source, VMWare, EMC)

In the case of theft or loss of a user device an organization could choose to enforce device lock and remote wipe. This can be done through a security policy enforced by the corporate email account that trigger your iPad or smart phone to self-destruct in order to prevent sensitive corporate data from unauthorized access. However it is to be noted that it typically involves remotely wiping all content from the device, but an employee's personal tablet or smartphone also has photos, videos, contact information, calendar events, and other information that will be permanently erased as well.

Network-based enforcement is yet another approach to address BYOD and relies on the network to enforce policies and controls around what the client, data, and user can do or access. Network based enforcement requires a great deal of granularity and intelligence on the network to provide adequate access controls to prevent nefarious activity. A key advantage of network-based enforcement is the location of the targeted data ultimately resides on the network. Establishing controls on the network itself allows an organization to block malicious software or activities coming from mobile devices before any damage can occur to the network. (Source, Cisco)

2.6 Literature Review Summary: Balancing BYOD Productivity and Security

The literature review has clearly shown just how beneficial and productive BYOD can be; increasing the productivity value of an employee to about $ 1,3000 (Approximately Kshs. 117,000) per annum/employee. This would mean millions of shillings of productivity value to organizations with tens of employees. However, it is to be noted that this would require a comprehensive BYOD approach that incorporates all the necessary security policies. This has been captured by the conceptual framework below and how the various variables (BYOD usage, productivity and security) shall form the basis of this study.

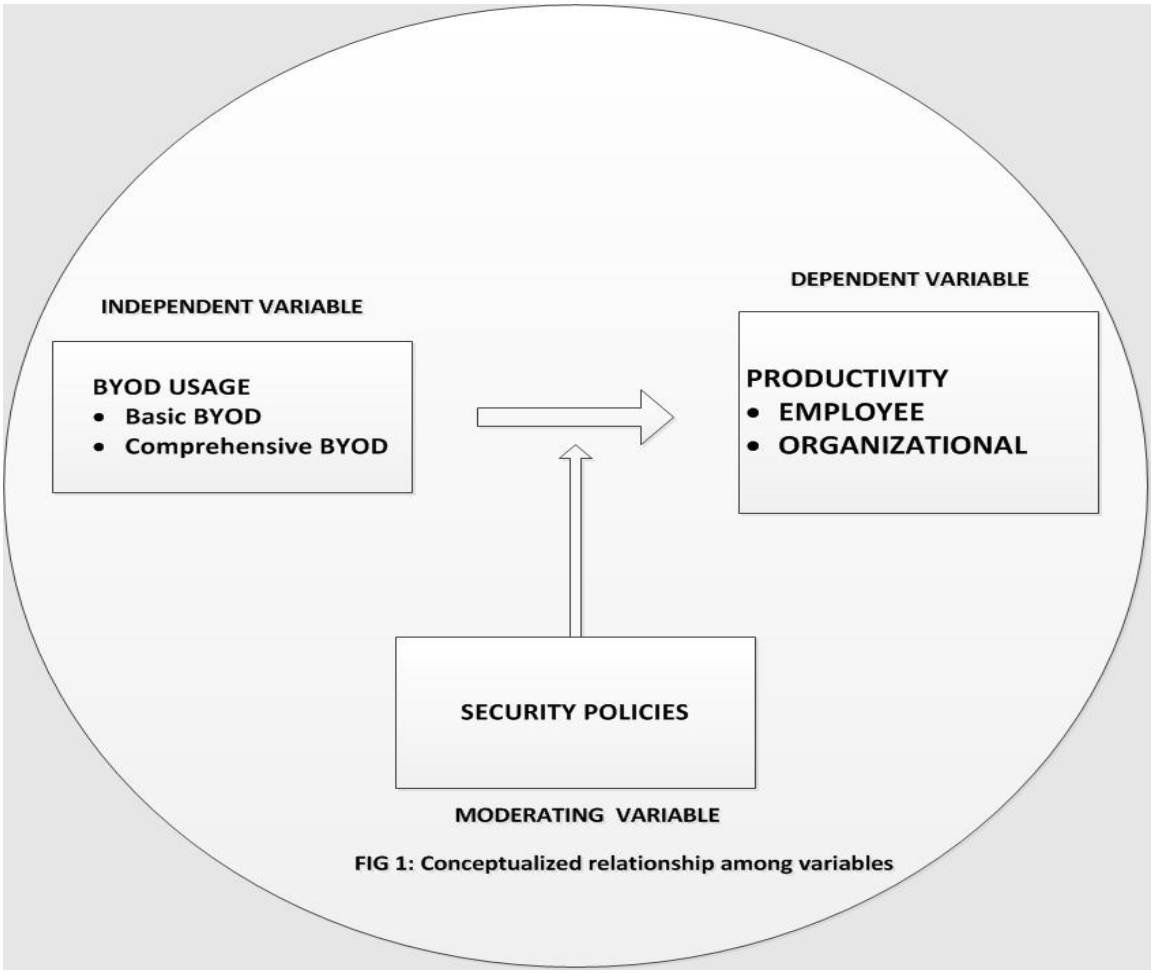


FIG 1: Conceptualized relationship among variables

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

This chapter describes the exact steps that will be undertaken to address your hypotheses or research questions (Rugg and Petre, 2007). Gordon and Marian (2007) state that this chapter outlines the procedure that the researcher will use to collect and analyze data. They further highlight that the following areas are key to a research study but this may vary depending on the nature of research; research design, target population, data collection and data analysis.

3.2 Research Design

This is defined as the strategy, the plan and the structure of conducting a research project (Carriger, 2000). This study intends to use an exploratory case study research design and the reasoning is because the BYOD concept is not as clearly defined, understood or explored within the Kenyan context. Babbie and Earl (2007) stipulate that the main goal of an exploratory research design is to provide insights into, and an understanding of, the problem confronting the researcher.

The researcher aims to conduct a case study on two insurance firms herein referred to as Company A and Company B respectfully. These two firms form a good representative of the insurance firms in the country. Company A on one hand offers domestic package insurance, car insurance, personal accident schemes and even sportsman insurance. At the corporate scene it insures for fire, burglary, marine, workmen's compensation, public liability, group personal accident, plate glass, money, motor and fidelity guarantee. Company B on the other hand deals with general Insurance, a category having property, liability, and people (workers compensation). It also has life insurance and retirement benefits administration that has products in both group and individual categories.

The selection of the two insurance companies for this study is informed by the fact that they are the extreme opposite of each other in terms of years of operations, size, profitability and workforce. This ensures that the study will cut across the big and already established players in

the insurance industry and also the small/mid-sized and emerging players. Company B for can trace its "roots" back to the early beginning of the 20th century when its parent company established an agency representation in Kenya in 1915. The firm has evolved into one of the most financially sound composite insurance companies in Kenya with assets in excess of Ksh.2 billion and a paid up capital Ksh. 450 million. On the other hand Company A began its operations in early nineties, with a paid up capital of KShs.20 million and a staff of nine. The firm has experienced rapid growth and now boasts of capital of about 2 billion and a staff base of about 60 employees.

3.3 Data Collection

The study will use primary data. Primary data by use of questionnaires and interviews is critical to this study as it will help the researcher get more reliable, authentic and objective data (Kumar, 2010). The researcher aims to have a one on one interview with the employees of the insurance firms and possibly secure interviews with the management. Questionnaires are meant for those employees who may for one reason or another be unavailable for an interview.

The questionnaires shall be in the form of an interview guide with open ended questions depending on the particular issue an answer is been sought. Secondary data will be collected in the form of reviewing policies and any other documentation in these firms with regard to BYOD and ICT usage. It shall be designed in a manner to cover the research objectives of BYOD usage, productivity and challenges.

3.4 Data Analysis

The process of data analysis will involve various stages. The nature of the data will be both qualitative and quantitative .completed questionnaires will be edited for completeness and consistency. The data will be coded and checked for any errors and omissions. Responses from the questionnaires will be tabulated and coded. Qualititative data will also be analyzed through content analysis. According to Mugenda and Mugenda (1999), content analysis is used to

determine the presence of certain words or concepts within texts or sets of tests. Researchers quantify and analyze the presence-meanings and relationships of such words and concepts, then make inferences about the messages within the texts, the writers(s), the audience, and even the culture and time of these are a part.

This study focuses on the relationship between respondents' use of own devices (the independent variable) and their level of productivity (dependent variable) and as influenced by the security policies (moderating variable). The researcher will explore answers from the questionnaires based on these research issues and show just how the factors interplay as per the below conceptual framework.

CHAPTER FOUR: DATA ANALYSIS, FINDINGS AND DISCUSSIONS

4.1 Research Conduct

Much of the data was collected through in-depth interviews held at each company. In-depth interviews were held at each of the company, one with the ICT Manager and the other with the Human Resources department making a total of 4 in-depth interviews. The interviewer took detailed notes during these interviews and this data has extensively been used to analyze this study. Data was also collected from the administered fifteen (15) questionnaires to randomly selected respondents at both companies, of the 15 questionnaire respondents, 11 responded thus representing a response rate of 73 percent.

The researcher has heavily employed qualitative techniques to analyze the data collected but has also used quantitative methods to offer simple explanations to the study findings. Two techniques have been extensively used to analyze the data collected from this study, these are; descriptive statistics and content analysis.

4.2 Case Descriptions

This chapter looks at a brief history of the two firms under this study, the nature of their business, their size in terms of staff numbers, revenue and assets. The main objective is to clearly bring out the opposite extreme of these two firms so that the study is a representative of the happenings across the insurance industry irrespective of a firms size, business portfolio, asset base, employee numbers, growth and years in operation. The essence of this is to show that BYOD as a concept cuts across and its benefits and challenges are felt across in the same manner.

COMPANY A

Founded in the early nineties the company has grown immensely and is one of the few insurance firms currently making a positive net profit. With a humble beginning of just a few million

shillings, the company has seen its asset base grow close to 1.5 billion and its staff base has also swollen from an initial less than 10 to near 100 employees in 2013.

The company is experiencing a fast growth rate but still is categorized as a medium size player. With regard to its product offering, it has a package at the personal level that encompass domestic package insurance, car insurance, personal accident schemes and even sportsman insurance. At the corporate scene Company A insures for fire, burglary, marine, workmen's compensation, public liability, group personal accident, plate glass, money, motor and fidelity guarantee.

COMPANY B

Company B on the other hand has a deep history that dates back to the early nineteen hundred. It is a big player in the insurance industry locally with branches in most of the counties major towns. The company has evolved into one of the most financially sound composite insurance companies in Kenya with an asset base in excess of Ksh.2 billion and a paid up capital of over five hundred million Kenyan Shillings. As a composite insurance company, Company B deals in both general Insurance and life assurance business with such packages as property, liability, and people (workers compensation) insurance, life insurance and retirement benefits administration that has products in both group and individual categories.

4.3 Thematic Content Analysis

This section presents an analysis of the data collected for the two companies in line with the objectives of this study.

4.3.1 COMPANY A

BYOD Usage Patterns

This section seeks to establish whether BYOD is been used at the company and if yes what model it takes and to what extent it's been used.

Company A ICT Manager describes BYOD encroachment as inevitable; he adds that whether you allow or deny employees, these devices one way or another will find their way into the company premises. He further states that, it would be more prudent to sit down with the employees and agree on what is and what is not allowed rather than applying a blanket rule which could prove more of a nightmare. The ICT manager speaks of how hard initially it were to control the influx but overtime they have crafted an "un-written" rules with regard to personally owned devices. "In my company for instance, we don't allow employees to just walk in with their laptops due to the sensitive nature of the data we handle", says the Manager. Unless a user is explicitly allowed to bring in a laptop and in which case it has to undergo thorough screening before it's allowed on the corporate network.

The manager however says that they allow employees to come in with their smart phones, iPads and tablets and they equally restrict the kind of data and resources that can be accessed by these devices. He is quick to add that, management staff are provided with company laptops and they are the only group allowed to take them outside the premises thou they have signed some form of non-disclosure, usage and ethics agreement.

Results from the respondents clearly show BYOD utilization in terms of devices. From the 5 point scale used, the table below gives the results.

Table 4.1 BYOD usage Patterns

Laptops	45%
Smart Phones	90.9%
iPads	45%
Tablets	27%
Others	0%

In conclusion it is evident from the usage pattern table above, smart phones are the most heavily utilized personal devices within the Company A followed closely by iPads and laptops. It is

however to be noted that the low laptop usage level is as a result of restrictions something not so pronounced within the other devices.

BYOD Security Challenges

This section explores the security challenges company A is facing in respect to BYOD, it looks at the host of challenges as well as what the company is doing to address these challenges.

Security remains the biggest challenge to BYOD adoption, this is so because, there's no one full proof to the risks posed by BYOD or any other ICT threat. "Trust remains key to BYOD" , this is not any further from the truth as noted from Company A's ICT Manager, he says that Trust is the key thing irrespective of how many control measures and policies you put in place. He emphasizes that, security should be owned up by everyone; employees and the organization alike. To this end, the company does from time to time hold ICT security awareness meetings and seminars to educate their employees.

According to Company A's ICT Manager, Threat of data loss is their major concern more than Viruses, malware and even hacking. He notes that, data loss either to competitors or to the general public could have crippling effects to the insurance firms ranging from commercial espionage and loss of clients to law suits emanating from accidental exposure of confidential client data. Below is a table highlighting the most common security challenges the company faces according to the manager.

Table 4.2 BYOD Security challenges

Threat of data loss	100%
Viruses	30%
Malware	30%
Hacking	20%
Others	50%

In conclusion, it is clearly evident that data loss stands out as the biggest threat emanating from BYOD usage. This is closely followed by malware and viruses, a threat the organization says is

easier to contain due to strong antivirus and anti-malware applications. Hacking does also stand as a highly potential security threat and this the company says is amplified by own device usage which present a lot of security loop holes that could easily be manipulated to launch an attack on the organization.

BYOD and Productivity in Company A

This section looks at the impact if any of BYOD on employee and organizational productivity. If there is an impact then, it sets to establish whether negative or positive.

Without doubt we know and have seen increased levels of performance and productivity with regard to BYOD, "I personally work better and am more efficient using my laptop and smart phone compared to the company's PC and analog phone" says Company A's Human Resource officer. We have field officers and even some of our staff would be happy to carry some of their work to home when working from the office becomes hard, she adds.

The respondents note that been more productive is their greatest motivation to BYOD usage. They cite that even the other motivations behind using BYOD such as increased convenience and enhanced collaboration all add up to increased productivity.

The HR and ICT departments are however worried that despite all these positives they might end up losing company hours when the users decide to engage and do their personal stuff on these devices. The Company's management cites social media and Chat applications as the greatest productivity headache they have to deal with. They have however put in some controls that block most of the social networks during working hours and only allow access before 8, during lunch break and after 5pm. The management however still has to deal with the headache of Chat applications such as Whatsapp which is hard to control as it's not a network run application.

In conclusion it is clear that indeed BYOD does have both a positive and negative impact to employee and in extension organization productivity. The positives however outweigh the negative impact and as the management put it is possible to control the negative impact.

Benefits of BYOD to employees and Company A

This section seeks to establish other motivations behind BYOD usage by the employees.

Asked on how they benefit from using their own devices, the respondents gave a whole list of how they gain from using their devices compared to company availed ones. The table below is an indicator of the many various ways the users benefit from BYOD.

Table 4.3 BYOD Benefits

Increased Productivity	100%
Highly Convenient	100%
Increased Collaboration	70%
Increased Flexibility	70%
Ease of use	90%
Keep pace with changing technology	60%
More innovative	45%

In conclusion it is apparent that productivity and convenience stand out as the greatest motivation for BYOD usage followed closely by increased levels of collaboration and flexibility. Employees did also cite ease of use at nighty percent as another great motivation; this as they put it was because they are familiar with their own devices and as such required no training on them as they have already mastered how to maneuver them.

BYOD Onboarding

Onboarding means allowing users to bring on their own devices and having mechanisms in place to facilitate access to the corporate systems and infrastructure. This section seeks to establish whether the company does facilitate onboarding and if yes how.

Completely denying our employees from embracing BYOD will not take away the problem and it's a high time we dealt with it albeit bit by bit, notes Company A ICT Manager. He adds that

the secret lies in regulating access, educating the users and coming up with clear rules and policies that are well understood and embraced by everyone. To this end, the company is pushing for a phased approach to BYOD, and have begun the journey by allowing some users at certain levels to come in with their own set of devices including smart phones, laptops, and iPads though they all have to be subjected to thorough screening. Once they have put this in place they can now let users come in with their devices in a phased approach so that they can have time to deal with the challenges that may come up and also to ensure that proper infrastructure and access control mechanisms are in place.

4.3.2 COMPANY B

BYOD Usage Patterns

This section seeks to establish whether BYOD is been used at the company and if yes what model it takes and to what extent it's been used.

A senior ICT officer at company says they strictly do not allow their employees to use their personal laptops within company premises, a rule known and applied to everyone. He adds that they however allow employees to use their smart phones, iPads and to an extent their tablets thou we have restricted access to corporate data and mostly we support these devices for email and internet only.

Respondents from this company confirm this as there is almost 0 percentage usage of personal laptops within the premises but they are quick to add that they aren't restricted to use their other data enabled devices such as smart phones and iPads.

Results from the respondents clearly show high smart phone and iPads utilization with an almost 0 percentage laptop usage which they basically tie to restrictions. From the 5 point scale used, the table below gives the results.

Table 4.4 BYOD usage Patterns

Laptops	1	16%
Smart Phones	6	100%
iPads	5	83%
Tablets	3	50%
Others	0	0%

From the usage table above, it is easy to note that smart phones are the mostly highly utilized own devices in this company. This is closely followed by iPads at eighty three percent and tablets at fifty percent. Laptops come in a distance fourth at 16 percent. It is however important to note that laptop usage in this company is strictly controlled and monitored and this explains its low usage.

BYOD Security Challenges in Company B

This section explores the security challenges faced by company B with respect to BYOD, it looks at the host of challenges as well as what the company is doing to address these challenges.

Just like in company A, security is cited as the biggest headache and this explains why they wouldn't even allow laptops in the premises. "Laptops carry more data and are much trickier to control and secure", notes the senior ICT Officer and this he adds' was one of the main reason they decided to disallow it till such a time when they have controls and policies in place. The officer adds that they don't have explicit policies or controls in place with regard to BYOD usage and as such they wouldn't know or control what users are able to access. Incidentally the company is equally more worried about data loss more than any other threat as they already have substantial controls to diffuse most of the other threats. According to them; hacking, viruses and malware aren't much of a big threat.

In conclusion company B tends to be more conservative with regard to BYOD and that explains their slow approach to BYOD.

BYOD and Productivity in Company B

Just as with company A, this section looks at the impact if any of BYOD on employee and organizational productivity. If there is an impact then, it sets to establish whether negative or positive.

All respondents in Company B agree on the impact of BYOD to performance and are unhappy that they aren't allowed to bring in their laptops. Some say they have to carry whatever pending work they have on flash and memory disks and then work on it with their laptops from home. They add that this is even more riskier than allowing them to come in with their laptops. The convenience of using their iPads for mobility and meetings is cited as a real productivity booster.

Benefits of BYOD to Employees and the Organization

This section seeks to establish other motivations behind BYOD usage by the employees.

According to these respondents convenience and mobility are one of the greatest motivation for BYOD. They also cited productivity, increased flexibility, ease of use and keeping pace with changing technology as other great motivation for BYOD usage.

The table below is an indicator of the many various ways the users benefit from BYOD.

Table 4.3 BYOD Benefits

Increased Productivity	100%
Highly Convenient	90%
Increased Collaboration	60%
Increased Flexibility	75%
Ease of use	90%
Keep pace with changing technology	50%

In conclusion, it is apparent that productivity stands out as the greatest motivation for BYOD followed closely by convenience and ease of use at ninety percent. Increased flexibility, collaboration and the desire to keep pace with changing technology were also cited as motivators behind adopting BYOD.

BYOD Onboarding

This section seeks to establish whether the company does facilitate onboarding and if yes how.

Currently we rely on restrictions, notes Company B's ICT Officer. He however adds that this neither a good nor permanent solution as it has spiral effects on the employees productivity and morale. "It is our desire to give them the best work environment and we know this encompass BYOD but for now they have to bear with the situation" says the Officer.

The company has however, developed plans to this effect and is even procuring iPads and smart phones for its employees as well as providing support and infrastructure to run these devices on. They also hope to provide controls and policies in the near future that will let employees safely come with and use their own laptops.

4.4 Case Analysis and Discussion of Findings

This section does a comparison of the two companies and analyzes the data based on the objectives.

4.4.1 BYOD Usage Patterns

Study from the two companies show a similar usage pattern for BYOD. What is apparent is the desire to use laptops even though it stands outs as the most highly restricted BYOD device in the two companies. Smart phones currently stand as the highest utilized own device gadget and the iPads are equally gaining popularity. Tablets are yet to gain much footing and this is due to their prohibitive costs, says Company A ICT Manager.

4.4.2 BYOD Security Challenges to Organizations

With regard to corporate data security, the threat of data loss has emerged as the greatest worry for both companies. ICT departments from both companies cite securing corporate data and information as their primary objective. This is the reasoning they have behind restricting laptop usage as they insist for now they don't have the technical capacity to control any data held within the laptops. They agree that it's easier to restrict the smart phones and iPads to mails, internet and limited applications but Laptops do provide a whole different level of security challenge.

However, with the popularity of cloud computing and storage (Gartner, 2012), this challenge shall soon be a thing of the past as all processing and storage shall be done at the cloud level which will even handle all security related concerns. Both companies say that they already have budgets for infrastructure upgrade and even their ICT departments are already working on migrating some ERP functions and applications to the mobile platform.

4.4.3 BYOD and Productivity

Data from the two companies tally on productivity and it has emerged as the greatest motivation behind embracing BYOD. They all agree that irrespective of how you frame the individual benefits, all of them end up aiding into the productivity of the employee in one way or another. Convenience for instance means that the employee is flexible and can almost literally work from anywhere, including at home, after working hours, while in traffic and all this goes to enhance their output.

4.4.4 BYOD Onboarding

Secure onboarding of BYOD is a key priority for both companies and this explains their desire and plans to come up with explicit and clear cut policies on BYOD onboarding and usage. The situation as is at both companies is domineered by unwritten rules and regulations something they all agree is bound to change very soon. Due to the importance of BYOD, the company are

already drafting plans and developing infrastructure projects that will allow for integration of BYOD into their mainstream ICT infrastructure. It is also important to note that quite some progress has been made at both companies in respect to onboarding with company A already purchasing laptops for their management staff and allowing them to take them home amid some agreement. A similar development is happening at Company B with managent already procuring Smart phones and iPads for some staff something that they hope to grow and cover a majority of its staff.

4.4.5 Discussion

From the literature review, it was apparent that BYOD is a very prevalent and highly utilized concept in the developed countries. We saw instances where firms are using it to attract and retain superior employees while others are moving to a completely new model where they literally ask employees to come in with their own set of laptops, iPads, tablets and so on (Madden, 2013). The trend has also gained pace locally even though amid a lot of challenges such as lack of supporting infrastructure and lack of rules and policies to govern the same. Locally there are also numerous restrictions' as seen in Company A and B with regard to some aspect of BYOD such as laptop onboarding. This happens because unlike in the developed countries where they have policies to regulate usage and very strong technical controls for implementation, locally such mechanisms do not exist and where they do they happen to be too weak for any meaningful deployment.

Same as in literature review, productivity has emerged as the biggest driver of BYOD usage and is closely followed by convenience. Local users also cite increased collaboration, flexibility, ease of use, innovation and the desire to keep pace with technology also as been some motivation for BYOD usage.

Security challenges as seen from this study are the greatest hindrance to BYOD adoption especially from the organization perspective. Locally there's little infrastructure and control to support safe BYOD onboarding and as such we have seen organization are resulting to denying or simply restricting access to some devices.

CHAPTER FIVE: SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

In line with the general objective of the study, this chapter summarizes the conclusion and recommendations which were arrived at after analysis of the data. It also gives the limitations of the research and gives suggestions for further research.

5.2 Summary of Findings

The main objective to this study was to establish the relationship between organizational Productivity and BYOD usage and also look into security challenges posed by BYOD and how the insurance industry in Kenya is dealing with them. The researcher also set to establish BYOD usage patterns in the insurance industry and also establish the various different ways both organizations and employees benefit from BYOD. Data on usage patterns, benefits, productivity as well as security aspect of BYOD in the insurance industry was collected from respondents through questionnaires and in-depth interviews with ICT and Human Resource management at within the industry.

The results of the research study indicate that BYOD has become a key element in employee and by extension organization productivity. The study goes further to show the many forms in which employees productivity is enhanced due to use of BYOD. It is clear from the study that BYOD usage has a strong positive impact on the overall performance of insurance companies by making workers accomplish tasks more effectively and efficiently. By using such devices as laptops, iPads, smart phones and tablets the users report increased flexibility to the way they work, increased collaboration with colleagues and clients, ease of device use as they require no training, and extremely high levels of convenience as they can literally work from any place they choose.

It is however to be noted that BYOD adoption even though picking pace is still not very popular locally a factor brought about by the fact that BYOD as a concept is not been driven by the

organizations. However, this is changing and the future looks bright as the organizations are making steps albeit slowly in light with embracing BYOD.

This study also highlights the major security concerns and challenges posed by BYOD usage. It however goes further to show just how the insurance firms can work together with the employees to make this a secure experience. Given the direction ICT is taking and the ever fast paced innovations, security whether from BYOD shall always remain live. What is important as noted by the insurance firms is to put security controls and policies in place and most important educate the employees on safe usage to protect both personal and corporate data and information.

5.3 Conclusions

Based on the results from data analysis, findings and discussions above. One can safely conclude the following:

First, even though most employees are not familiar with the term BYOD, use of personal devices at the work place is common. Employees' continue to walk in with their laptops, smart phones, iPads and other personally owned computing devices oblivious of the security risks they pose to the organization. This practice continues to put corporate data at risk, thou no major security incidents have been reported. Own device usage continue to open up potential security loopholes thus exposing the organization.

Secondly, asked why they would prefer their own devices, the employees cite productivity and convenience as the biggest drivers of BYOD. This hasn't escaped the attention of the insurance firms, as they site high responsiveness and increased motivation from the employees. This impact hasn't escaped the attention of management and as seen from both Company A and B, there has been increased effort to facilitate and safely onboard own devices. The organizations are now procuring laptops, smart phones and iPads for their staff and there are increased efforts to upgrade infrastructure to support the same.

Thirdly, insurance firms acknowledge the positive impact of BYOD explaining the reasoning behind which they are drafting policies on personally owned and other mobile devices. This is

further, expounded by the open mindedness to BYOD and the willingness to engage users in coming up with agreeable terms to own device onboarding and usage for the mutual benefit of all. This has seen employees been more knowledgeable on safe BYOD usage as well as an understanding of the risks they pose both to their own personal and corporate data, as such they have become more proactive and caution.

Fourth, the security challenges emanating from BYOD hasn't escaped the attention of both the employees and the insurance firms and they all agree on the need to work together. Most of the security challenges from BYOD are inherent and can be reduced. BYOD is mainly hampered by a lack of knowledge of risks posed by own device both from the employee and organization perspective

Lastly, the insurance firms agree that BYOD cannot be wished away and as such have plans to facilitate phased onboarding, addressing security challenges as they go along, dealing with infrastructure issues, addressing compensation issues as the insurance firms indeed appreciate that the employees are spending quite a lot on their own devices while doing company work.

5.4 Recommendations of the Study

From the study the study, the researcher observes that BYOD still remain a new concept locally thou its usage is common taking many different form. As such it is recommended that training on BYOD usage should be conducted in the organizations irrespective of whether these mobile computing devices are provided for by the company or are personally owned.

Policies on BYOD usage and related security also remain vague and as such the organizations should fast track this. The researcher recommends an all-inclusive approach; the employees should be at the center of formulating these usage rules and guidance. This approach has over the years been proven to ease acceptance as the employees easily own up and observe the policies.

BYOD usage hasn't picked up at the same rate as observed in western countries in the literature review. As such and due to the benefits emanating from BYOD, the researcher recommends that the organizations should look for ways to increase adoption. This means a wide range of effort towards the same right from friendly usage policies to compensations schemes as well as

offering the required infrastructure support. It is also recommended that to maximize usage, the organization should look for ways to offload some of their applications and data processing to these devices through mobile apps, VPN support and virtualization, cloud computing and containerization among others.

5.5 Limitations of the Study

The major constraint to this study was the availability of respondents especially the non-managerial employees as most are not allowed to speak to outsiders without prior permission and also due to their demanding jobs and working hours.

Possible bias was another hindrance and withholding of information for fear of painting their organization in bad light. This was especially so with the managers.

5.6 Suggestion for Further Research

This study's focus was on BYOD productivity and security dimensions and how an organization can strike a balance between the two. It came out clearly that indeed this concept though been used still is very new within the Kenyan context and as such can be explored further with its impact been assessed in different industries part from insurance.

From this study it is clear that BYOD does has a big impact on employees' performance, however this may need to be quantitatively studied and as such provides an avenue for further research. The researcher thus recommends a quantitative study with hypothesis testing to establish the impact of BYOD to productivity quantitatively.

REFERENCES

Babbie and Earl (2007) *The Practice of Social Research* (12th Edition) Cengage Learning

CIO (2013) *How to Craft the Best BYOD Policy*
http://www.cio.com/article/732665/How_to_Craft_the_Best_BYOD_Policy Retrieved August 3, 2013, from the CIO

CiteWorld (2013) *Containerization, The BYOD Disaster*.
http://www.citeworld.com/consumerization/22094/containerization-byod-disaster?page=1 Retrieved July 05 24, 2013, from CiteWorld

Current Analysis (2012) *Action Learning Project:* Bring Your Own Device *(*BYOD*)* Retrieved on August 26th 2013, from *www.bf.umich.edu/bfleadership/docs/2012/byod- research-paper.pdf*

Forbes (2013) Calculating true cost of BYOD
http://www.forbes.com/sites/eliseackerman/2013/05/28/calculating-the-true-cost-of-byod/ Retrieved July 01, 2013, from Forbes

Fortinet (2012) *Enabling Secure BYOD, How Fortinet Provides a Secure Environment for BYOD*

Gartner (2012) A holistic approach to your BYOD challenge. *Creating a Bring Your Own Device (BYOD) Policy.* Retrieved August 19th 2013 From HP.

iPass survey (2012) The iPass Global Mobile Workforce Report, *Understanding Enterprise Mobility Trends and Mobile Usage.* Retrieved August, 20th 2013, from iPass

Jack Madden (2013) BYOD, Enterprise Mobility Management. *Does BYOD save money, yes or no?* Retrieved from
http://www.brianmadden.com/blogs/jackmadden/archive/2013/07/26/does-byod-save-money-yes-or-no.aspx

Jason kolb and Jeremy kolb (2013) *The Big Data Revolution*. (Kindle edition) (Applied Data Labs Inc. 2013)

Jeff Loucks , Richard Medcalf, Lauren Buckalew , Fabio Faria (2012) *The Financial Impact of BYOD Top 10 Global Insights from the Cisco IBSG Horizons Study*

Joseph Bradley, Jeff Loucks, James Macaulay, Richard Medcalf and Lauren Buckalew (2013) BYOD: *A Global Perspective, Harnessing Employee-Led Innovation*, Cisco IBSG Horizons.

Kathryn Weldon(2012) Bring Your Own Device: *How to Protect Business Information and Empower Your Employees at the Same Time.*

Olive M. Mugenda, Abel G. Mugenda (1999) Research Methods: *Quantitative and Qualitative Approaches*. Nairobi Acts Press

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

Paruchuri R. Krishnaiah (1988) *Handbook of Statistics* (2nd Edition) North-Holland, Amsterdam.

Peter Drucker, Peter Ferdinand Drucker (1966) *The Age of Discontinuity* (New York: Harper and Row, 1969)

Peter Drucker (1959) Landmarks *of Tomorrow*. Harper & Row (New York, NY: Harper & Brothers, 1959)

PwC (2012), Bring your own device *Agility through consistent delivery*. Retrieved August 20th 2013 from *www.pwc.com/us/en/byod-agility-through-consistent-delivery.jhtml*

Ranjit Kumar (2010) Research Methodology: *A Step-by-Step Guide for Beginners* (3rd Edition) SAGE Publications

Trend Micro (2012) BYOD and the Consumerization of IT: *Key Strategies to capture and measure the value of consumerization of IT*

Wolfgang Reinhardt, Benedikt Schmidt, Peter Sloep et al. (2011) *Knowledge worker roles and actions* - In Knowledge and Process Management

Zeus Kerravala (2012) *BYOD Requires New Network Strategies*. ZK Research (2012). Retrieved August 21st 2013 from Xirrus

APPENDICES ONE: QUESTIONNAIRE

My name is William Turi, an MBA student at the University of Nairobi. I am conducting a study on **"THE BRING YOUR OWN DEVICE PHENOMENA: BALANCING PRODUCTIVITY AND CORPORATE DATA SECURITY"** and kindly request for your assistance in completing the following questionnaire.

SECTION A: BYOD AND SECURITY

1. Do you let employees come in with their own computing devices at the work place?

   Yes [ ] No [ ]

2. If yes kindly tick against the kind of devices you allow on the corporate network

   Smart Phones [ ]
   Laptops [ ]
   iPads [ ]
   Tablets [ ]

   Others Specify _____

   _____

3. Do you allow these devices to connect to the corporate network?

   Yes [ ] No [ ]

4. If yes what kind of corporate data processing and or storage do you allow on these devices?

   Emails [ ]
   Business Applications [ ]
   Mobile Applications [ ]

Others Specify ——————————————————————

_____

5. Do you have any existing policies on BYOD usage?

Yes [ ] No [ ]

If yes please Specify ——————————————————————

_____

6. In a 5-point scale where: No extent=1, Little Extent = 2, Moderate Extent=3, Great Extent=4 and Very Great Extent=5, tick to indicate the extent to which you face the following BYOD challenges

BYOD Security Challenges	**No extent**	**Small extent**	**Moderate extent**	**Large Extent**	**Very Large extent**
	1	2	3	4	5
Viruses					
Malware					
Hacking					
Threat of Data Loss					
Others (Kindly Specify)					

SECTION B: BYOD BENEFITS

In a 5-point scale where: No extent=1, Little Extent = 2, Moderate Extent=3, Great Extent=4 and Very Great Extent=5, tick to indicate the main reason why you would adopt BYOD.

BYOD and Productivity	**No extent**	**Small extent**	**Moderate extent**	**Large Extent**	**Very Large extent**
	1	2	3	4	5
To help improve productivity					
For convenience					
To keep up pace with changing technology					
Personal Preference					
To create innovation					
To enhance Collaboration					
For Flexibility					
Ease of use					
More featuristic					
Others specify					

Others; Please list them down

a.

b.

c.

d.

e.

SECTION C: BYOD AND PRODUCTIVITY (MANAGEMENT STAFF)

1. Does the use of BYOD make your employees more Productive?

   Yes [ ] No [ ]

   If yes kindly list why this is so, _____

   _____

   _____

2. What Productivity challenges do you face with respect to BYOD?
   - **a.**
   - **b.**
   - **c.**
   - **d.**

3. How do u address the Productivity challenges mentioned above?
   - **a.**
   - **b.**
   - **c.**
   - **d.**

4. In what ways do you think you can help the users maximize BYOD benefits for the benefit of the company?
   - **a.**
   - **b.**
   - **c.**
   - **d.**

SECTION D: BYOD ONBOARDING (MANAGEMENT STAFF)

1. How are you addressing the security challenges brought about by BYOD (**in section A above**)?
    - **a.** Viruses
    - **b.** Malware
    - **c.** Hacking
    - **d.** Threat of Data Loss
    - **e.** Others
2. Are there any other challenges you face with respect to BYOD?

    Yes [ ] No [ ]

    If Yes, Kindly List down the challenges and how you address them _____

    _____

3. Currently what actions or in what ways have you ensured safe onboarding of the allowed devices?
    - **a.** Laptops
    - **b.** Smartphones
    - **c.** iPads
    - **d.** Tablets
    - **e.** Others

4. At the management level do you have any plans or a road map for BYOD going forward?

    Yes [ ] No [ ]

    If yes, kindly give a brief on the plans _____

    _____

Your time is highly valued and appreciated. Thank you