Computer Engineering and Intelligent Systems
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol.6, No.4, 2015

A Review of Impacts of Bring Your Own Device (BYOD) and Nomadic Computing on Enterprise Security Policies' Compliance: The Case of Higher Learning Institutions in Kenya

Peter Namisiko[1*] Dr. William Sakataka[2] Bethuel Sugut[3]
1.Lecturer, Department of Information Technology and Coordinator, School of Pure and Applied Sciences, Mount Kenya University (Kitale Campus), PO BOX 1869-30200, Kitale , Kenya
2.Lecturer of Development Studies and Strategic Management and Coordinator, School of Post Graduate Studies, Mount Kenya University (Kitale Campus), PO BOX 1869-30200, Kitale , Kenya
3.Lecturer, School of Business and Economics and Director Mount Kenya University (Kitale Campus), PO BOX 1869-30200, Kitale , Kenya
* E-mail of the corresponding author: namsiko@gmail.com

Abstract
Network design is driven by mobility and as such Wireless Local Area Networks (WLANs) have become a major component of corporate networks in today's business environment. A trend is emerging where there is explosive consumer adoption of smart phones and tablets due to their low price and broad applications support that these devices are offering since they are WLAN enabled. Desktop Computers and laptops are used to produce information; while tablets consume information and smart phones to communicate that information. BYOD (Bring your own device) is a term which refers to instances when employees use their personal computing devices (typically smart phones, tablets and laptops) in the workplace. This trend is here to stay and the challenge is that it is a double edged sword pitting user satisfaction and productivity on one end and organizations data security on the other. As more employees look to access corporate networks with their personal mobile devices, vendors must find ways of helping corporations allow such access in secure, efficient ways. This is due to the fact that technology is changing at a very fast rate and with consumerization of IT revolution there has been a cultural shift such that the users are the ones getting the latest, cutting edge technologies first, and they want to bring those devices to work. BYOD changes the security model of protecting the organizations' data by blurring the definition of that perimeter, through physical location and in asset ownership. This study reviewed Bring Your Own Device (BYOD) and Nomadic computing on Enterprise security policies' compliance in HLIs in Africa. A quantitative survey study approach was used in ten university campuses to determine 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 organization.
Keywords: BYOD, Nomadic computing, Enterprise Security

1. Introduction

In today's business environment, network design is being driven by mobility and as such Wireless Local Area Networks (WLANs) have become a major component of corporate networks. A trend is emerging where there is explosive consumer adoption of smart phones and tablets due to their low price and broad applications support that these devices are offering since they are WLAN enabled. Desktop Computers and laptops are used to produce information; while tablets consume information and smart phones to communicate that information. Companies are demanding their employees to be more productive due to the advancements in technology. This requires a robust flexibility in the Information Technology (IT) policy that allows use of personal and mobile devices to be used safely in a work capacity to raise employee productivity and generate significant competitive advantage. In such scenarios, BYOD presents an attractive option to organizations [1].

The number of mobile devices continues to grow exponentially. Available statistics indicate that the number of mobile devices will be about 10 billion in 2018. This is equivalent to 1.5 mobile devices for every person on the planet [1]. These devices are increasingly becoming embedded in all parts of our personal lives, and thereby organizations must allow their employees to use their own personal mobile devices to conduct work related activities alongside corporate provided devices that include desktop computers and laptops. In such as scenario, employers cannot stop the use of mobile devices for both work and personal agendas, but they need to know how to control it. Part of the reason for exponential growth of these devices is attributed to the fact that most organizations have generation Y forming a bulk of its workforce. These employees are technology hungry and savvy personalities who are keen to explore and try out new technologies as they come out [2]. Rapid growth and advancement of technological innovations and inventions in the IT sector has dramatically changed the IT model where IT managers controlled who can access corporate data using the devices provided by the company. With consumerization of IT revolution there has been a cultural shift such that the users are the ones

getting the latest, cutting edge technologies first, and they want to bring those devices to work. The use of BYOD in the company's premises greatly improved productivity in the work place [3]. This is because employees tend to be familiar with their own devices as opposed to those devices provided by the company. Due to the familiarity with their own devices, employees' job satisfaction tends to be high. A study conducted by [4] found that the biggest driver that led to organizations adopting BYOD at Nairobi Stock Exchange (NSE) was improved employee productivity and efficiency. Similar studies on the factors that influence the adoption of BYOD devices in the work place have indicated that demand for flexible working hours, end user demand, employee morale boost, improved employee productivity and efficiency, reduced total cost of IT infrastructure ownership reduced capital, expenditure on IT equipment as the major drivers of adoption of BYOD devices in work place [4][2][5]. BYOD trends significantly alter the security model of protecting the organizations' data by blurring the definition of that perimeter, through physical location and in asset ownership [1]. Since these devices can now be used to organizations' data; the organizations must formulate policies to control the impact to the security threats and establish normative procedures and support models that balances employees' needs and their security concerns. Premature deployment of BYOD into a corporate environment does introduce security risks that must be addressed otherwise the very assets that a company needs to protect can have their security compromised.

According to [6] some of the security challenges associated with BYOD include: Bandwidth and productivity drains, data and device loss, attacks against mobile devices and policies used to secure BYOD. The fact that mobile devices do not have same security policy requirements as desktop devices has contributed to bandwidth and productivity drains since more and more employees are turning to the use of mobile devices to access corporate internet in an organization as opposed to desktop computers. For instance, employees may use their mobile devices to access services such as video streaming and other applications that have been denied by standard organizations' security policy. This has an effect of placing a significant strain and bottleneck on the organization network bandwidth thereby reducing the productivity in that organization [6].

The BYOD movement started in Higher Learning Institutions (HLIs) ten years ago. This was promoted by generation Y students who demanded to use their personal devices on campus. The University administrators understood that allowing internet access by mobile devices might improve the educational experience of such students. The Centre for Digital Education (CDE) survey of nearly 150 IT professionals in K-20 education revealed that 85 percent of faculty and staff bring a personal device to work (laptop, tablet or smart phone) which they use to access their school or college's network [8]. BYOD devices with 3G (Third Mobile Generation Network) and 4G (Fourth Mobile Generations Networks) internet access can circumvent the institutions' security features. This may not only increase the risk of viruses spread on school networks, but also attempts may be made to access administration files and e-mail by the students. Therefore, education institutions implementing BYOD must take steps to alleviate privacy, security and regulatory concerns. Allowing personally owned devices to access the network can open the door to breaches of privacy and data security, as student and staff owned devices may lack the necessary protections and features to keep information safe. With all the risks that BYOD brings along with it, it is clear that in order for HLIs to protect their assets and remain secure, a change of strategy is required.

IT administrators in the HLIs must identify the potential BYOD risks in order to put in mechanisms that can mitigate these risks. In Kenya, literature available on the BYOD trends shows that majority of research has concentrated BYOD trends in corporate and other companies in. Minimal research has been conducted to ascertain the level of security implementation of BYODs in HLIs. This study reviewed this trend of Bring Your Own Device (BYOD) and Nomadic computing on Enterprise security policies' compliance in HLIs. The main objective of this study was to review BYOD and Nomadic computing on Enterprise security consumerization in HLIs in Kenya. The study had two main objectives:

a. Determine the extent of awareness to which BYOD and nomadic computing security risks to HLIs IT systems in Kenya.

b. 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.

The paper has four parts. First, a review of the literature related to BYOD and Nomadic computing on Enterprise security policies' compliance will be explored. Then, research methodology will be presented and data analysis techniques discussed. Next, the findings will be discussed and summarised. The paper will conclude with recommendations on BYOD and Nomadic computing on Enterprise security consumerization in HLIs in Kenya.

2. A Review of Related Literature

2.1 Theoretical Framework

Understanding what constitutes BYOD and Nomadic computing risks and prevention is important in determining a proper theoretical framework that can explain the reasons for implementing the BYOD security measures in an

organization. The theoretical framework adopted for this study was Protection Motivation Theory (PMT) from which appropriate constructs were made as possible BYOD and nomadic computing threats and risks. Protection motivation theory (PMT) was developed by [10] to understand fear appeal communication that is intended to influence attitude and behaviour change. According to this theory, Fear appeal refers to the communication that describes adverse consequences that happen if one fails to adapt to a communicator's recommendation. This theory posits that cognitive appraisal would mediate the effect of fear appeal's components on attitude change by arousing "protection motivation." Protection motivation consists of two processes: threat appraisal and coping appraisal [11]. Threat appraisal is a process of evaluating maladaptive behaviour; it includes a response reward (advantage of maladaptive behaviour) and a perception of threat (severity and vulnerability). Coping appraisal is a process of evaluating the ability to cope with and remove the threat. This process encompasses response efficacy, self-efficacy, and response costs [12]. From the theory, it can be inferred that employee's assessment of the consequences of the security threat and the probability of exposure to a substantial security threat arising from BYOD and nomadic computing may lead him/her formulate or not formulate security policies that control the same risks. Another process that plays a central role in protection attitudes is the coping appraisal. This evaluates response efficacy, response cost, and self-efficacy. Response efficacy relates to beliefs about whether the recommended coping response will be effective in reducing the threat. Response costs refer to beliefs about how costly performing the recommended response will be. The table below illustrates the constructs obtained from PMT.

Table 1: Theoretical Constructs from PMT

No.	Construct
	Perceived probability of security breach
	Perceived severity of security breach
	Security breach concern level
	Response efficacy
	Response cost
	Security policy compliance intention
	Security policy attitude
	Self-efficacy

Source: [13]

The following conceptual Framework can be derived based on theoretical framework described:

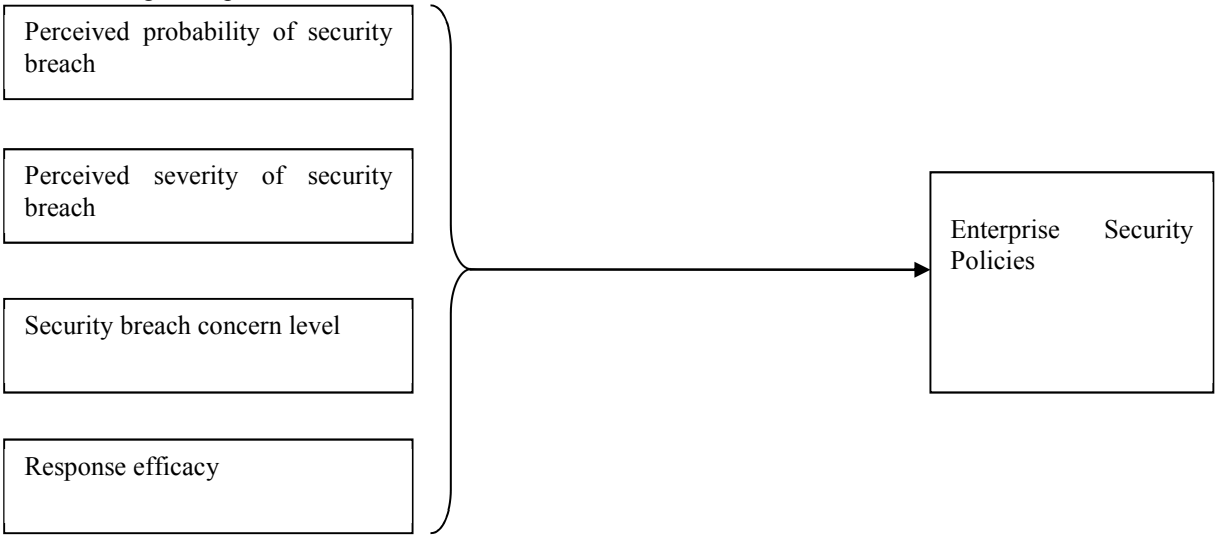

Figure 1: Framework for BYOD security policy compliance
Source: Researcher's own

2.2 Review of BYOD and Nomadic computing

There has been an explosion of technology that has led to the consumerization of IT in recent years [4]. As a result of this explosion, devices and services that were historically available only in the workplace and provided by IT departments are now widely available to and affordable by consumers. This has been fuelled by the introduction of devices such as the Apple iPhone and iPad, Google Android smart phones and tablets. Lower

cost of these devices has increased consumers' appetite for the latest technology. This is what BYOD and Nomadic computing brings to a work place. In BYOD and nomadic computing scenarios, enterprises wish to integrate their employees' mobile devices in enterprise operations (e.g., reading emails, editing documents) [6]. The BYOD movement started in Higher Learning Institutions (HLIs) ten years ago. This was promoted by generation Y students who demanded to use their personal devices on campus. The University administrators understood that allowing internet access by mobile devices might improve the educational experience of such students. The Centre for Digital Education (CDE) survey of nearly 150 IT professionals in K-20 education revealed that 85 percent of faculty and staff bring a personal device to work (laptop, tablet or smart phone) which they use to access their school or college's network [8].

2.3.1 BYOD and Nomadic computing Security Policies' Compliance Issues

Literature available on impacts of BYOD and nomadic computing on Enterprise security policies' compliance identifies the following compliance issues:

2.3.1.1 Perceived probability of security breach

Employees who perceive that a security threat can impose significant damages or disturbances are more likely to be concerned about enforcing security measures than those employees who do not perceive that a security threat can impose significant damages or disturbances. For such employees, the likelihood of them being concerned is low. This implies that when employees perceive the threat to be real they are concerned and they are more likely to have a more positive attitude towards protection mechanisms such as security policies [14]. According to [6], the likelihood that a security violation will cause a significant outage that will result in loss of productivity or causing a significant outage to the Internet that result in financial losses to organisations may spur the IT administrators to put in place security controls that have a deterrence 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.*

2.3.1.2 Perceived severity of security breach

The perceived severity of security breach refers to the likelihood that actions from outside an organization can bypass or contravene security policies, practices, or procedures within an organization. This relates to whether IT Administrators believe that information stored on organisation computers is vulnerable to security incidents.

This has the effect of lowering the productivity of employees and the profitability of organisations. [15]posits that increased incidents of security breaches have the effect of lowering the productivity of an organization and profitability of the organization by compromising the organization's data. This contradicts the hypothesis that many researchers have proposed as regards to increased productivity due to implementation of BYOD and nomadic computing[4][16][17]. 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.*

2.3.1.3 Security breach concern level

Security breach concern level relates to whether IT Administrators feel security issue affects their organisation directly or directly. The level of awareness by the IT Administrators is important in determining whether they can mount security controls that can have a deterrent effect. A study conducted by [13] found that security breach concern was found to have a significant effect on attitudes of IT administrators towards security policies. In this study, IT staff members were asked whether they thought IS security issue is exaggerated (Reverse coded). It was found to have a significant effect on attitudes of IT administrators towards security policies. This has a significant impact on enforcing security policies within institutions. 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.*

2.3.1.4 Response efficacy

According to PMT, response efficacy defines the beliefs that illustrate whether the recommended coping response will be effective in reducing the threat. In this study, an employee's perception regarding the effectiveness of abiding by the organisation's computer security policies is important in enforcing compliant policies within HLIs. According to [12], a security threat encompasses a threat to employee's mobile device and the organization's computing resources. Therefore, compliance with an organization's BYOD ISSP would benefit the organization and the employee. Thus,

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

2.3.2 Knowledge Gaps

BYOD trends significantly alter the security model of protecting the organizations' data by blurring the definition of that perimeter, through physical location and in asset ownership [1]. Since these devices can now be used to organizations' data; the organizations must formulate policies to control the impact to the security threats and establish normative procedures and support models that balances employees' needs and their security concerns. Premature deployment of BYOD into a corporate environment does introduce security risks that must

be addressed otherwise the very assets that a company needs to protect can have their security compromised. Therefore, education institutions implementing BYOD must take steps to alleviate privacy, security and regulatory concerns. Allowing personally owned devices to access the network can open the door to breaches of privacy and data security, as student and staff owned devices may lack the necessary protections and features to keep information safe. With all the risks that BYOD brings along with it, it is clear that in order for HLIs to protect their assets and remain secure, a change of strategy is required.

IT administrators in the HLIs must identify the potential BYOD risks in order to put in mechanisms that can mitigate these risks. In Kenya, literature available on the BYOD trends shows that majority of research has concentrated BYOD trends in corporate and other companies in. Minimal research has been conducted to ascertain the level of security policy implementations of BYODs in HLIs.

3. Methodology

To test the above model, we used a survey methodology for data collection. This study focussed on reviewing the impacts of Bring Your Own Device (BYOD) and Nomadic Computing on Enterprise Security Policies' Compliance in Higher Learning Institutions in Kenya. Data was collected from IT administrators in 10 Campuses in both Public and Private Universities in Kenya. A target population of 10 expert employees from both Public and Private Universities in Kenya was considered based on purposive sampling technique. These were employees that had acquired knowledge, skills and experience in the ICT industry.

The initial and follow up of questionnaires generated 10 usable responses, resulting in a response rate of 100%. This response rate from an unsolicited mailed questionnaire suggested that respondents found the topic interesting and relevant. As shown in table 1, the subjects were not evenly distributed with men accounting for 67% and women accounting for 33%.

Table 1: Descriptive statistics of measured items

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

As illustrated in table 2, 10 respondents (100%) demonstrated the understanding of BYOD use in HLIs. This is attributed to the fact that all the respondents in the study had knowledge and experience in the ICT industry. From the findings, a total of 6 respondents (60%) demonstrated awareness of BYOD and security risks it poses to the IT infrastructure. This large percentage on awareness was due to the fact that IT Administrators in these institutions had knowledge and experience on ICT matters. 3 respondents (30%) of the respondents indicated lack of awareness of BYOD and its security implications on enterprise assets while 10% of the respondents were not sure on the extent of awareness of BYOD and security implications for IT infrastructure in an institution. From the same findings, it was found that only 3 out of 10 Campuses had a policy of BYOD on enterprise security. A majority of Campuses (6 out 10) in the study had no policy regarding BYOD policy on enterprise security.

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

3.1 Findings

This study sought to determine the extent of awareness to which BYOD and nomadic computing security risks to HLIs IT systems in Kenya and 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. 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 employed both descriptive and inferential statistics to analyse the data. Descriptive statistics used included use of histograms, frequency tables and pie charts to represent data. This was useful in comparing groups that differed in size. In the survey, the respondents were asked to indicate whether 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 based on Likert scale strongly agree (SA), Agree (A),

Undecided (U), Disagree (D) and Strongly Disagree (SD). The table below summarises the descriptive statistics of the measured items based on 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

From the findings, 50% of the respondents cited Perceived probability of security breach as indicator towards enforcement of BYOD security compliance on enterprise. 30% of the respondents disagreed that perceived probability of security breach had an impact on enforcement of BYOD security compliance on enterprise. This findings reinforce findings by Rodgers and Prentice-Dunn who found out that if employees perceive the threat to be real and are concerned, they are more likely to have a more positive attitude towards protection mechanisms such as security policies [14]. 60% of the respondents cited Perceived severity of security breach as indicator towards enforcement of BYOD security compliance on enterprise. Only 20% of the respondents disagreed that perceived severity of security breach had an impact on enforcement of BYOD security compliance on enterprise. This is because when IT Administrators believe that information stored on organisation computers is vulnerable to security incidents, they are likely to put in place enforcement measures since the prospect of lower productivity and lower profits in an organization are higher. 70% of the respondents cited security breach concern level as indicator towards enforcement of BYOD security compliance on enterprise. 30% of the respondents disagreed that perceived probability of security breach had an impact on enforcement of BYOD security compliance on enterprise. This large percentage is attributed to the fact that security breach concern has a significant effect on attitudes of IT administrators towards security policies [13]. 50% of the respondents cited response efficacy as indicator towards enforcement of BYOD security compliance on enterprise. Only 20% of the respondents disagreed that response efficacy had an impact on enforcement of BYOD security compliance on enterprise. This is because individuals have more favourable security attitudes when they have high perceptions of citizen effectiveness. It also likely that employees who believe that their actions have a beneficial impact on their organisation will have a more positive attitude towards security policies [12].

Inferential statistics was 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 Perceived probability of security breach, Perceived severity of security breach, security breach concern level and response efficacy. A number of hypotheses concerning the correlations of some of the survey's variables were tested. This 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.

A logistic regression model was used to predict the enforcement of enterprise security policies' compliance with respect to BYOD and nomadic computing among the IT administrators in HLIs. Logistic regression was used since there was need to predict whether the presence or absence of Perceived probability of security breach, Perceived severity of security breach, security breach concern level and response efficacy had an implication on enforcement of a BYOD security policy. The table below summarises the findings 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

Hypothesis	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

4. Conclusion

This study reviewed Bring Your Own Device (BYOD) and Nomadic computing on Enterprise security policies' compliance in HLIs in Africa. BYOD trends significantly alter the security model of protecting the organizations' data by blurring the definition of that perimeter, through physical location and in asset ownership. Premature deployment of BYOD into a corporate environment does introduce security risks that must be addressed otherwise the very assets that a company needs to protect can have their security compromised. 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 organization.

IT administrators in the HLIs must identify the potential BYOD risks in order to put in mechanisms that can mitigate these risks. Therefore, education institutions implementing BYOD must take steps to alleviate privacy, security and regulatory concerns.

Acknowledgement
We wish to thank Mount Kenya University, Research and Development Directorate for assisting us with the funds for publication.

References

[1] EY, "Bring your own device Security and risk considerations for your mobile device program," EY, 2013.
[2] W. T. Kamau, "The Bring Your Own Device Phenomena: Balancing Productivity and Corporate Data Security," University of Nairobi, 2013.
[3] Cisco, "BYOD Security Challenges in Education: Protect the Network, Information, and Students," 2014.
[4] M. E. Mbalanya, "Bring your own device and corporate information Technology security: case of firms listed on the Nairobi Securities exchange limited," University of Nairobi, 2013.
[5] Company85, "BYOD and the security implications of consumerisation." 2014.
[6] D. Gessner, J. Girao, G. Karame, and W. Li, "Towards a User-Friendly Security-Enhancing BYOD Solution," *NEC Tech. J.*, vol. 7, no. 3, p. 113, 2013.
[7] R. Absalom, "Legislation Review: A Guide for BYOD Policies." Ovum, 2012.
[8] e.Rupublic, "Simplifying Bring Your Own Device (BYOD) in Education." e.Rupublic, 2013.
[9] J. Burt, *BYOD trend pressures corporate networks. eWeek, 28 (14), 30-31*. 2011.
[10] R. W. Rogers and S. Prentice-Dunn, "Protection motivation theory.," 1997.
[11] P. Norman, H. Boer, and E. R. Seydel, "Protection motivation theory," 2005.
[12] F. Putri and A. Hovav, "Employees' Compliance with BYOD Security Policy: Insights from Reactance, Organizational Justice, and Protection Motivation Theory," 2014.
[13] T. Herath and H. R. Rao, "Protection motivation and deterrence: a framework for security policy compliance in organisations," *Eur. J. Inf. Syst.*, vol. 18, no. 2, pp. 106–125, 2009.
[14] R. W. Rogers and S. Prentice-Dunn, "Protection motivation theory.," 1997.
[15] N. Singh, "BYOD Genie Is Out Of the Bottle–'Devil Or Angel,'" *J. Bus. Manag. Soc. Sci. Res.*, vol. 1, no. 3, pp. 1–12, 2012.
[16] K. W. Miller, J. Voas, and G. F. Hurlburt, "BYOD: security and privacy considerations," *It Prof.*, vol. 14, no. 5, pp. 0053–55, 2012.
[17] J. Burt, "BYOD trend pressures corporate networks," *eweek*, vol. 28, no. 14, pp. 30–31, 2011.

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

Academic conference: http://www.iiste.org/conference/upcoming-conferences-call-for-paper/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar