BRING YOUR OWN DEVICE PHENOMENON AND INFORMATION SECURITY AT JARAMOGI OGINGA ODINGA TEACHING AND REFERRAL HOSPITAL (JOOTRH), KISUMU, KENYA

BY

SHONDO EVOGE FREDRICK

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF MASTER OF BUSINESS ADMINISTRATION (MBA)

SCHOOL OF BUSINESS, UNIVERSITY OF NAIROBI

2019

DECLARATION

This research project is my original work and has not been presented for award of degree in any other university.

Signé é é é é é é é é é é é é é é Dateé é é é é é é é é é é .

Shondo Evoge Fredrick
D61/858866/2016

Signé é é é é é é é é é é é é é é é Dateé é é é é é é é é é é é .

Professor Kate Litondo
Department of Management Science
University of Nairobi

ACKNOWLEDGEMENT

I wish to thank my supervisor Professor Kate Litondo, her relentless support, direction and supervision in coming up with this document. and all lecturers on defense panel who played a major role during my presentation by giving me the direction to take in order to come up with a good project that is in tune with this studyôs objectives.

DEDICATION

I appreciate the encouragement from my wife and children for encouragingme during entire period of study and parents who always stood with me in prayers.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS AND ACRONYMS

ANOVA: Analysis of Variance

BYOD: Bring your own device

CEO: Chief Executive Officer

JOOTRH: Jaramogi Oginga Odinga Teaching and Refferal Hospital

PMT: Protection Motivation Theory

TAM: Technology acceptance Model

ABSTRACT

Bring your own device phenomenon can lead to breach of information security and lead to several litigations in which case the responsible organization can lose lots of money as costs and damages. Yet, bring your own device improve efficiency of information security if properly deployed and relevant policies put in place to safeguard it. It was necessary to conduct a study related to bring your own device on information security. Thus, the objective of the current study was to establish bring your own device on information security at the OgingaOdinga Teaching and Referral Hospital in Kisumu County. The specific objectives of the study were to establish the extent to which JOOTRH is using bring your own device phenomenon; to determine the challenges of bring your own device phenomenon; and to establish the effect of bring your own device phenomenon on information security. The study used a case study design and a simple random sampling method to obtain a sample of 83 respondents out of 106 respondents. Data was collected using questionnaires and then analyzed using both descriptive and inferential statistics. Greater extent of using bring your own device phenomenon has a significant positive effect (β =0.423, $p< 0.05$) on information security. The study also established that challenges of bring your own device had insignificant negative effect (β = -0.184, $p< 0.05$) on information security. Further, the study established that the effect of bring your own device phenomenon is explained by 47.8% variation of information security.

CHAPTER ONE: INTRODUCTION

1.1 Background of the Study

during the fourth industrial revolution, bring your own device (BYOD) is more likely than not to be fore grounded in many institutions, health sector included. Going by Wanyonyi, Rodrigues, Abeka, and Ogara (2017), protection of health information is not only interposing, but also salient in ensuring efficient health delivery to those who seek medical attention or consultation. Such is because health information keeps records of patients, some of which are sensitive or embarrassing or both, and which must be treated with the sensitivity and care that they require. Yet bring your own device mode of operation is a potential ground for such sensitive information to be misused by those who should care them. A lot of discussions have been fronted on why health information should be secured, but the reasons for protecting health information also has legal implications and is thus not negotiable.

There are theories that have been advanced to explain bring your own device phenomenon. For instance protection motivation theory as Askar and Shen (2016) points out, is a model premised coping and threat appraisal imperatives. It posits that information technology is preferred by organizations on the basis of how the threats can be tackled and how the organization can cope with threats posed as a result of using such information technology. Bring your own device has threats and coping mechanisms that can be utilized to leverage on its merits while mitigating the associated threats. On the other hand, Technology acceptance theory model (TAM) is also another theory that anchors bring your own device methodology. According to Scherer, Siddiq, and Tendeur (2019), technology acceptance theory is founded on two assumptions namely, ease of use and usefulness. As the name suggests, information acceptance theory is mainly intended

for wider presentation of information technology. The application of bring your own device phenomenon are therefore paramount for its implementation in the hospitals in particular and health sector in general.

The merits of bring your own device phenomenon cannot be overemphasized in the health sector, and more so, in a learning health facility like Jaramogi Oginga Odinga Teaching Referral Hospital. According to Wanyonyi, Rodrigues, and Abeka (2017), the vulnerability in health sector makes it possible if not easier for unauthorized third parties to infiltrate the institution in particular the data of the hospital. Infiltration of hospital data has several consequences which pose danger not just for the hospital, but also for the patients whose information has been infiltrated. For instance, such information can be used by third parties to embarrass the patient or get the health information which braches the privacy of the individual. Such privacy breaches can result to law suits which may cost the hospital lots of money in damages.

1.1.1 Bring Your Own Device.

|According to De Shield (2017) posted that modus operandi, the likes of which organization employees are allowed to bring to work and utilize personally owned laptops, Mobile phones, and tablets to transact organization business. Although BYOD is a relatively new phenomenon, having been introduced in the year 2009, its merits such as increased job satisfaction has been felt everywhere in the world. According to Magruder, Lewis, and Burks (2015), bring your own device arrangement ensures that employees are able to work on familiar interfaces and are also able to work out of the office which contribute to work-life integration in particular and job satisfaction in general.

The proliferation of BYOD to modern work places according to Olalere, Abdullah, Mahmod, & Abdullah (2015), whether mainstreamed or not, has been due to cloud computing and portable devices. However, many health institutions have not streamlined the policies regarding BYOD yet employees have continue to utilize their own devices in work places at the expense of the safety of information safety. Although the merits of bring your own device may be great for organizations such as health institutions, the dangers it poses in terms of information security cannot be underestimated.

1.1.2 Information Security

The importance of information security in any organization cannot be debated. Magruder et.al (2015) asserts that information security is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information, and in the hospital set up like Jaramogi Oginga Odinga Teaching and Referral Hospital details of patient need to be kept and handled with a lot of confidentiality, however Bring your own device has a lot of implications on information security that could be detrimental if not mitigated in good time. For instance, Wangutusi (2013) points out that bring your own device can cause exposure of the organization confidential information to unauthorized parties. For instance, if the phone gets lost and it is found by another unauthorized person, such person may get access to the confidential information of the organization and misuse the same. Furthermore, compromise of the bring your own device denies the system to legitimate users especially during the period the system or network is under the control of hackers or such criminals

Further, Magruder et.al (2015) contends that theft of enterprise information is yet another implication of bring your own device upon deployment in the organization. Such theft can be

orchestrated by malicious wireless access points or by short message service links that can be sent to telephone or a mobile device and end up harvesting information from such devices. The problem is that the information obtained through theft can be misused to the advantage of the organization and its clients or patients in a health organization. Furthermore, application malfunction can also be an implication of bring your own device BYOD in an organization setting. As Olalere et.al (2015) points out, malicious users of the system as a result of bring your own device phenomenon can cause malfunction of the system and hence ground network operations to a halt. Its implication is infrastructure disruption in which case the network infrastructure gets disrupted and hence interferes with the efficiency and effectiveness of the network. In hospital environment, such disruption can cause fatal mistakes to the patients.

1.1.3 Health Industry in Kenya

Kenyaôs health development trajectory according to Kimathi (2017) is traceable to the early 1990s when Kenya Health Policy document was propounded by the government of the day. The document was meant to put in place a robust program for the people of Kenya from different positions and persuasions while also supporting private players in the hospital industry. Although the document did not begin the health reforms, especially because there was some kind of medical intervention during the colonial period, it streamlined the operations of hospital industry in the country. The reforms have continued to take different shapes by different government and tangible results have been realized which has culminated to free access to medication in many counties in Kenya today. However, compared to developed economies, Kenya still has a long way to go.

The problems of health sector are still numerous. As Alali (2015) contends, Kenya only spends about 7% of the GDP on health care yet public sector account for 60% of where Kenyanôs seek medication with private players taking the rest. Additionally, corruption, poor remuneration of doctors, lack of adequate equipment and physician attitudes have also been cited as salient challenges at the health sector in Kenya. The marginalization of the poor in seeking the highest possible treatment and periodic strikes by the physicians and hospital workers adds to the limping state of the health sector. Although there are different levels of hospitals and health centers spread across the country, they are not adequately stocked to deal with complications that are brought to their attention from time to time. In regard to the information security deployment, Kenya has not been left out. As Muinga et.al (2018) points out, Kenya has implemented the e-Health strategy that is a system of collecting health information and using it in a way that increases accuracy and efficiency as well as decision making. Additionally, information systems have also been developed and put in the HIV clinics to help in administration of services across HIV facilities across the country. However, lack of adequate budget makes it difficult for such health facilities to develop and implement sufficient health record safeguards to protect electronic health records, hence putting such data at risk of abuse.

1.1.4 Jaramogi OgingaOdinga Teaching and Referral Hospital

According to Mbenywe (2018), JOOTRH is the main Referral Hospital in Kisumu County whose original bed capacity was 200. However, because of high number of patients some of which come from outside the county, the bed capacity has been improvised to 526 beds. In total the hospital serves more than 5 million patients from the expansive western Kenya. The hospital also has in and outpatient services as well as surgical and accidents and emergency center that attends

to those who need such services. Additionally, what contributes to congestion of the hospital is that all the sub-county hospitals including Kombewa, Muhoroni, and Ahero refer patients some of whom have minor medical needs that can be taken care of at the sub-county hospital.

In addition, the hospital as Oketch (2015) points out is one of the referral hospitals in Kenya and part of which serves 60% of the Kenyan population. The hospital management comprises a 12 member team board led by a chairman and an executive officer (CEO) who oversees the operations of the hospital. The running of day to day activities is therefore under the chief executive officer. As such, the hospital is regulated by the government of Kenya with the health care regulations just like other Referral hospitals in the country. After the devolution, the hospital was reverted to the Kisumu County government on whose shoulder, the ultimate responsibility lie. The hospital also collects between 0.4 and 0.6 million Kenya shillings on a daily basis which money is directed to the county government revenue account before disbursement to fund the operations of the hospital.

In regard to information communication infrastructure, JOOTRH has health record system in place. According to Wanyonyi et al (2017), the hospital has several information communication and technology systems that hand different facets of the hospital management. For example, health record system collates and stores all health information for every patient that visits the facility. This has replaced paper based health record that is prone to loss or mishandling. The system also ensures efficiency and availability of data for policy and practice. For instance, once a patient has been diagnosed, they are sent to the hospital pharmacy to collect drugs in a paperless fashion. However, it cannot be conclusively argued that the systems are safeguarded from misuse by unauthorized persons. Bring your own device in relation to JOOTRH will have

a number of benefits , one being that it will lead to employee satisfaction because by using their own devices they will be able to deliver efficiently since the devices are owned by them and they do a lot with the devices , another benefit is that it will be cost saving to the organization ,since employees are using their own devices the cost factor shift from employer to employee and the organization will be able to use the available funds for another task, in addition BYOD will lead to increased output and innovation because the employees are comfortable using their devices and are generally fortified with the latest technology which will be beneficial to the organization.

1.2 Research problem

Bring your device (BYOD) phenomenon finds itself centrally placed in the discourse of office automation and in the wake of the fourth industrial revolution (4IR). As Akar and Shen (2016) asserts, BYOD enables employees of organizations to not only work on familiar interfaces of their devices, but also contribute to work-life integration because assignments can be executed away from the work station. Furthermore cloud computing and the availability of mobile devices has made BYOD methodology to take center stage in nearly all contemporary organizations. However, without safeguards to protect data, especially in sensitive environments like hospital industry, information security breaches become inevitable. The need to protect patient data in the hospital industry arises from the realization that medical reports of patients may be available to unauthorized persons that can be used against such people and end up embarrassing them. As Olalere et.al (2015) points out, the implications of bring your own device are numerous. For instance, failure to have proper mechanisms to guard against patient data may lead to exposure of confidential information, theft of hospital information, application malfunction as well as

infrastructure disruption all which has the potential to undermine efficiency and effectiveness of service delivery to those who need it most.

The demerits of bring your own device phenomenon cannot be overemphasized in the health sector, and more so, in a learning and referral hospital like JOOTRH. As Wanyonyi et al (2017) contends, in the year 2017, the vulnerability in terms of unauthorized access of electronic health records (EHR) stood at 93.5% while that of theft of the records stood at 80.8% at JOOTRH. Such high level of possibility of security breach poses a serious ramification to the safety of information security. Yet, challenges of bring your own device methodology can be established through empirical study as well as their implications to inform policy and practice.

Similarly, it must be born in mind that just like technology has its ups and downs, bring your own device methodology cannot fail to have its challenges. Magruder et.al (2015) asserts that data leakage which is pilferage of data to unauthorized party outside the organization is a key challenge of bring your own device methodology. Additionally network vulnerability which makes it easy for unauthorized parties to access the network or the system is also another challenge of BYOD phenomenon. Network vulnerability can be occasioned by weak passwords which makes it easier for penetration by third parties. Furthermore, malware which is malicious software targeted at getting access to the system by third parties is additional challenge. For instance, social media links can be used by hackers to get access of employee device and compromise information security of the organization such as the hospital.

Lots of empirical studies have been done about the challenges of BYOD methodology and its implications on information security in a number of geographic scopes. For instance, DeShield

(2017) concentrated on bring your own device and challenges of its implementation in the United States of America. Additionally, Magruder et.al also examined bring your own device in organizations in the United States of America. Furthermore, Olalere et.al (2015) examined meta-analysis on bring your own device and security implications in Malaysia. Further, Akin-Adetoro (2016) examined application of bring your own device within the small and medium enterprises in South Africa.

Locally, Kamau (2013) focused on bring your own device and data security in the insurance industry in Kenya. Similarly, Wangutusi (2013) also sought to find out the user behavior in the insurance industry. In addition, Wanyonyi et.al (2017) looked at security controls while using bring your own device at JOOTRH in Kisumu County, Kenya. Although the studies are plausible, they do not specifically investigate the relationship between BYOD and information security in Kenya health facilities, and through this study the knowledge gap will be answered.

1.3 Objective of the Study.

The general objective of this study was to investigate BYOD phenomenon at the Kenyan health industry, specifically to:

a) Establish the extent to which JOOTRH is using BYOD phenomenon
b) Determine the challenges of using this phenomenon
c) Establish the effect of BYOD on information security at JOOTRH.

1.4 Value of the Study

This could be valuable in theory building. As such, the study could build more on protection motivation theory by incorporating the findings to ensure that there are ways and means for

protecting data while using information communication and technology as demonstrated by the theory. The study could also add more information to technology acceptance model (TAM). As such, the study findings could build the theory more by advocating the use of information technology in a way that does not undermine information security.

Further, the study could be utilized for practice. Health administrators and managers of different units could utilize the study to fully automate working environment while protecting data of patients. As such, when the data of the patients are protected, no misuse and embarrassment could be caused to patients and thereby enhancing the doctor patient relationship and service delivery not just for the county residents, but also for any other patient that could seek medical attention at JOOTRH and other hospitals alike.

Furthermore, the study could be utilized for policy formulation. The county governments could formulate policies on how to use bring your own device methodology in a way that protects the information regarding patients. Such policy could also cover the streamlining of bring your own device so that the methodology is used across board. As such, the hospital industry could save more that would have been used to buy computer equipment for employees.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

It is the documentation of the comprehensive review of the study. Other than the introduction section it looked at the theoretic foundation of the study. It also presented the empirical review of literature. Similarly, the section presented summary of gaps arising from the empirical literature review. Finally, it looks at the conceptual framework underpinning the study.

2.2 Theoretical Foundation of the Study

It is anchored on Protection Motivation Theory and Technology Acceptance Model.

2.2.1 Protection Motivation Theory (PMT).

Is one of the theories from health sciences that can be used to explain challenges of bring your own device and the implications thereof in any organization such as health institutions. According to Westcott, Ronan, Bambrick, & Taylor (2017), the theory was developed by Rogers in the mid-1970s purposely to help in explaining how individuals can protect themselves in times of health hazards and natural disasters. For example, it helped to explain the individual measures that individuals could take to mitigate diarrhea during times of floods. Such mitigation mechanisms from the individual then helped to ensure that the adverse health outcomes as a result of natural disasters and during disease outbreak were mitigated. Progressively; the theory has been widely applied in computing and related disciplines. Askar and Shen (2016) asserts that the theory has two main assumptions namely, threats appraisal and coping with threats.

The theory posits that whenever an organization faces threats related to computer use and application, it is important that such threats are appraised so that relevant response can be put in

place to mitigate such threats. Similarly, the theory posits that a mechanism of dealing with data security is coping with the threats. For example, if the threat that the organization is dealing with does not affect the organization to a level that the organization can incur huge loses, then the organization can cope with the threat. For instance, employee mobile device can be stolen and then data related to the organization can be accessed. Such is a threat but the organization can cope with such threats by putting in place mechanisms for coping such as changing or deleting access credentials (Askar and Shen, 2016)

As Wescott et.al (2017) asserts, the theory was construed to explain how individuals can deal with threats. In the same way, the theory is applicable in the current study to explain challenges of bring your own device and the implications thereof. In the current study, the threats are the challenges of bring your own device phenomenon which include data leakage, network vulnerabilities as well as malware. The organization must therefore find ways inherent in the organization to deal with such threats or challenges for the purposes of safe information security.

2.2.2 Technology Acceptance Model (TAM).

The model is relevant to the present study is known and according to Chuttur (2009) was fore grounded by Fred Davis and Richard Bagozzi in the 1989 to solve the problem of failure by employees to use systems in the work place. The trio then decided to come up with a model that could ensure mass application of technologies in the work places to ensure efficiency and effectiveness. The first algorithm of the system consisted of the system specification, motivation of employees and the use of technology. The specification of the system was intended to demonstrate the good specifications to the employees to endear them to the system. Motivation

aspect was made to make the system the best place to work and the use of technology was the desired output for efficiency and effectiveness of the organization at the time.

As Scherer et al (2019) postulates, the theory has two main assumptions which are ease of using the system as well as application of the same. For a wider application of technology, which is the comprehensive objective of the theory, there has to be easiness of use of the system. It therefore means that user interface and manuals must be user friendly and the design of the system must be easy to work with. Similarly, the usefulness of the technology must be without question. There are various technological appliances with different uses in different organizations. As such, the usefulness of the technological appliance preferred by the organization must be based on its benefits or usefulness to such organization. As Chuttur (2009) asserts, the model was based for wider application of technology. The model therefore fits in the current study and is the basis of using your own device phenomenon. The easiness of use and usefulness of technology devices is intricately linked with bring your own device for institutions such as hospitals. For employees to use their own devices such devices must be easy to use and must be useful for the organization work which will result to worker fulfillment, better output, inventions and cost savings to the organization Furthermore, it is on such devices that challenges abound. Such challenges include malware threats, network vulnerabilities as well as data leakage. Technology acceptance theory therefore seeks to explain how information, communication and technology can be used widely by an organization despite the challenges inherent in them.

2.2.3 Bring your Own Device Phenomenon and Information Security

The implications associated with BYOD on information security cannot be gainsaid, especially if there are no mitigation mechanisms in place. For instance, data leakage as Magruder et.al (2015)

points out happens when the technology device in the hand of employee is maliciously accessed by a third party who is not authorized to access it. There are several ways around which data leakage can happen within an organization. For instance, loss of mobile device can be picked by a third party who is not authorized to access information and then may end up misusing the information thereof. Such leakage of information leads to implications that end up disadvantaging the organization. For example, the confidential information may be exposed which deals a blow to information security.

In addition, network vulnerabilities are yet another challenge associated with bring your own device (BYOD) phenomenon. DeShield (2017) postulates that network vulnerabilities are the various ways in which a network of an organization may infiltrated either by an outsider or employee of the organization for reasons that undermines objectives of the organization. Inside connections and weak passwords are just some of the ways in which a network of an organization can be vulnerable and leads to theft of enterprise information. Theft of enterprise information is therefore an implication of network vulnerability and such stolen information may be used in the wrong way by the third party.

Furthermore, malware is another challenge that confronts data security in any organization or institution. According to Wanyonyi (2017) malware is malicious software that is developed by third parties to solicit information for malicious use. Such software can find themselves in the devices of employees in many ways. For example, short message service links and third party app stores are some of the sources of malware. Such malware may cause many problems to the system such as infrastructure disruption which renders the network infrastructure less useful to the organization during the time of attack.

2.3 Bring Your Own Device phenomenon and Information Security.

Data leakage and information security have been researched tenaciously by various researchers. Olalere et.al (2015) studied the influence of BYOD phenomenon and their influence on security concerns. The study used secondary data and hence literature survey design was the study design of choice. The study therefore included peer reviewed journals and other related academic journals. The study data was formerly analyzed using descriptive statistics. The study established a significant positive relationship between the malicious user of device and information security. Further, Alsaleh, Alomar and Alarifi (2017) focused their study on mobile phones and security perceptions. The study used in-depth interviews. The study used secondary materials as a source of data. As such, academic publications and unpublished academic materials ensued. The study deployed a descriptive survey design and data was evaluated using thematic content analysis. The study data revealed that loss of mobile devices contributed to undermining of information security within organizations that were in the literature.

Additionally, Obonle (2015) sought to study mobile devices and network security. The study also utilized secondary data and hence literature survey design was employed to anchor the study. The study then used peer reviewed journals and published as well as unpublished academic materials for the study. Qualitative methods were used to analyze data. The study findings revealed that remote access by attacker contributed to information security vulnerability.

In addition, Salahdine and Kaabouch (2019) sought to look at how social engineering attacks impacted on information security. The study employed survey design and used secondary data as a source. Publicly available and published academic materials were used to solicit data. Descriptive statistics was used .It established social engineering contributed to infrastructure

disruption of the organization network. Furthermore, King, Henshel, Flora, Cains, Hoffman and Sample (2018) were more interested in maliciousness and cyber security in their study. The researchers utilized literature review design and hence secondary data ensued. Secondary data were sourced from multiple disciplines such as law, sociology, economics, and other business disciplines. Data was then analyzed through qualitative means. The study result revealed that malicious application did not contribute to application malfunction. Just like data leakage, there has also been several scientific studies on network vulnerabilities and their implications on information security. Carstens and McCouley-Bell (2004) studied the influence of password and data security. The study used both experimental design and study design. The study sampled a total of 280 respondents. Inferential statistics was then analyzed. and results revealed weak passwords had a significant positive relationship with information security.

Further, Colwill (2009) researched on human factors and implications on data security. The study sampled a total of 98 respondents. The study employed survey study design. The study then utilized quantitative methods to analyze data which was primary in nature. The study findings revealed that Trojan human had significant positive association with information security. Furthermore, Maillart, Zhao, Grossklags, & Chuang (2017) pursued to find out the influence of bugs on data security. The study utilized empirical study design. The study was conducted in Geneva Switzerland. Quantitative methods were used for analysis. The study findings revealed that bugs contributed to information security disruption.

Additionally, Li (2017) pursued to investigate the influence of inside breach on data security. The study utilized empirical study design. Although the study sampled students in universities, there was no sample size number indicated and the study was mainly primary in nature. The

study findings revealed that inside connection contributed to information security breach. In addition, Sharma (2016) studied the influence of wireless networks and information security. The study employed meta-analysis design. Secondary data was then used in the study. The secondary data was sourced from journals and publications. Qualitative method of data analysis was then used to analyze data. The study established that wireless access points had no effect on information security.

Various scientific studies have also been done on the subject of malware and information security. Faghani and Nguyen (2017) for example directed their study on Trojan malware and social networks. The study utilized analytical model and relied on secondary data for the study. As such online social network data was used while no sample size was indicated. The study showed that there was not considerable relationship between Trojan apps and information security. Further, Medani, Zakaria, Gani, and Zaidan (2011) sought to investigate short message links and security concerns. The study utilized experimental design. Purposive sampling technique was also utilized for sampling with a total of 208 respondents being sampled. Inferential statistics was then applied and revealed short message services had positive association with information security. Additionally, Harris, Brookshire, Patten, and Regan (2015) studies mobile application and security concerns. The study employed survey design as the preferred methodological framework. Prediction model was then applied to predict the characteristics of the applications being downloaded. The results revealed that third party app stores had significant positive association with information security. In addition, Gupta and Dhani (2015) focused their research on networking platforms and security implications. Exploratory study design was utilized . The study sampled 245 respondents. Quantitative means

was then applied. Results revealed social media links had a significant positive relationship with information security. Furthermore, Wabende (2014) studied malware threats and information security. The study employed a case study design in a health institution sampling 98 respondents at random. Data was then analyzed using inferential statistics. The results revealed that email links donôt have a significant positive relationship with information security.

2.4Summary of Knowledge gaps

Although there are different findings, plausible studies have been done linking bring your own device phenomenon and information security. Apart from the inconsistencies in finding, the studies also suffer from methodological limitations like the usage of experimental design and small sample size in the studies. Experimental design creates artificial situations which can influence the generalization and reliability of findings. Similarly, small sample sizes make it hard to simplify the study discoveries beyond the geographical scope of the study. Father, the studies investigated single variables of bring your own device phenomenon and how such variables influence information security in various organizations. The studies did not focus on the three objectives namely, extent of use; challenges; as well as effect of bring your own device phenomenon on information security at the Jaramogi Oginga Odinga Teaching and Referral Hospital in Kisumu Kenya. Therefore, bring your own device phenomenon and information security at Jaramogi Oginga Odinga Teaching and Referral Hospital in Kisumu Kenya is missing

2.5 Conceptual framework.

The conceptual framework in Figure 2.1 shows independent variables at the left side and dependent variables at the right side. The independent variables are laptops, Ipads, Tablets as well as Mobile phones. The implications of such variables which are the BYOD variables are

what constitute the dependent variables which are the implications of the same. The implications therefore include exposure of confidential information, denial of system to legitimate users, theft of enterprise information, application malfunction as well as infrastructure disruption.

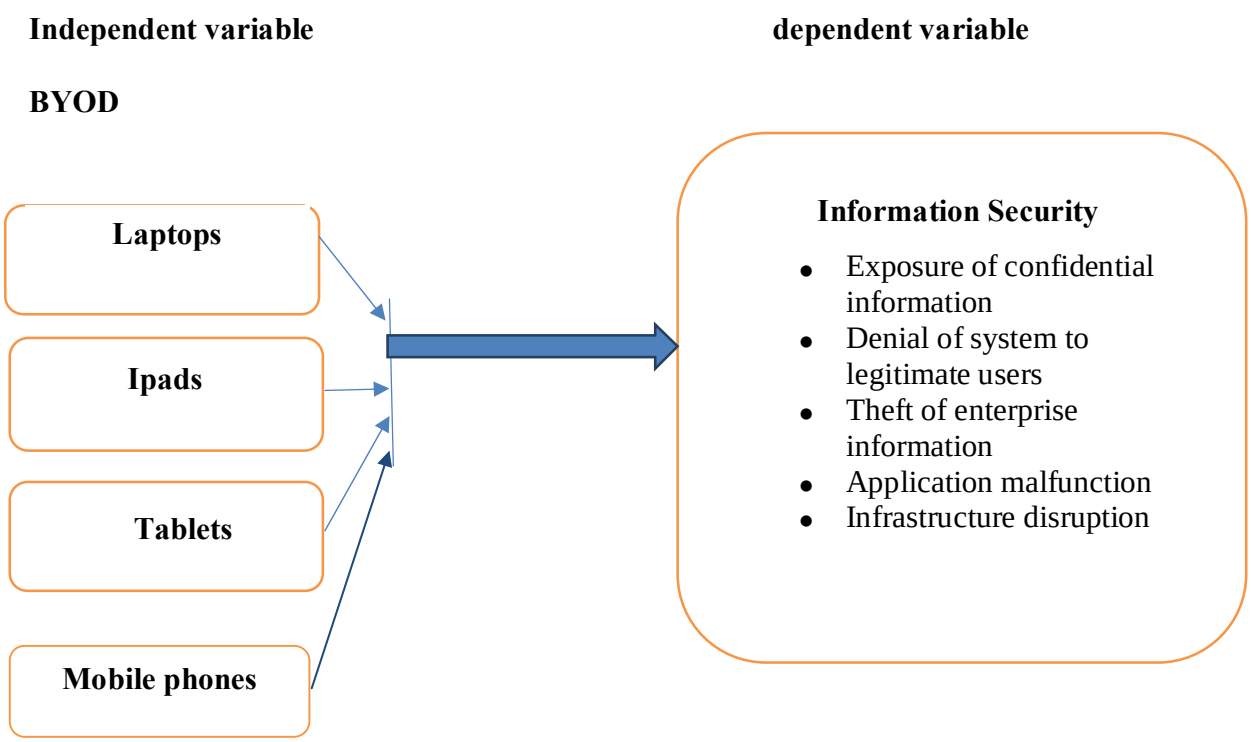

Figure 2. 1 Conceptual framework of the study

Source: Research data (2019)

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

This chapter describes the steps taken to solve the research problem. It outlines the procedure that the researcher will undertake to collect and analyze data; the key areas of the study are research design, population of study, sample design, data collection and data analysis

3.2 Research Design

It is the conceptual structure within which the study is conducted to solve research problem and by using case study designs as Kothari(2004) that seeks to obtain in-depth information from one single bounded case or element and hence allows deeper insights of the subject of investigation. Case study design thus allow amount and value of data which may not be obtained using other study designs and therefore contribute to reliable generalization of findings. The researcher therefore acknowledged that by using correlation study design, the objectives of the study were achieved.

3.3 Population of Study

The populations of the study were employees numbering 106 from the administration of the hospital who comprises of junior level management, middle level management and topmost management in JOOTRH. These categories of employees are ones who interact with BYOD devices in there day to day interaction. They included chief accountant, human resource manager, ICT manager, operations manager, procurement manager

3.4 Sample Design

The study used a sample size Table as cited by Saunders, Lewis and Thornhill (2012) and which uses 95% confidence level and 5% margin of error respectively. According to the Table in a population of 106, a sample of 83 respondents is adequate for the study. Sample size estimation tables as Saunders et.al (2012) further points out are pre-calculated samples from where a sample size can be obtained without the need for further calculations. The study will then use simple random sampling to include the 83 respondents.

3.5 Data Collection

The study employed questionnaire for data collection. All the aspects of the studyôs variables were captured by the structured questionnaire .The questionnaire used a 5 point likert scale that was then be coded for purposes of analysis. Mugenda and Mugenda (1999) assert that the greater use of questionnaire is that it saves time yet can collect a lot of information. Questionnaires also ensure that the study is guided and hence minimize instances of outliers.

3.6 Data Analysis

In the current study, the researcher used descriptive and inferential statistics to analyze the study data. For such reason, the study used frequency and percentage as well as mean and standard deviation. Descriptive statistics as Mugenda and Mugenda (1999) contends, is a data analysis technique that describes the data to draw inferences for purposes of generalization of the study. Regression and correlation were used to draw generalization. The model was as below.

$$Y1 = \beta_0 + \beta_1 X_i + \beta_2 X_i + \beta_3 X_i + \varepsilon_i \quad \text{é é é é é é é é é é é é é é é é .Eq.3.1}$$

Where:

β_0 ï Is the constant or intercept
β_i (i=1,2,3)-Are the regression coefficients
X_1- Independent variable extent of bring your own device usage
X_2- Independent variable challenges of BYOD
Y_i- Dependent variable-information security
ε- Is the error component

CHAPTER FOUR: DATA ANALYSIS, RESULTS AND DISCUSSIONS

4.1 Introduction

This chapter concern itself with data analysis, results and discussions of the subject matter of the study. The study sought to investigate BYOD phenomenon and information security at JOOTRH. The study had two specific purposes which were to establish the extent to which JOOTRH is using bring your own device phenomenon and to determine challenges of using the phenomenon. The total sample size was 83 and so the questionnaires were administered to 83 respondents out of which 73 questionnaires were successfully returned which was a return rate of 88% making it possible to continue with the analysis.

4.2 General Information about Respondents

The general information of respondents were about gender characteristics, age category and level of education

4.2.1 Gender of respondents

The study established that 59% who were male respondents were the majority, and that 41% who were female respondents were the minority. The results are shown in Table 4.1.

Table 4. 1 Gender of respondents

Gender of respondents	Frequency	Percentage
Male	43	59%
Female	30	41%
Total	**73**	**100**

4.2.2 Age of Respondents

According to the study findings, majority of respondents (41%) were within the age bracket of 31 and 43 years. Only 7% of respondents belonged in the age bracket of above 60 years. However, 27% of respondents and 25% of respondents indicated that they fell in the age groups of 18-30 and 44-56 respectively. The results are further shown in Table 4.2.

Table 4.2 Age of Respondents

Age (Years)	Frequency	Percentage
18-30	20	27%
31-43	30	41%
44-56	18	25%
Above 60	5	7%
Total	**73**	**100**

4.2.3 Level of Education

According to Table below, the researcher established that 55% who were the majority of respondents had tertiary level of education. Secondary education level had 18% of respondents indicating that they belonged in the category. Additionally, 27% of respondents indicated that they belonged at the University level of education. The results are further demonstrated in Table 4.3

Table 4. 3 Respondents Level of Education

Level of education	Frequency	Percentage
Secondary education	13	18%
Tertiary level	40	55%
University level of education	20	27%
Total	**73**	**100**

4.2.4 Management Level of Respondents

As demonstrated in Table 4.4, majority of respondents (55%) belonged in the lower level of management. Only 15% of respondents belonged in the upper level of management while 30% of respondents belonged in the middle level of management structure.

Table 4. 4 Management level of respondents

Management level	Frequency	Percentage
Lower management	40	55%
Middle level management	22	30%
Upper level management	11	15%
Total	**73**	**100%**

4.3 Extent of Using Bring Your Own Device Phenomenon

The researcher sought to know the extent of using the bring your own device in terms of the devices used, ownership of the device, access of internet, and regularity of usage

4.3.1 Types of Devices Used

As shown in Table 4.5, mobile phones were used by the majority of respondents at 50.9% followed by Tablets at 20.5% in that order. Laptop and ipad tied at 13.7% of usage.

Table 4. 5 Types of devices used

Device type	Frequency	Percentage
Tablet	15	21%
Mobile phone	38	51%
laptop	10	14%
IPad	10	14%
Total	**73**	**100**

4.3.2 Ownership of the Device

Table 4.6 shows ownership of the devices used for work

Table 4. 6 Ownership of the device

Ownership of the device	Frequency	Percentage
No	13	18%
Yes	60	82%
Total	**73**	**100**

4.3.3 Internet Access

The researcher also sought to determine whether or not respondents get access to internet and the results were demonstrated in Table 4.7

Table 4. 7Internet Access

Ownership of the device	Frequency	Percentage
No	3	4%
Yes	70	96%
Total	**73**	**100**

4.3.4 Regularity of device Usage

The study results as shown in Table 4.8 indicate that always usage of bring your own device had a mean of 4.21 and a standard deviation of 0.021 while using the devices had 4.32 and 0.021 as mean and standard deviation. Usage in rare situations had 3.33 and 0.341 as mean and standard deviation respectively. A mean of 2.28 and 0.251 as standard deviation had never been attained.

Key

To a small extent =1	To some extent = 2	To a moderate = extent 3	To a great extent = 4	To a very great extent = 5

Table 4. 8 Regularity of device usage

Item for response	N	Min	Max	Mean	Std. Deviation
Always	73	1	5	4.21	.021
Sometimes	73	1	5	4.32	.232
Rarely	73	1	5	3.33	.341
Never	73	1	5	2.28	.251
Total	**73**	**1**	**5**	**3.535**	**0.845**

4.4 Challenges of Bring Your Own Device

The researcher also sought to determine challenges of bring your own device. The results were as put in Table 4.9. According to Table 4.9, limited storage for data handling had a mean of 2.98 and

a standard deviation of 0.102 while poor network challenge had a 3.77 and 0.401 as mean and standard deviation. Slow down as a result of virus attack had a standard deviation of 0.042 and a mean of 4.22 while vulnerability as a result of weak password had a 2.78 and 0.504 as mean and standard deviation. Malicious access to device had 3.42 and 0.352; unauthorized access to confidential information had a mean of 2.98 and a standard deviation of 0.231. Theft of enterprise information had a mean of 2.88 and a standard deviation of 0.421 while loss of device with important information had 2.54 and 0.421 as mean and standard deviation respectively. Disruption of internet access due to poor signal strength had 4.81 and 0.323 as mean and standard deviation

Key

To a small extent =1	To some extent = 2	To a moderate extent = 3	To a great extent = 4	To a very great extent = 5

Table 4. 9 Bring your own device

Statement	N	Min	Max	Mean	Std. Deviation
Limited storage space of your device to handle organization data	73	1	5	2.98	.102
Poor network coverage that makes the device not to function well	73	1	5	3.77	.401
Virus attack to your own device that slows performance	73	1	5	4.22	.042
Weak password on devices that are easily cracked by hackers	73	1	5	2.78	.504
Malicious access to your device that leads to manipulation of data	73	1	5	3.42	.352
Unauthorized access to confidential information	73	1	5	2.98	.231
Theft of enterprise information	73	1	5	2.88	.901
Loss of device with important information	73	1	5	2.54	.421
Disruption of internet access due to poor signal strength	73	1	5	4.81	.323
Overall mean and Standard deviation	**73**	**1**	**5**	**3.376**	**.364**

4.5 Information Security

Table 4.10 shows that exposure to confidential information by unauthorized person scored a mean of 2.91 and a standard deviation of 0.122 while virus attack on the device due to access of entrusted sites had 4.61 and 0.901 as mean and standard deviation respectively. On the other hand weak password on the device that is easily accessible had a mean of 2.98 and a standard deviation

of 0.022 while theft of enterprise information had 3.21 and 0.604 as mean and standard deviation. Loss of device had a mean of 3.45 and a standard deviation of 0.522 respectively. Similarly, lack of proper security guidelines laid down by the organization on the usage of your own device phenomenon had 2.82 and 0.421 as mean and standard deviation. In terms of the organization not offering regular training workshops to familiarize employees with the latest security updates in safe handling of devices, the mean was 4.21 while the standard deviation was 0.013 in that order.

Key

To a small extent =1	To some extent = 2	To a moderate = extent 3	To a great extent = 4	To a very great extent = 5

Table 4. 10 Information Security

Statement	N	Min	Max	Mean	Std. Deviation
Exposure to confidential information by unauthorized person	73	1	5	2.91	.122
Virus attack to the device due to accessing entrusted sites	73	1	5	4.61	.901
Weak password on the device that is easily accessible	73	1	5	2.98	.022
Theft of enterprise information	73	1	5	3.21	.604
Loss of device	73	1	5	3.45	.522
Lack of proper security guidelines laid down by the organization on usage of your own device	73	1	5	2.82	.421

Organization not offering regular training workshops to familiarize with the latest security updates in safe handling of our devices	73	1	5	4.21	.013
Overall mean and Standard deviation	**73**	**1**	**5**	**3.456**	**0.400**

4.6 Effect of Bring Your Own Device In Information Security

The model summary in Table 4.11 indicate that the coefficient was ($R^2 = 0.478$) and the model was good given the significant positive F statistic.

Table 4. 11 Summary of the Model

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics					Durbin-Watson
					R Square Change	F Change	df1	df2	Sig. F Change	
1	.659[a]	.478	.456	.55771	.479	21.969	3	67	.000	2.341

a. Predictors: (Constant), extent of bring your own device, challenges of bring your own device mean score business skills
b. Dependent Variable: Information security

Table 4.12 shows that F (3, 67) = 21.969, $p < 0.01$ implying that the model was fit for use and that the independent variables explain information security.

Table 4. 12: ANOVA Results

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	22.321	3	7.171	21.969	.000[b]
Residual	23.320	67	.322		
Total	45.641	69			

a. Dependent Variable: performance of youth enterprise development fund

Table 4.13 shows that the extent of using bring your own device had a significant positive effect on information security (β =0.423, p< 0.05) while challenges of bring your own device phenomenon had negative insignificant influence (β = -0.184, p< 0.05) on information security. The results indicate that BYOD increased information security in organization, however, challenges of using BOYD did not have any significant influence on information security in organizations

Table 4. 13: Regression Coefficients

Model	Unstandardized Coefficients		Standardized Coefficients	T	Sig.	95.0% Confidence Interval for B		Co linearity Statistics	
	B	Std. Error	Beta			Lower Bound	Upper Bound	Tolerance	VIF
(Constant)	1.211	.319		4.174	.000	.711	1.924		
1.Extent of usage mean score	.311	.086	.423	3.471	.001	.122	.513	.377	2.414
2.challenges mean score	-.135	.074	-.184	-1.484	.112	-.291	.053	.426	2.325

a. Dependent Variable: performance of youth enterprise development fund

4.7 Discussion of Findings

On the demographics, the male respondents were 59% while female respondents were 41% indicating that the researcher was not biased and that responses were received from both gender hence reliability of generalization. All the respondents (100%) were also at least 18 years and above demonstrating they were mature and dependable to be used for generalization. Similarly, all respondents (100%) had formal education meaning that the respondents had the capacity to read and understand the questionnaire and thus provide responses which were then used for generalization and hence reliability. In addition 55% of respondents were from lower level of management while 30% were from middle level management with only 15% from upper management meaning that all levels of management were covered hence reducing the bias of generalization.

The study also pursued to establish the extent of using bring you own device at JOOTRH. The study established that the usage bring your own device was to a greater extent given that 82% of respondents indicated that they use the devices always or sometimes. The study also established that the impactful positive influence the extent of the usage of information security had on information security (β =0.423, p< 0.05). This finding is supported by a study conducted by Obonle (2015) who established that the prevalence of usage of information technologies affected information security. The study supports technology acceptance theory that states that the only possible way of application of information technology is on the basis of easiness of use and the usefulness of the particular information technology. Therefore, the study creates new knowledge which was hitherto missing on the extent of use of BYOD and its effect on information security in health institution.

The study also sought to establish challenges of bring your own device within JOOTRH and the study establish that the challenges were significant given the overall mean of 3.376 and that the responses were consistent given the low standard deviation. Further, the study established that challenges of bring your own device phenomenon had negative insignificant influence (β = -0.184, $p < 0.05$) on information security. The study therefore supports protection motivation theory which posits that the basis of using any technology is for the purposes of coping and ability to tackle the threats. Therefore, it can be deduced that because of the inability to tackle threats or coping with the challenges, the insignificant negative correlation was achieved. The discovery is reinforced by the study conducted by Henshel, Flora, Cains, Hoffman and Sample (2018) who established that information security challenges negatively affected organizations. The study therefore creates new knowledge on the effect of challenges of bring your own device on information security.

CHAPTER FIVE: SUMMARY, CONCLUSIONS, RECOMMENDATIONS, LIMITATION OF THE STUDY

5.1 Introduction

This final chapter of the reports handled the summary of major findings, conclusions and recommendations. It also tackled limitations of the study.

5.2 Summary

The study sought to establish the extent to which bring your own phenomenon is used at JOOTRH and the study established that bring your own device is used to a great extent with an overall mean being 3.535 and that the usage was consistent across management levels. The study further established that the extent of using bring your own device phenomenon significantly and positively influenced information security (β =0.423, p< 0.05).

The study also established the challenges of using information security. As such the challenges of using information security were explained by an overall mean of 3.535 which was significant. The study further established that challenges of bring your own device did have any significant effect on information security (β = -0.184, p< 0.05).

5.3 Conclusion

The study concludes that using bring your own device phenomenon increases information security in organizations. Greater extents of using bring your device therefore plays a role on information security. Challenges of bring your own device does not play a key significant role on information security at JOOTRH. Further, the study concludes that the effect of bring your own device phenomenon is explained by 47.8% variation of information security.

5.4 Recommendations

Having researched exhaustively JOOTRH should continue using bring your device and streamline the phenomenon to make it more robust. The study also recommends that JOOTRH should not spend a lot of resources on mitigating challenges of bring your own device and instead such resources should be directed at buying more equipment that enhance bring your own device. The study further recommends that other researchers should look at bring your own device phenomenon in financial institutions where data security is also a priority.

5.5 Limitation of the Study

Use of small sample was a limiting factor as 83 questionnaires were administered but only received feedback from 73 respondents. Although the sample helped in providing reliable generalization, it can only be generalized within the geographical scope of the study. The limitation was however reduced by using scientific method. Research by its very nature is scientific and thus some aspect of the generalization may find application outside the scope of the study.

REFERENCES

Akin-Adetoro, A. (2016). Bring your own device (BYOD) adoption in South African small and medium enterprises. Unpublished thesis.University of Cape Town. South Africa.

Alali, S.I. (2015). *Factors affecting strategy implementation at St. Monica hospital Kenya*. Unpublished research project. University of Nairobi, Kenya

Alsaleh, M., Alomar, N., &Alarifi, A (2017). Smartphone users: understanding how security mechanisms are perceived and new persuasive methods. *Plos One* 12(3):e0173284

Askar, M.A., &Shen, K.N. (2016).*Understanding bring your own device (BYOD) and employee information security behaviors from a work-life domain perspective*. A paper presented at the Twenty-second American Conference on Information Systems, San Diego (1-10). United States of America

Carsteins, D.S., & McCauley-Bell, P.R. (2004). Evaluation of the human impact of password authentication practices on information security. *Information Science Journal* 7(2004):67-85

Chuttur, M.Y. (2009). Overview of the technology acceptance model: origins, development and future directions. *Sprouts: Working Paper on Information Systems* 9(37)9-37

Colwill, C. (2009). Human factors in information security: the inside threat- who can you trust these days? *Information Security Technical Report* 14(4):186-196

DeShield, L. (2017). *The challenges of implementing Bring Your Own Device*.Unpublished project.College of Technology and management. Walden University, United States of America

Faghani, M.R., & Nguyen, U.T., (2017). Modelling the propagation of Trojan malware in online social networks.*Transaction on Dependable and Secure Computing* 15(2017):1-18

Gupta, A., &Dhami, A. (2015).Measuring the impact of security, trust and privacy in information sharing: a study on social networking sites.*Journal of Direct, Data and Digital Marketing Practice* 17(1):43-55

Harris, M.A., Brookshire, R., Patten. K.P., & Regan, E.A. (2015).*Mobile application installation influences: have mobile devices users become desensitized to excessive permission requests*. Unpublished research. University of South Carolina, United States of America.

Kamau, W.T. (2013). *The bring your own device phenomenon: balancing productivity and corporate data security.*Unpublished project. University of Nairobi, Kenya.

Kimathi, L. (2017). Challenges of the devolved health sector in Kenya: teething problems or systemic contradictions? *Africa Development* 42(1):55-77

King, Z.M, Henshel, D.S., Flora, L., Cains, M.G Hoffman, B., & Sample, C. (2018). Characteristics and measuring maliciousness for cyber security risk assessment. *Frontiers in Psychology* 9:39 doi:10.3389/fpsy.2018.00039

Kothari, C.R. (2004). *Research methodology: methods and techniques*. 2nd Edition, New Age International Publishers, New Delhi

Li, Y., (2017). *Information Security Research: external hacking, inside breach, and profound technologies.*Unpublished thesis.Iowa State University.United State of America.

Magruder, J.S., Lewis, S.X., Burks, E.J., &Smolinski, C. (2015). Bring your own device (BYOD) - who is running organizations? *Journal of Accounting and Finance* 15(1):55-61

Maillart, T., Zhao, M., Grossklags, J., & Chuang, J. (2017). Given enough eyeballs, all bugs are shallow? Revisiting Eric Raymond with bug bounty programs.*Journal of Cyber Security* 3(2):81-90

Mbenywe, M. (2018, September 29). Kisumuôs main referral hospital sick without beds and nurses *Standard*

*Digital*https://www.standardmedia.co.ke/article/2001297262/shocking-story-of-nyanza-s-ailing-hospital

Medani, A., Zakaria, O., Gani, A., &Zaidan, A. A. (2011). Review of mobile short message service security issues and techniques towards the solution. *Scientific Research and Essays* 6(6):1147-1165

Mugenda, O.M., &Mugenda A.G. (1999).*Research methods: quantitative and qualitative approaches*. Nairobi: Acts Press

Muinga, N., Magare, S., Monda, J., Kamau, O., Houston, S., Fraser, Sé .Paton, C. (2018).Implementing an open source electronic health record system in Kenya health care facilities: case study.*Journal of Medical Internet Research Medixcal Informatics* 6(2):e22 doi: 10.2196/medinform.8403

Obonle, E.M (2015). *The influence of mobile devices on network security*.Unpublished thesis.Lagos State University. Nigeria

Oketch, A. (2015, September 17). Jaramogi hospital plans revival with sh.100 billion facelift. *Business Daily*.https://www.businessdailyafrica.com/news/Jaramogi-Hospital-plans-revival-with-Sh100bn-facelift/539546-2875132-mtjd0m/index.html

Olaler, M., Abdullah, M.T., Mahmood, R., & Abdulla, A. (2015). A review of bring your own device on security issues. Sage Open 1-11 doi: 10.1177/2158244015580372

Saini, S., & Sharma, Y.K., (2016).A research study of wireless network security.*International Journal of Advance Research in Computer Science and Software Engineering* 6(3):473-479

Salahdine, F., &Kabouch, N. (2019). Social engineering attacks: a survey. *Future Internet Review*. 11(89):10.3390/fi11040089

Scherer, R., SIddiq, F., &Tondeur, J. (2019). The technology acceptance model (TAM): a meta-analytic structural equation modeling approach to explaining teachersô adoption of digital technology in education. *Computers and Education* 128(2019):13-35

Saunders, M., Lewis, P. &Thornhill, A. (2012).*Research methods for business students 9th*ed). London: Prentice Hall.

Wabende, S.M. (2014). *The influence of Malware threat on information security*.Unpublished thesis. Kenyatta University, Kenya

Wangatusi, G.N.M. (2013). *An exploration on how bring your own device user behavior impacts on an organization's information security: a case study of Madison Insurance Company Kenya Limited*. Unpublished project. University of Nairobi, Kenya.

Wanyonyi, E., Rodrigues, A., Abeka, S., &Ogara, S. (2017). Effectiveness of security controls on electronic health records. *International Journal of Scientific and Technology Research* 6(12):47-54

Westcott, R., Ronana, K., Bambrick, H., & Taylor, M (2017). Expanding protection motivation theory: investigating an application to animal owners and emergency responders in bushfire emergencies. *BMC Psychology* 5(1) doi.org/10.1186/s40359-017-0182-3

APPENDIX: QUESTIONNAIRE

SECTION A: DEMOGRAPHIC OF RESPONDENTS

In this section, tick the choice that best represents your characteristics. Give as honest answers as possible. The responses will only be used for academic purposes. Donâ provide your name.

1. Which gender do you identify with?

Female [ ]
Male [ ]

2. What is your age category in years?

18-30 [ ]
31-43 [ ]
44-56 [ ]
Above 60 [ ]

3. What is your level of education?

Secondary education [ ]
Tertiary education [ ]
University education [ ]

4. What is your job category?

Lower management [ ]
Middle management [ ]
Upper management [ ]

SECTION B: EXTENT OF USING BRING YOUR ON DEVICE

In this, please provide your response in the space provided by ticking one of the boxes; kindly provide response which is honest as possible

1. Which of the following devices do you use for work? (*you can tick more than one on the usage section*)

No.	Device	Usage
1	Tablet	
2	Mobile phone	
3	laptop	
4	Ipad	

2. Do you own the device that you use to discharge your duties?

Yes	No

3. Do you access the internet with the device that you use for work?

Yes	No

4. To what extent do you use your own devices at work?

Always	
sometimes	
Rarely	
Never	

SECTION C: CHALLENGES

To what extent do you agree that the following could be a challenge to the usage of your own device at work? Please tick where appropriate

1= **to a small extent** 2= **to some extent**

3= **to a moderate extent** 4= **to a great extent** 5= **to a very great extent**

Statement	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
Limited storage space of your device to handle organization data					
Poor network coverage that makes the device not to function well					
Virus attack to your own device that slows performance					
Weak password on devices that are easily cracked by hackers					
Malicious access to your device that leads to manipulation of data					
Unauthorized access to confidential information					
Theft of enterprise information					
Loss of device with important information					
Disruption of internet access due to poor signal strength					

SECTION D: INFORMATION SECURITY

To what extent does the following pose as security issue in your organization?

1= **to a small extent** 2= **to some extent**

3= **to a moderate extent** 4= **to a great extent** 5= **to a very great extent**

Statement	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
Exposure to confidential information by unauthorized person					
Virus attack to the device due to accessing entrusted sites					
Weak password on the device that is easily accessible					
Theft of enterprise information					
Loss of device					
Lack of proper security guidelines laid down by the organization on usage of your own device					
organization not offering regular training workshops to familiarize with the latest security updates in safe handling of our devices					