THE IMPACT OF BRING YOUR OWN DEVICE (BOYD) AND NOMADIC COMPUTING ON ENTERPRISE SECURITY POLICIES' COMPLIANCE: THE CASE OF HIGHER LEARNING INSTITUTIONS IN KENYA.

EDWIN NG'ANG'A WANGARI

ICT-G-4-0527-17

A RESEARCH STUDY SUBMITTED TO THE SCHOOL OF COMPUTING AND INFORMATICS IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF BACHELOR IN COMPUTER SCIENCE OF GRETSA UNIVERSITY.

January, 2023

DECLARATION

I declare that this is my original work and I have done to the best of my knowledge. It has not been submitted to any other institution of higher education anywhere. The sources that I have used have been acknowledged by references.

NAME..Hagaai Edwin Ngang'a

SIGNATURE: ..

DATE: ...11/12/2023.....

SUPERVISOR: This proposal has been submitted with my approval as the University supervisor.

SIGNATURE: .....

DATE: 11/12/2023

LECTURER: .....Peter Siele

School of computing and informatics.

Gretsa University.

ii

ACKNOWLEDGEMENT

I thank the Almighty God for the guidance, clarity of mind, wealth of ideas and the ultimate support from the departure of this journey until its fulfilment.

My gratitude to my supervisor, Mr Philip Bittok for guidance and encouragement throughout the process of coming up with this business plan project.

DEDICATION

I dedicate this business plan to God with every reason for its fulfilment is all because of his everlasting grace. I also dedicate this work with lots of love and appreciation to my parents, friends and family, who gave me their absolute support throughout this period.

TABLE OF CONTENTS

ABSTRACT

Mobility is driving network design, and as such, wireless local area networks (WLANs) have become an important part of enterprise networks in today's business environment. A trend is emerging where consumer adoption of smartphones and tablets is exploding due to their low price and the broad application support that these devices offer because they are Wi-Fi enabled. Desktop computers and laptops are used to gather information; while tablets consume information and smartphones communicate that information. BYOD (Bring Your Own Device) is a term that refers to instances where employees use their personal computing devices (usually smartphones, tablets, and laptops) in the workplace. This trend will continue, and the challenge is that it is a double-edged sword: user satisfaction and productivity on the one hand and enterprise data security on the other. As more employees want to access corporate networks with their personal mobile devices, vendors need to find ways to help companies provide that access in a secure and efficient manner. This is due to the fact that technology is changing very fast and with the consumerization of the IT revolution, there has been a cultural shift, so the users are the ones who get the latest cutting-edge technologies first and want to get these devices working. BYOD is changing the security model for protecting corporate data, blurring the definition of this perimeter by physical location and asset ownership. In this study, bring your own device (BYOD) and nomadic computing were examined for corporate security compliance in HLIs in Africa. A quantitative survey approach was used at ten university campuses to identify BYOD security compliance issues. The study found that Perceived probability of security breach, Perceived severity of security breach, security breach concern level and response efficacy had an impact on Enterprise Security Policies' Compliance in an enterprise.

CHAPTER ONE: INTRODUCTION

1.1. Background to the Study

In today's business environment, mobility drives network design, and wireless local area networks (WLANs) have become an important part of enterprise networks. A trend is emerging where consumer adoption of smartphones and tablets is exploding due to their low price and the broad application support that these devices offer because they are Wi-Fi enabled. Desktop computers and laptops are used to gather information; While tablets consume information and smartphones communicate that information. Businesses are demanding greater productivity from their employees due to advances in technology. This requires strong flexibility in information technology (IT) policies that enable the secure use of personal and mobile devices at work to increase employee productivity and create significant competitive advantages. In such scenarios, BYOD is an attractive option for companies (EY, 2013).

The number of mobile devices continues to grow exponentially. Available statistics indicate that the number of mobile devices will be around 10 billion in 2018. This equates to 1.5 mobile devices for every person on the planet (EY, 2013). These devices are becoming increasingly integrated into all areas of our personal lives and as a result, companies must allow their employees to use their own personal mobile devices for work-related activities alongside company-provided devices, including desktop computers and laptops. In such a scenario, employers cannot prevent the use of mobile devices for both business and personal purposes, but need to know how to control them. One of the reasons for the exponential growth of these devices is attributed to the fact that in most companies, Generation Y makes up a large part of their workforce. These employees are technology-hungry and savvy individuals interested in exploring and trying new technologies as they come to market (Kamau, 2013). The rapid growth and advancement of technological innovations and inventions in the IT sector has dramatically changed the IT model where IT managers controlled who could access corporate data using company-provided devices. With the consumerization of the IT revolution, there has been a cultural shift such that the users are the ones acquiring the latest, cutting-edge technologies first, and they want to accompany those devices to work. The use of BYOD in the company premises significantly improved productivity in the workplace (Cisco, 2014). This is because employees are typically familiar with their own devices, rather than the ones the company provides them with. Due to the familiarity with their own devices, job satisfaction among employees tends to be high. A study conducted by (Mbalanya, 2013) found that the biggest factor that led companies to adopt BYOD on the Nairobi Stock Exchange (NSE) was

improved employee productivity and efficiency. Similar studies on the factors influencing the adoption of BYOD devices in the workplace have shown that demand for flexible working hours, end-user demand, employee morale increases, employee productivity and efficiency improves, the overall cost of IT infrastructure is reduced and capital and IT expenses decrease Devices as the main driver for the adoption of BYOD devices in the workplace (Mbalanya, 2013) (Kamau, 2013) (Company85, 2014). BYOD trends are significantly changing the security model for protecting corporate data, blurring the definition of this perimeter with physical location and asset ownership (EY, 2013). Since these devices can now be used for data processing by enterprises; Enterprises must formulate policies to control the impact of security threats and establish normative procedures and support models that balance employee needs and security concerns. Prematurely adopting BYOD in an enterprise environment introduces security risks that need to be addressed, otherwise the security of the very assets a company needs to protect can be compromised.

1.2. Statement of Research Problem

According to (Gessner, Girao, Karame and Li, 2013) security challenges associated with BYOD include: loss of bandwidth and productivity, data and device loss, attacks on mobile devices, and policies to secure BYOD. The fact that mobile devices are not subject to the same security policies as desktop devices has contributed to bandwidth and productivity losses as more employees use mobile devices instead of desktop computers to access the corporate Internet within enterprise. For example, employees can use their mobile devices to access services such as video streaming and other applications that are denied by standard corporate security policies. As a result, the bandwidth of the corporate network is heavily burdened and a bottleneck is created, which reduces the productivity in this enterprise (Gessner, Girao, Karame and Li, 2013). The BYOD movement started ten years ago in Higher Learning Institutions (HLIs). This was encouraged by Generation Y students, who demanded the use of their personal devices on campus. The university administration was aware that enabling internet access via mobile devices could improve the educational experience of these students. The Center for Digital Education (CDE) survey of nearly 150 IT professionals in the K-20 education found that 85 percent of faculty and staff bring a personal device (laptop, tablet, or smartphone) to work that they use to access the access the network of your school or university (e.Republic, 2013). BYOD devices with 3G (Third Mobile Generation Networks) and 4G (Fourth Mobile Generations Networks) Internet access may bypass facility security features. Not only does this potentially increase the risk of spreading viruses on school networks, but it

can also lead to attempts to access student administrative files and e-mail. Therefore, educational institutions implementing BYOD must take steps to address privacy, security, and regulatory concerns. Allowing personal devices to access the network can lead to privacy and data security breaches, as student and staff devices may lack the necessary protections and features to ensure information security. With all the risks BYOD brings, it's clear that a shift in strategy is required to enable HLIs to protect their assets and remain secure. IT administrators in the HLIs need to identify the potential BYOD risks in order to put in place mechanisms that can mitigate those risks. In Kenya, the available literature on BYOD trends shows that the majority of research focuses on BYOD trends in enterprises and other enterprises. Minimal research has been conducted to determine the level of security implementation of BYODs in HLIs.

1.3. Purpose of the Study

This study examined this trend of bring your own device (BYOD) and nomadic computing in terms of corporate security compliance in HLIs.

1.4 Conceptual Framework

Dependent Variables Independent-variable.

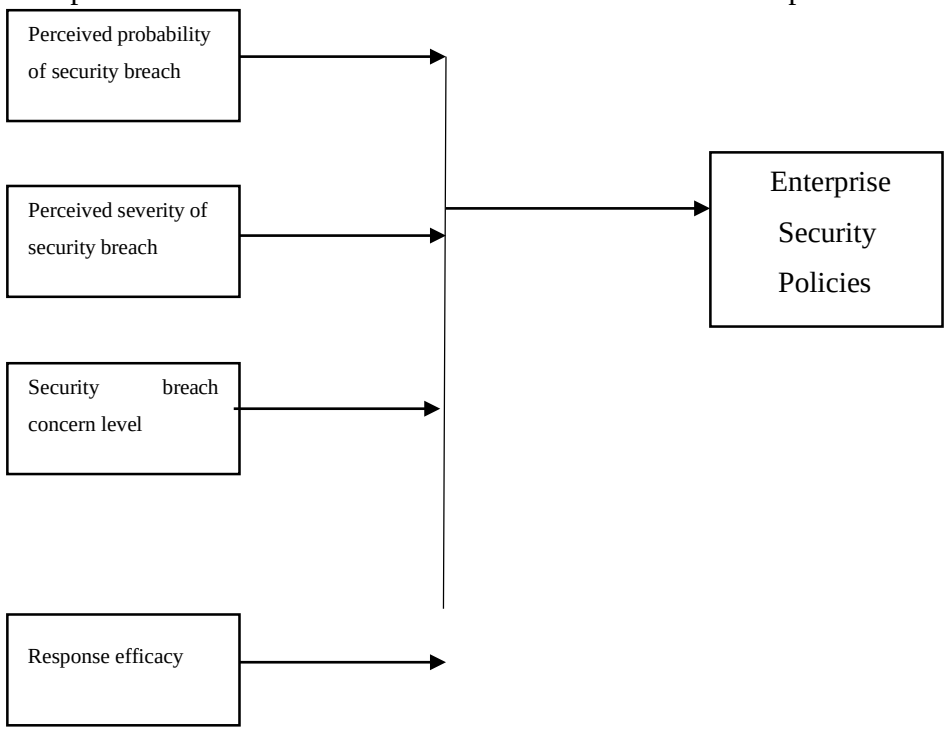


Figure 1 Conceptional framework

1.5 Research Questions

The study was conducted to answer the following specific research questions:

1.What is the perceived probability of security breach?

2.What are the security breach concern levels?

3.What are the security policy compliance intentions?

1.6 Objectives of the Study

1.6.1 General Objective

To ascertain BYOD and Nomadic computing on Enterprise security policies' compliance in HLI's.

1.6.2 Specific Objectives

The objectives below guide the study:

1. To determine the extent of awareness to which BYOD and nomadic computing security risks to HLI's IT systems in Kenya.
2. To investigate factors that lead IT Administrators in HLIs enforce BYOD security policies with a view to understanding BYOD security compliance in a more holistic manner.

1.7 Hypotheses of the Study

H_1: The perceived probability of a security breach will positively affect the level of BYOD security breach concern by IT Administrators in HLIs.

H_2: The perceived severity of a potential security breach will positively affect the level of BOYD security breach concern by IT Administrators in HLIs.

H3: Higher levels of security breach concern levels by IT Administrators in HLIs will result in more positive attitudes effecting towards BYOD security policies.

H4: The perceived effectiveness of users' actions with IT in HLIs will positively affect one's attitude towards BYOD security policies.

1.8 Significance of the Study

The contributions from the validated and proposed research solutions are:

1. The network performance analysis will help the network administrator enhance their network performance faster and more effectively.

2. The network will be more manageable, and traffic conditions will be much better, improving network capability.

3. The bandwidth usage assessments determine whether the bandwidth usage for each application is sufficient and thus meets the needs and requirements of the users.

1.9 Scope of the Study

The study is aimed at developing security policies and monitoring network performance in higher learning institutions.

1.10 Limitations of the Study

The study is limited to developing and implementing algorithm dynamically for queuing mechanisms due to limitations of time, cost and complexity.

CHAPTER TWO: LITERATURE REVIEW

2.1. Theoretical framework(s)

In order to establish an appropriate theoretical framework that can explain the rationale for implementing BYOD security measures in an enterprise, it is important to understand what constitutes BYOD and nomadic computing risks and prevention. The theoretical framework used for this study was the Protection Motivation Theory (PMT), from which appropriate constructs for potential BYOD and nomadic computing threats and risks were created. Protection motivation theory (PMT) was developed by (Rogers and Prentice-Dunn, 1997) to understand fear appeal communication intended to influence attitude and behavior changes. According to this theory, fear appeal refers to communication that describes adverse consequences of not conforming to a communicator's recommendation. This theory posits that cognitive appraisal would mediate the effect of fear appeal components on attitude change by arousing protective motivation. Protection motivation consists of two processes: threat assessment and coping assessment (Norman, Boer and Seydel, 2005). Threat assessment is a process for assessing mismatch behavior. These include a response reward (benefit of maladaptive behavior) and a perception of threat (severity and vulnerability). The coping assessment is a process of assessing the ability to deal with and eliminate the threat. This process includes response effectiveness, self-efficacy, and response costs (Putri and Hovav, 2014). The theory suggests that assessing the impact of the security threat and the likelihood of being exposed to a significant security threat from BYOD and nomadic computing may or may not result in employees formulating security policies that control the same risks. Another process central to protection recruitment is the coping assessment. This assesses the effectiveness of the response, the cost of the response, and self-efficacy. Response effectiveness relates to the belief that the recommended coping response will be effective in reducing the threat. Response cost is the assumption of how expensive it will be to carry out the recommended response.

2.2. Review of BYOD and Nomadic computing

In recent years, there has been an explosion in technology that has led to the consumerization of IT (Mbalanya, 2013). As a result of this explosion, devices and services that were once only available in the workplace and provided by IT departments are now widely available and affordable to consumers. This has been fueled by the introduction of devices such as the Apple iPhone and iPad, and Google Android smartphones and tablets. The lower cost of these devices has increased consumer appetites for the latest technology. This is what BYOD and nomadic

computing are bringing to the workplace. In BYOD and nomadic computing scenarios, companies want to integrate their employees' mobile devices into business processes (e.g., reading e-mails, editing documents) (Gessner, Girao, Karame and Li, 2013). The BYOD movement began ten years ago in Higher Learning Institutions (HLIs). This was encouraged by Generation Y students, who demanded the use of their personal devices on campus. The university administration was aware that enabling internet access via mobile devices could improve the educational experience of these students. The Center for Digital Education (CDE) survey of nearly 150 IT professionals in the K-20 education found that 85 percent of faculty and staff bring a personal device (laptop, tablet, or smartphone) to work that they use to access the access the network of your school or university (e.Republic, 2013).

2.3. BYOD and Nomadic computing Security Policies' Compliance Issues

The following compliance issues are identified in the available literature on the impact of BYOD and nomadic computing on corporate security compliance:

2.3.1. Perceived probability of security breach

Employees who believe that a security threat could cause significant harm or disruption are more likely to be concerned about enforcing security measures than employees who do not believe that a security threat could cause significant harm or disruption. Such employees are unlikely to be concerned. This means that when employees perceive the threat as real, they are concerned and are more likely to have a more positive attitude towards protection mechanisms such as security policies (Rogers and Prentice-Dunn, 1997). According to (Gessner, Girao, Karame and Li, 2013), the likelihood that a security breach will result in a significant outage resulting in lost productivity, or in a significant Internet outage resulting in financial loss for enterprises, may prompt IT administrators to implement security controls designed to consequence have a deterrent effect. Thus,

H1: The perceived probability of a security breach will positively affect the level of BYOD security breach concern by IT Administrators in HLIs.

2.3.2. Perceived severity of security breach

The perceived severity of a security breach relates to the likelihood that actions taken from outside enterprise will circumvent or violate a security policy, practice or procedure within an enterprise. The question is whether IT administrators believe that the information stored on the organization's computers is vulnerable to security incidents. As a result, employee productivity and organizational profitability decrease. (Singh, 2012) believes that increased incidents of

security breaches will reduce an organization's productivity and profitability by compromising the organization's data. This contradicts the hypothesis that many researchers have put forward regarding increased productivity due to the implementation of BYOD and nomadic computing (Mbalanya, 2013) (Miller,Voas and Hurlburt, 2012)(Burt, 2011). Thus,

H2: The perceived severity of a potential security breach will positively affect the level of BYOD security breach concern by IT Administrators in HLIs.

2.3.3. Security breach concern level

The level of concern about security breaches relates to whether IT admins feel that security issues are directly or indirectly affecting their organization. The level of knowledge of IT administrators is important to determine if they can implement security controls with a deterrent effect. A study conducted by (Herath and Rao, 2009) found that concerns about security breaches have a significant impact on IT administrators' attitudes towards security policies. In this study, IT pros were asked if they thought the IS security issue was overblown (reverse-coded). It has been found to have a significant impact on IT administrators' attitudes towards security policies. This has significant implications for the enforcement of security policies within organizations. Thus,

H3: Higher levels of security breach concern levels by IT Administrators in HLIs will result in more positive attitudes effecting towards BYOD security policies

2.3.4. Response efficacy

According to PMT, response effectiveness defines the beliefs that illustrate whether the recommended coping response is effective in reducing threat. This study examines an employee's perception of the effectiveness of adhering to the organization's computer security policies, which is important for enforcing compliant policies within HLIs. According to (Putri and Hovav, 2014), a security threat includes a threat to employees' mobile devices and corporate computing resources. Therefore, compliance with an organization's BYOD ISSP would be beneficial to the organization and the employee. Therefore,

H4: The perceived effectiveness of users' actions with IT in HLIs will positively affect one's attitude towards BYOD security policies.

2.4. Knowledge Gaps

BYOD trends are significantly changing the security model for protecting corporate data, blurring the definition of this perimeter with physical location and asset ownership (EY, 2013).

As these devices can now be used for data collection by organizations; Organizations must formulate policies to control the impact of security threats and establish normative procedures and support models that balance employee needs and security concerns. Prematurely adopting BYOD in an enterprise environment introduces security risks that need to be addressed, otherwise the security of the very assets a company needs to protect can be compromised. Therefore, educational institutions implementing BYOD must take steps to address privacy, security, and regulatory concerns. Allowing personal devices to access the network can open the door to privacy and data security breaches, as student and staff devices may lack the necessary protections and features to keep information secure. With all the risks that BYOD brings, it's clear that a shift in strategy is required to enable HLIs to protect their assets and remain secure.

IT administrators in the HLIs need to identify the potential BYOD risks in order to put in place mechanisms that can mitigate those risks. In Kenya, the available literature on BYOD trends shows that the majority of research focuses on BYOD trends in enterprises and other enterprises. Minimal research has been conducted to determine the level of security policy implementation of BYODs in HLIs.

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Research Design

To test the above model, we used a survey methodology to collect data. The focus of this study was to examine the impact of bring your own device (BYOD) and nomadic computing on corporate security compliance at higher education institutions in Kenya.

3.2 Study Area

Data was collected from IT administrators at 10 campuses of public and private universities in Kenya.

3.3 Target Population

Based on a targeted sampling technique, a target population of 10 experts from public and private universities in Kenya was considered. These were employees who had acquired knowledge, skills and experience in the ICT sector.

3.4 Sampling Technique

A purposive sampling technique was used to select study participants. The technique was used to ensure fairly equal representation of the variables for the study.

3.5 Sample Size

The sample size targeted population size of 10, that is 10 IT Administrators with a confidence level of 95% and confidence interval of 0.04. Using the Yamane formula; n=N/{1+Ne^2}

where:

n=sample size N=population

size e=acceptable

error=0.05

Therefore, the sample size of the population will be 10.

3.6 Measurement of Variables

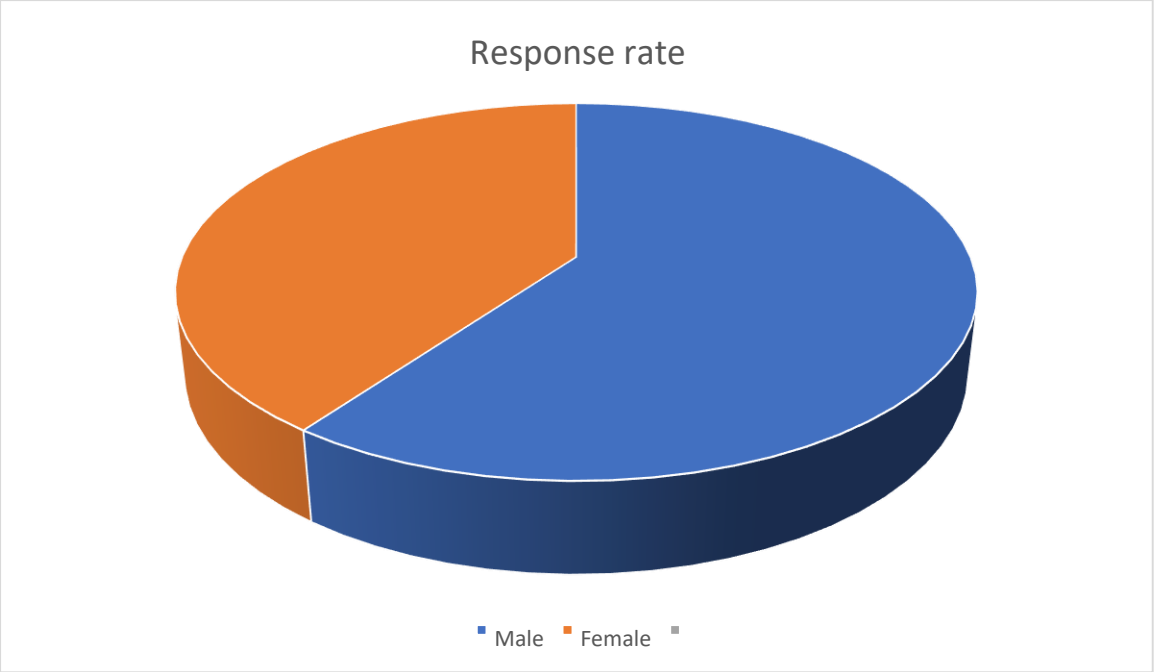
The variables were measured, altered and manipulated where numeric figures were used to classify the data using nominal measurement level and the representation of the variable Traffic utilization was represented on the y-axis to time variable which was represented on the x-axis.

3.7 Research instruments

During the initial survey and the follow-up to the questionnaires, 10 usable answers were generated, which led to a response rate of 100%. This response rate to an unsolicited questionnaire sent by mail indicated that respondents found the topic interesting and relevant. As shown in Table 1, the distribution of subjects was not even: males accounted for 67% and females for 33%.

Table 1: Descriptive statistics of measured items

Gender	Frequency	%Response Rate
Male	6	60
Female	4	40
Total	10	



As shown in Table 2, 10 respondents (100%) showed understanding for the use of BYOD in HLIs. This is attributed to the fact that all respondents in the study had knowledge and experience in the ICT industry. According to the results, a total of 6 respondents (60%) showed an awareness of BYOD and the associated security risks for the IT infrastructure. This high percentage of awareness was due to the fact that the IT administrators in these institutions had knowledge and experience in ICT matters. 3 respondents (30%) of respondents reported a lack of awareness of BYOD and its security impact on corporate assets, while 10% of respondents were unsure of the level of awareness of BYOD and its security impact on IT infrastructure in an organization. The same findings revealed that only 3 out of 10 campus locations had a

corporate BYOD security policy. The majority of campuses (6 out of 10) in the study had no BYOD corporate security policies in place.

Table 2: Level of understanding of BYOD and security implications on IT infrastructure

Measured items	Yes	No	Not Sure	Total
Understanding of BYOD	10	0	0	10
Extent of awareness of BYOD and security risks it poses to IT infrastructure	6	3	1	10
Whether there exists a BYOD policy on enterprise security in the institution	3	6	1	18
Total	19	9	2	

Source: Research data

3.8 Validity of Measurements

The questionnaire designed for the study underwent a validation process for face and content validity. In the validation process of this study, copies of the questionnaire were emailed to the expert IT Administrators. These experts carefully went through the research questionnaire to determine the adequacy and appropriateness of the instrument. They suggested structuring the questionnaire according to the Likert method, on a five-point scale instead of a modified 4point Likert method. The researcher prefers the modified Likert scale because according to the normal Likert scale, “strongly agree” is 5 points, “agree” is 4 points, “undecided” is 3 points, “disagree” is 2 points, and “strongly disagree”. agree” 1 point awarded. Many researchers and educators feel that there is no logical reason to assign the weight of 3 points to someone who is undecided on a particular question. Therefore, the modified 4-Likert scale is preferred. However, the other useful observations and suggestions made by the experts have been modified and corrected. After validation of the questionnaire, the instrument was piloted using staff representatives from each department in the institutions.

This was done to;

- see how the subject will respond to the questionnaire
- whether the items are clear enough and easy to understand, whether there is a need to include more items in certain areas.
- or whether there are some items to which they do not wish to respond,
- and to determine the practicality of the proposed method of data analysis for the study.

However, due to the pilot testing, the researcher could understand the ambiguity of some items and had done so to modify the questionnaire level. That is, the researcher resorted to plain English.

CHAPTER FOUR: FINDINGS AND DISCUSSIONS

4.1 Introduction

The aim of this study was to determine the level of awareness with which BYOD and nomadic computing bring security risks to the IT systems of HLIs in Kenya and to examine factors that lead IT administrators in HLIs to adopt BYOD security policies enforce to understand BYOD security compliance more holistically. Based on the conceptual framework, the following variables were identified:

a. Perceived probability of security breach
b. Perceived severity of security breach
c. Security breach concern level
d. Response efficacy

This study used both descriptive and inferential statistics to analyze the data. Descriptive statistics used included the use of histograms, frequency tables, and pie charts to represent data. This was useful when comparing groups of different sizes. In the survey, respondents were asked whether the perceived probability of security breach, the perceived severity of security breach, Security breach concern level, and response efficacy had an impact on Enterprise Security Policies' Compliance based on the Likert Scale "totally agree" (SA), "agree" (A)., Undecided (U), disagree (D) and totally disagree (SD). The table below summarizes the descriptive statistics of the measured items based on the Likert scale.

Table 3: Descriptive statistics of measured items

Measured item	SA	A	U	D	SD	Total
Perceived probability of security breach	3	2	2	2	1	10
Perceived severity of security breach	4	3	1	1	1	10
Security breach concern level	5	2	1	1	1	10
Response efficacy	3	2	3	1	1	10
Total	15	8	7	5	3	40

Source: Research data

The results show that 50% of respondents cited the perceived probability of security breach as an indicator of the organization's enforcement of BYOD security compliance. 30% of respondents disagreed that the perceived probability of security breach had an impact on the enterprise's enforcement of BYOD security compliance. These findings reinforce those of

Rodgers and Prentice-Dunn, who found that when employees perceive the threat as real and are concerned, they are more likely to have more positive attitudes toward protection mechanisms such as security policies (Rogers and Prentice-Dunn, 1997). 60% of respondents cited the perceived severity of security breach as an indicator of the enterprise's enforcement of BYOD security compliance. Only 20% of respondents disagreed that the perceived severity of security breach had an impact on the enterprise's enforcement of BYOD security compliance. 60% of respondents cited the perceived severity of security breach as an indicator of the enterprise's enforcement of BYOD security compliance. Only 20% of respondents disagreed that the perceived severity of security breach had an impact on the enterprise's enforcement of BYOD security compliance. This is because if IT administrators believe that the information stored on the enterprise's computers is vulnerable to security incidents, they are likely to take enforcement action since the prospect of lower productivity and lower profits is higher in an organization. 70% of respondents cited security breach concern level as an indicator of how enterprises are enforcing BYOD security compliance. 30% of respondents disagreed that the perceived likelihood of a security breach had an impact on enterprises' enforcement of BYOD security compliance. This high percentage is attributed to the fact that concerns about security breaches have a significant impact on IT administrators' attitudes towards security policies (Herath and Rao, 2009). 50% of respondents cited response efficacy as an indicator of the enterprise's enforcement of BYOD security compliance. Only 20% of respondents disagreed that the response efficacy had an impact on enforcing BYOD security compliance in enterprises. This is because individuals have more positive safety attitudes when they have high perceptions of citizen effectiveness. It is also likely that employees who believe their actions have a positive impact on their organization have more positive attitudes toward security policies (Putri and Hovav, 2014).

4.2 Assessing the Hypotheses Testing

Inferential statistics were used to verify the relationship between Enterprise Security Policies' Compliance with respect to BYOD and nomadic computing characteristics that were identified in the conceptual framework. These included the perceived probability of security breach, perceived severity of security breach, security breach concern level and response efficacy. A number of hypotheses regarding the correlations of some survey variables were tested. These included:

H1: The perceived probability of a security breach will positively affect the level of BYOD security breach concern by IT Administrators in HLIs.

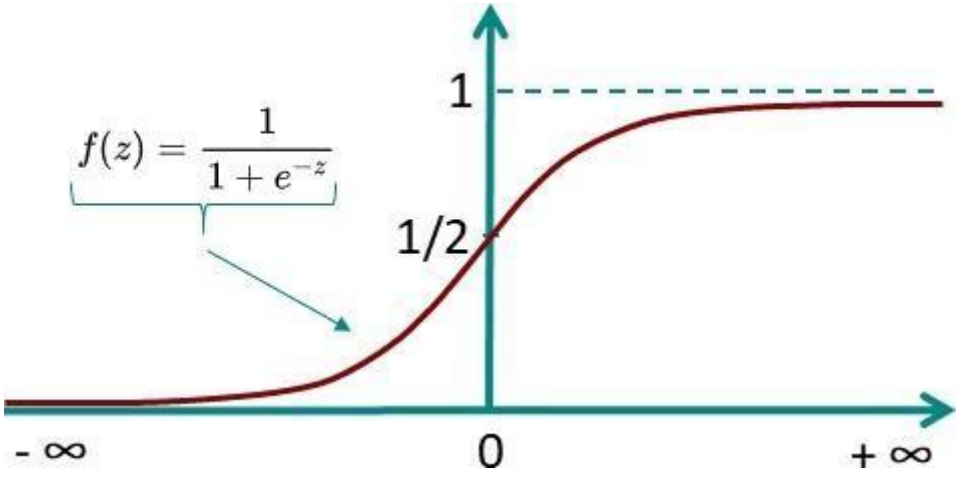
H2: The perceived severity of a potential security breach will positively affect the level of BYOD security breach concern by IT Administrators in HLIs.

H3: Higher levels of security breach concern levels by IT Administrators in HLIs will result in more positive attitudes effecting towards BYOD security policies.

H4: The perceived effectiveness of users' actions with IT in HLIs will positively affect one's attitude towards BYOD security policies.

4.3 Logical Regression model

The logistic model is based on the logical function. The special thing about the logistic function is that for values between minus and plus infinity, it always assumes only values between 0 and 1.

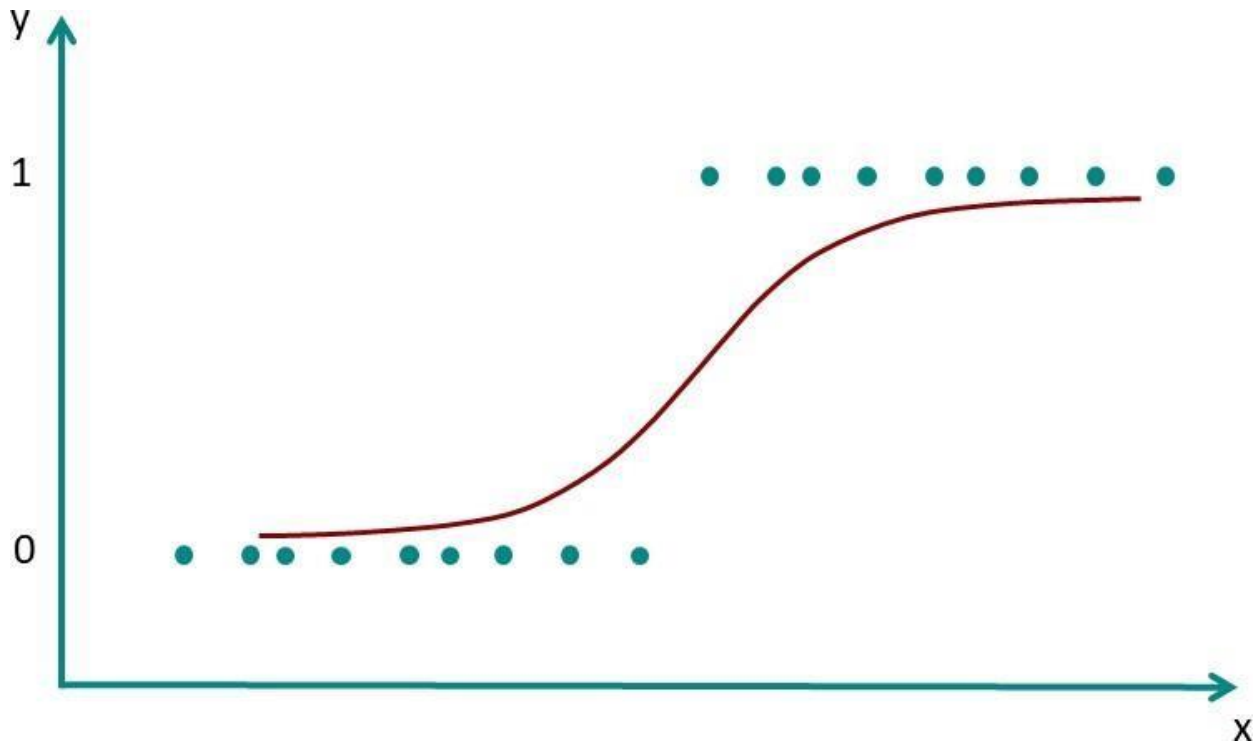


So, the logistic function is perfect to describe the **probability *P(y=1)***. If the logistic function is now applied to the upper regression equation the result is

$$\hat{y} = b_1 \cdot x_1 + b_2 \cdot x_2 + \ldots + b_k \cdot x_k + a$$

$$f(z) = \frac{1}{1+e^{-z}} = \frac{1}{1+e^{-(b_1 \cdot x_1 + \ldots + b_k \cdot x_k + a)}}$$

This now ensures that no matter in which range the x values are located, only numbers between 0 and 1 will come out. The new graph now looks like this:



A logistic regression model was used to predict IT administrators' enforcement of enterprise security policy compliance related to BYOD and nomadic computing in HLIs. Logistic regression was used because it was necessary to predict whether the presence or absence of the perceived probability of security breach, the perceived severity of security breach, security breach concern level and response efficacy would have an impact on the enforcement of a BYOD security policy. The table below summarizes the results of the logistic regression model.

Table 4: Logistic regression analysis

Variable	Beta	Std. Error	Wald	Sig	Exp (β)	Marginal Effect
Perceived probability of security breach	0.109	0.083	6.355	0.012**	0.811	0.096
Perceived severity of security breach	0.239	0.156	3.917	0.008***	1.362	0.049
Security concern level	0.104	0.164	1.075	0.014**	1.185	0.388
Response efficacy	0.139	0.137	1.523	0.097*	1.184	0.336
Constant	2.16	2.212	1.127	0.218	18.93	

*significant at 10% level, **significant at 5%, ***significant at 1%

Source: Research data

The findings show that the estimated coefficient of Perceived probability of security breach was positive and significant at the 5 percent level of significance, implying enforcement and compliance of BYOD security policy increases with increase in Perceived probability of

security breach. Therefore, the null hypothesis that perceived probability of a security breach will positively affect the level of BYOD security breach concern by IT Administrators in HLIs was accepted. The Perceived severity of security breach was positive and significant at 1 percent level of significance, implying that the probability of enforcement and compliance of BYOD security policy increases with increase in Perceived severity of security breach. The marginal effect result shows that, holding the other factors constant, the probability of enforcement and compliance of BYOD security policy increases by 4.9 percent when the IT administrators understand the effect of perceived severity of security breach in an institution. Therefore, the null hypothesis that the perceived severity of a potential security breach will positively affect the level of BYOD security breach concern by IT Administrators in HLIs was accepted. The estimated coefficient of security concern level was positive and significant at the 5 percent level of significance, implying that the probability of implying enforcement and compliance of BYOD security policy increases with increase in security concern level awareness by IT administrators. The marginal effect result shows that, holding the other factors constant, the probability of enforcement and compliance of BYOD security policy increases by 38.8 percent when the IT administrators understands the importance of security concern levels within the enterprise. Therefore, the null hypothesis that higher levels of security breach concern levels by IT Administrators in HLIs will result in more positive attitudes effecting towards BYOD security policies was accepted. The estimated coefficient of response efficacy was positive and significant at the 10 percent level of significance, implying that the probability of enforcement and compliance of BYOD security policy increases with increase in response efficacy by IT administrators. The marginal effect result shows that, holding the other factors constant, the probability of enforcement and compliance of BYOD security policy increases by 33.6 percent when IT administrators responds effectively and efficiently on matters of BYOD security in an institution. Therefore, the null hypothesis that perceived effectiveness of users' actions with IT in HLIs will positively affect one's attitude towards BYOD security policies.

A summary of the hypothesis findings can be illustrated in the table below:

Table 5: Summary of Hypotheses

Hypotheses	Independent variable	Whether significant or not
H1	Perceived probability of security breach	Yes
H2	Perceived severity of security breach	Yes
H3	Security concern level	Yes
H4	Response efficacy	Yes

CHAPTER FIVE: CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusion

In this study, bring your own device (BYOD) and nomadic computing were examined for enterprise security compliance in HLIs in Africa. BYOD trends are significantly changing the security model for protecting corporate data, blurring the definition of this perimeter by physical location and asset ownership. Prematurely deploying BYOD in an enterprise environment introduces security risks that need to be addressed. Failure to do so can jeopardize the security of the very assets a company needs to protect. The study found that the perceived probability of security breach, the perceived severity of security breach, Security breach concern level and response efficacy had an impact on Enterprise Security Policies Compliance in an organization. IT administrators in the HLIs must identify the potential BYOD risks in order to implement mechanisms that can mitigate these risks. Therefore, educational institutions implementing BYOD must take steps to address privacy, security, and regulatory concerns.

REFERENCES

EY. (2013) *Bring your own device Security and risk considerations for your mobile device program*.

W. T. Kamau. (2013) *The Bring Your Own Device Phenomena: Balancing Productivity and Corporate Data Security*, University of Nairobi.

Cisco. (2014) *BYOD Security Challenges in Education: Protect the Network, Information, and Students*.

M. E. Mbalanya. (2013) *Bring your own device and corporate information Technology security: case of firms listed on the Nairobi Securities exchange limited*, University of Nairobi.

Company85. (2014) *BYOD and the security implications of consumerisation*.

D. Gessner, J. Girao, G. Karame, and W. Li. (2013) *Towards a User-Friendly SecurityEnhancing BYOD Solution.* NEC Tech. J., vol. 7, no. 3, p. 113.

R. Absalom. (2012) *Legislation Review: A Guide for BYOD Policies.* Ovum.

e.Rupublic. 2013 *Simplifying Bring Your Own Device (BYOD) in Education.* e.Rupublic.

J. Burt. (2011) *BYOD trend pressures corporate networks*. eWeek, 28 (14), 30-31. 2011.

R. W. Rogers and S. Prentice-Dunn. (1997) *Protection motivation theory.*

P. Norman, H. Boer, and E. R. Seydel. (2005) *Protection motivation theory*.

F. Putri and A. Hovav. (2014) *Employees' Compliance with BYOD Security Policy: Insights from Reactance, Organizational Justice, and Protection Motivation Theory*.

T. Herath and H. R. Rao. (2009) *Protection motivation and deterrence: a framework for security policy compliance in organizations,* Eur. J. Inf. Syst., vol. 18, no. 2, pp. 106–125. R.

W. Rogers and S. Prentice-Dunn. (1997) *Protection motivation theory*.

N. Singh. (2012) *BYOD Genie Is Out Of the Bottle–'Devil Or Angel,'* J. Bus. Manag. Soc. Sci. Res., vol. 1, no. 3, pp. 1–12.

K. W. Miller, J. Voas, and G. F. Hurlburt. (2012) *BYOD: security and privacy considerations,* It Prof., vol. 14, no. 5, pp. 0053–55.

J. Burt. (2011) *BYOD trend pressures corporate networks,* eweek, vol. 28, no. 14, pp. 30–31.

APPENDICES

APPENDIX A: COST AND MATERIAL ESTIMATES

The below table shows the total cost of the entire project.

ITEM	COST (Ksh)
Stationary	500
Travel Expenses	1000
Printing and photocopy	500
Food and Luxury	1000
Miscellaneous	500
Internet and Research Equipment	1000
TOTAL	4500

APPENDIX B: QUESTIONNAIRE

Questionnaires are design to help in obtaining data on the impact of bring your own device and nomadic computing on enterprise security policies' compliance. Both open-ended and closedended questionnaires are used. All responses are treated with higher confidentiality.

Instructions:

I. Please only tick where appropriate (tick one).

II. Please don't indicate your name anywhere on this questionnaire.

SECTION 1: Background information

1. What is your gender?

a) Male ☐

b) Female ☐

c) Other ☐

2. What is your age?

a) Age ……

3. What is your level of education?

a. Certificate ☐

b. Diploma ☐

c. Degree ☐

d. Masters ☐

4. How long have you been working in this institution?

I. 0-2 years ☐

II. 3-5 years ☐

III. 6-8 years ☐

IV. 8-10 years ☐

V. Over 10 years ☐

SECTION B: Success factors for adoption of green computing e-waste

The statements below shows whether the perceived probability of security breach, the perceived severity of security breach, Security breach concern level, and response efficacy had an impact on Enterprise Security Policies' Compliance. Please indicate your category to the statement by using 1- Strongly agree (SA), 2- Agree (A) 3- Neutral (N), 4- Disagree (D), 5- Strongly Disagree (SD)

Statement	1Strongly agree (SA)	2-Agree(A)	3-Undecided(U)	4-Disagree(D)	5-Totally disagree (SD)	Total
Perceived probability of security breach						
Perceived severity of security breach						
Security breach concern level						
Response efficacy						

APPENDIX C: WORK PLAN

Duration	Activity
1st month	Data collection
2nd month	Research writing
3rd month	Consultation
4th month	Research defense