International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2015): 6.391

Emerging Security Challenges due to Bring Your Own Device Adoption: A Survey of Universities in Kenya

Jairus E. Ounza[1], Samuel Liyala[2], Solomon Ogara[3]

[1, 2, 3]Jaramogi Oginga Odinga University of Science and Technology, School of Informatics and Innovative Systems, Kenya

Abstract: ***Although a number of researches have been carried out by various organizations across the globe to establish security challenges facing education institutions due to BYOD adoption there is no evidence that a similar study has been carried out for universities in Kenya. Since it is evident that security challenges due to Bring Your Own Device (BYOD) adoption differ across institutions there is need for security challenges facing universities in Kenya due to BYOD adoption to be identified. The study surveyed public and private universities in Kenya in order to investigate security challenges facing them due to BYOD adoption with a view of generating empirical data to enhance their preparedness towards addressing BYOD security challenges. Based on the findings of the study, it was established that BYOD adoption exposes the universities to: lack of control of user devices, lack of user awareness on emerging threats due to user owned devices, difficulties in maintaining inventories of multi-platform user owned devices and increased risk to organizational data. The study recommends that organisations implementing BYOD should continuously establish the security challenges they face as a result of adopting BYOD so as to put in place appropriate security measures to mitigate the challenges.***

Keywords: Adoption, BYOD, Inventory, Organizational Data, Risk, Security Challenges

1. Introduction

Although there are benefits to universities due to adoption of BYOD practice where faculty, staff and students are allowed to use their own mobile devices (smart phones, tablets and laptops) there is a need to establish emerging IT security challenges.

A number of researches have been carried out by various organizations across the globe to establish BYOD adoption security challenges facing education institutions. Educause centre for applied research identified several challenges related to BYOD security in their study which included; challenges of higher education institutions to secure their assets, intellectual property, data and ensuring integrity of their networks [1].

A survey by BYOD action learning program of university of Michigan staff on how personally-owned devices were being used within the university established inadequate security safeguards implemented on personally owned devices, employees retaining sensitive institutional data on personally-owned devices after they had changed roles or left the institution, lost, stolen, misused, or hacked devices not reported as security incidents and impairment of the university's ability to fully investigate security incidents when they involves personally owned devices as security challenges facing the universities [2].

[3] identified issues related to data security as challenges facing institutions of higher education in South Africa due to BYOD adoption which include unauthorized access to sensitive data stored on mobile devices, unauthorized access to data stored on the institution's network, attacks from malicious software and ability for authorized users to be impersonated.

Since it is evident that security challenges due to BYOD adoption differ across different institutions there is need for security challenges facing universities in Kenya due to BYOD adoption to be identified. A survey of these universities carried out in 2013 indicated that about 53% of students owned laptops while 53% owned smart phones [4]. There is however no documented evidence of a research to establish the IT security challenges facing the universities due to BYOD adoption.

Therefore, identifying security challenges facing universities in Kenya due to BYOD adoption and generating empirical data will enhance universities preparedness towards addressing security challenges due to BYOD adoption.

2. Aim

This study investigated the security challenges facing universities in Kenya due to BYOD adoption with a view of generating empirical data.

3. A Review of Security Challenges due to BYOD Adoption

Despite the benefits, BYOD adoption in organizations creates potential security concerns as a result of devices having access to organizations internal IT resources [5]. Security concerns arising due to BYOD adoption affect both the organizations and their employees. [6] illustrated a similarity between the BYOD initiative and the laptops introduction to organizations by pointing out that the threats and security concerns associated with BYOD initiative were "largely a replay'' of those previously faced with laptops. They advised that the BYOD phenomenon is a tougher challenge to security because of the large number of devices, fragmentation of devices and security levels initiated in organizations. [7], [6], [8], [9], [10], [11], [9], [12] and [13]

noted that there are four security challenges that are prevalent due to BYOD adoption namely; loss of device control, increased risk to organization data, challenges of managing BYOD devices and platforms and user awareness challenges.

3.1 Loss of Device Control

Loss of control and visibility a key security challenge due to BYOD adoption presents significant security risks because organizations no longer control the devices that their data is stored in [7], [6], [8], [12]. According to Mathew Gyde the general manager of Dimension Data group in charge of security solutions, organizations face increased security risks because they lack visibility of what is sitting on their network. He further observes that lack of visibility increases the opportunity of intrusion by rogue devices and applications [14]. Therefore enforcement of security policies is difficult for issues such as data leakage, theft, and regulatory compliance [6], [7]. This is attributed to 'ownership' which is the base of this problem since organizations have less visibility of the security environment for BYOD compared to a traditional networked environment.

According to [7], due to lack of control and visibility there are fewer options to mitigate security risks for unmanaged devices compared to managed devices. As organizations increasingly lose control over the security of BYOD devices employees have a more critical role to play in upholding organizational IT security. Another concern due to loss of control is the potential of the organization's network being infected by malware likely to spread from infected personal devices [6]. The malware might not specifically target the organization data, but it could create concerns about backdoor data leakage for BYOD scenarios [15]. Uncontrolled devices also have the potential of draining network resources and bandwidth because without control they may repeatedly connect automatically using the service set identification (SSID) acquired in previous connections [16].

3.2 Increased Risk to Organization Data

BYOD increases security risks for any organization's data. Innovation council a team composed of 1000 global information security leaders cited lost or stolen devices as a top security concern. The main risk is due to the likelihood of lost or stolen devices containing sensitive data. On the other hand a research by Osterman indicates that less than 1 in 4 of user owned devices can be wiped remotely thus the risk of organization's data falling into the wrong hands [17]. Storage of critical information assets on employee-owned devices poses a great threat to the organizations due to intended or inadvertent disclosure of sensitive data such as private customer information and proprietary company information [6]. For example it is possible to file share or store with minimum zero security sensitive documents downloaded onto personally owned devices thus exposing the organization to the risk of data breach [18]. The relatively small size and ease of portability exposes BYOD devices and the information stored on them to higher risks of being lost or stolen [9], [10]. Password weaknesses and operating system defences on consumer devices also contributes to this risk. Another challenge to the organization's data is the unwillingness of their employee's to backup data [19].

3.3 Challenges of Managing BYOD Devices and Platforms

Adoption of BYOD introduces new challenges of managing devices as they access the organization's IT resources. To manage BYOD adoption organizations have to set aside additional funds to develop new infrastructure to accommodate and manage use of different BYOD devices and operating systems running on them [16]. Many organizations are not able to effectively manage BYOD due to challenges of maintaining inventories of devices accessing their resources [11]. When the devices are unmanaged it is difficult to identify/map and connect these privately owned devices to the right organization information resources [16]. Due to their inability to control user owned devices organizations find it difficult to manage the security of their information resources held in user owned devices [20].

Organizations also face challenges of managing employee owned devices as a result of device owners connecting more than one device to access their IT resources and the ability of users to constantly upgrade these devices at will. In a report by [21] at least 80% of employees possessed more than one mobile device while more than 30% of employees did not utilize any password to safeguard data located on their private devices. A global survey by Fortinet a world leader in high-performance network security showed that most employees prefer to use their own devices at work despite it being against their organization's security policies. Users also hold themselves not the organization responsible for their devices security issues [22]. Because both personal and organization data coexist on same devices it is very difficult to find a balance between strict security control for the organization's data and privacy of personal data especially when the devices are not corporate issued assets [9].

3.4 User Awareness Challenges

Users are the weakest links even in the most sophisticated security systems [23]. Lack of user security awareness is the primary contributor to some of the BYOD security challenges [12]. User's risk exposing organization data held in their devices because they are increasingly downloading and installing third party applications to their devices while disregarding security concerns [13].

Users also expose the organization's data to security threats when they connect to unsecured networks or browse malicious WebPages [24]. Majority of user's do not install any third party security software and many of them do not believe that security softwares are essential for the security of their devices [13]. Users also have tendencies of forgetting guidelines set by policies or at times are unaware of existing policies or changes which highlight the need for constant IT security training reinforcement. On other occasions employees who strongly disagree with limitations

enforced by BYOD security policies often actively seek loopholes to exploit [8].

Most security breaches occur because trusted organizations internal employees subvert existing security controls [25]. [26] stated that, ''the way in which people interact with information assets and how they behave in the working environment will in time become the way in which things are done in the organization''. The processes and procedures defined at the organizational level together with the guidance of managers and other influential individuals shape the attitudes of employees [26]. This eventually becomes the culture of the organization because people who don't know how to do things rarely do them well [27]. [28] found out that users had dismal behaviour records of complying with basic security guidelines.

4. Methodology

This research study was carried out for both public and private chartered universities in Kenya. This was a descriptive research study that enabled the narration of facts on the status of BYOD security challenges faced by the universities in Kenya. Survey research design was used to undertake the study. This research design enabled the researcher to reach out to the respondents who were geographically spread out across the country via online thus saving the researcher the cost of physically going to the respondents. The design also enabled the researcher to reach a wide number of respondents within a short time. The method that was applied for this study was the mono method since this study employed only one quantitative data collection technique (questionnaire) and one corresponding quantitative analysis procedure (descriptive analysis technique). This study employed cross sectional time horizon because the objective was to gather information on BYOD security challenges during the period of the research. Time horizon also often employs survey design which was used for this study.

4.1 The Study Population and the Sample Size

This study comprised of a finite population because the number of elements were fixed and its targeted respondents were system/network administrators of all public and private chartered universities in Kenya. According to a list obtained from the commission of higher education (CUE) website, the total numbers of public and private chartered universities were 39 [29]. Thus, the study population was 39 where each university was represented by one system/network administrator.

Further, the study employed probability sampling design which provided each university with equal chance of being included in the sample [30]. The sample of study was determined by use of normal approximation to the hypergeometric distribution [31] as shown in equation (i).

$$n = \frac{NZ^2pq}{E^2(N-1)+Z^2pq} \quad \text{..... (i)}$$

Equation (i): Calculating sample size for small populations adopted from [31].

n = required sample size
N = population size
p and q = population proportions {values set to 0.5} [31].

Z=Value that specifies the level of confidence you want in your confidence interval when you analyze your data. Typical levels of confidence for surveys are 95% in which case z is set to 1.96 [31].

E =Accuracy of sample proportions. Note for the sample proportions to be accurate E should not be lower than $1/N$ [31]. Therefore a value of {0.03} was used.

According to [32] in most business and management researches, researchers use 95% to within plus or minus 3 to 5 percent of true values to estimate the population's characteristics while the z value is 1.96 when using 95% confidence.

Using equation (i) the sample size of the research study was found to be 38 as shown below.

$$n = \frac{39 \times 1.96^2 \times 0.5 \times 0.5}{0.03^2(39-1)+1.96^2 \times 0.5 \times 0.5}$$

Therefore, n= 38

To eliminate one university so as to remain with the required sample size of 38 universities a web application research randomizer [33] was used. The universities were coded each with a unique number of 1-39. The codes were then fed to the web application where one university represented by the code generated randomly was eliminated.

4.2 Research Instrument

Data for the study was gathered through questionnaires that were sent to the respondents via e-mail. Questionnaires suited this study well since the targeted universities are geographically spread out across the country. The questionnaires were addressed to the network/system administrators who by virtue of being in charge of central universities IT infrastructure were in a position to respond adequately to questions on challenges inherent due to BYOD adoption. The questionnaire was developed based on a five point likert scale where 5 represented the most positive response (strongly agree) while 1 represented the most negative response (strongly disagree). The questions sought to establish security challenges facing universities due to BYOD adoption. The questions focused on Loss of device control [7], [6], [8]; increased risk to organization data [17], [6], [18]; challenges of managing different BYOD devices and platforms [11], [16] and user awareness challenges [23], [12], [13], [24].

4.3 Response Rate

The study targeted responses from systems/network administrators on behalf of the universities to gather data. A total of 25 out of 39 respondents replied the questionnaire on behalf of their universities representing a total of 64.10%. A total of 14 respondents represented public universities while

11 respondents represented private universities as shown in table 1.1.

Table 1.1: Percentage rates of universities respondents.

University Category	*Respondent*	*Target*	*Received*	*Response Rate %*
Public	System/Network administrator	22	14	63.64%
Private	System/Network administrator	17	11	64.71%
Total		39	25	64.10 %

Source:[34]

According to [35], many survey studies in leading educational journals report a response rate of 50% or better. Thus in comparison the response rate for this study was sufficient to undertake analysis and generate conclusions. This study generated quantitative data while descriptive statistics was used for analysis. Data was analyzed, interpreted using Statistical Application System (SAS) and was presented using tables representing percentages and χ^2 values of the respondent's feedback. Data analysis focused on the significance of the statistical tests done on the data obtained from the respondent's.

5. Analysis of Study Findings

The value of χ^2 which was used to analyze findings of emerging security challenges due to BYOD adoption facing universities in Kenya was set at 0.05. All items that had values of 0.05 or below were considered while all items that were above 0.05 were dropped. The study findings indicated that three of the four challenges were found to be statistically significant at $\chi^2 (P \leq 0.01)$ with majority of the respondent either agreeing or strongly agreeing that their universities faced these security challenges. About 40% of the respondents agreed that their universities faced challenges due to loss of devices, about 52% of the respondents indicated that their universities had challenges of managing different BYOD devices and platforms while about 60% of the respondents indicated that their universities faced security challenges due to lack of user awareness. Respondents were equally divided on the increased risk to organizational data security challenge at $\chi^2 (P = 0.05)$. About 32% and 16% of the respondents strongly agreed and agreed respectively that their institutions faced this security challenge. These results are shown in table 1.2.

Table 1.2: Emerging challenges due to BYOD adoption

Questions to respondents	Respondents feedback in Percentages					Analysis values	
	SA	A	N	D	SD	χ^2	P> χ^2
Loss of device control	40	36	8	12	4	14	0.01
Increased risk to organization data	32	16	44	8	0	7.8	0.05
Challenges of managing different BOYD devices and platforms	28	52	16	4	0	12.6	0.01
User awareness challenges	28	60	12	0	0	8.96	0.01

Source: [34]

Key: SA=Strongly Agree; A=Agree; N=Neutral; D=Disagree; SD=Strongly Disagree

χ^2 = Chi Square Probability.

6. Discussion of Study Findings

This study sought to establish if universities in Kenya experienced security challenges emanating due to adoption of BYOD which include; loss of device control [7], [6], [8]; increased risk to organization data [17], [6], [18]; challenges of managing different BYOD devices and platforms [11], [16] and user awareness challenges [23], [12], [13], [24].

Based on the findings of the study, it is evident that majority of the BYOD security challenges are prevalent in universities in Kenya. This indicates that the challenges that this institutions of higher education face are similar to those experienced by other organizations and institutions of higher education in other parts of the globe. The only difference could be the impact and the magnitude.

User awareness challenge was found to be the leading IT security challenge facing universities in Kenya due to BYOD adoption [34]. These findings corresponded to views by [23] that users are perceived as the weakest links even in the most sophisticated security systems. This could be attributed to lack of awareness by users as noted by [12] which primarily contributes to challenges due to BYOD adoption.

Challenges of managing different devices and platforms was established to be the second major security challenge facing universities in Kenya due to BYOD adoption [34]. Due to users bringing more than one personal device to access university's IT resources, these universities find it difficult to maintain inventories of the devices.

Loss of device control was the third security challenge that universities in Kenya face [35]. Universities in Kenya lack visibility of devices in their networks making them susceptible to intrusion, data leakage, device and data theft. The aforementioned BYOD challenges risks organizational data [34] for the universities surveyed.

7. Summary of Findings

Based on the findings of the study it was established that universities in Kenya face most of the emerging IT security challenges due to BYOD adoption. Universities were found to lack control of user devices; they also face challenges of enlightening their users on IT security challenges emerging due to user owned devices. These universities were found to have challenges of managing different user devices, different operating systems and application softwares running on the devices. Lastly BYOD adoption was found to increase risk to organizational data.

8. Conclusion and Recommendations

It is evident that most organizations that adopt BYOD are exposed to emerging IT security challenges due to BYOD adoption. These are global challenges which also cut across universities in Kenya. Security challenges found to be

prevalent in the universities include; user awareness, loss of device control, increased risk to organization's data and challenges of managing different BYOD devices and platforms. Emerging BYOD security challenges are dynamic and they keep on changing by the day. For this reason this study recommends that; establishing challenges due to BYOD adoption should not be a onetime activity but a continuous process. In addition, appropriate security measures should be put in place to mitigate the challenges.

References

[1] Dahlstrom, E., & DiFilipo, S. (2013). The consumerization of technology and the Bring-Your-Own-Everything (BYOE) era of higher education.*EducauseCenter for Applied Research*

[2] Action Learning Project: Bring Your Own Device (BYOD). (2012). Retrieved 17 March 2015, [Online]. Available:http://www.bf.umich.edu/bfleadership/docs/2012/byod-research-paper.pdf

[3] De Kock, R., & Futcher, L. A. (2016, August).Mobile device usage in higher education institutions in South Africa. In *Information Security for South Africa (ISSA), 2016* (pp. 27-34). IEEE.

[4] Kashorda, M., & Waema, T. (2014). E-Readiness survey of Kenyan Universities (2013) report. *Nairobi: Kenya Education Network*.

[5] Moreira, F., Cota, M. P., & Gonçalves, R. (2015). The Influence of the Use of Mobile Devices and the Cloud Computing in Organizations. In*New Contributions in Information Systems and Technologies* (pp. 275-284).Springer, Cham.

[6] Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). BYOD: Security and privacy considerations. *It Professional*, *14*(5), 53-55.

[7] Morrow, B. (2012). BYOD security challenges: control and protect your most sensitive data. *Network Security*, *2012*(12), 5-8.

[8] Thomson, G. (2012). BYOD: enabling the chaos. *Network Security*, *2012*(2), 5-8.

[9] Ghosh, A., Gajar, P. K., & Rai, S. (2013). Bring your own device (BYOD): Security risks and mitigating strategies. *Journal of Global Research in Computer Science*, *4*(4), 62-70.

[10] Ghosh, A. K., & Swaminatha, T. M. (2001). Software security and privacy risks in mobile e-commerce. *Communications of the ACM*, *44*(2), 51-57.

[11] Ernst & Young. (2013). Security and Risk considerations for your mobile device program.

[12] Ernst& Young,. (2012). *Bring Your Own Device (BYOD) trends and audit considerations*. Retrieved 21 March 2015, [Online] Available: https:// azslide. com/ trends-and-audit-considerations_ 596ad23c1723ddd7a5aab3ed.html

[13] Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security*, *34*, 47-66.

[14] Ashford, w. (2013).*Enterprises struggle with security challenge of BYOD, study shows*. *Computer Weekly*.[Online]. Available: http://www.computerweekly.com/news/2240207325/Enterprises-struggle-with-security- challenge-of-BYOD-study-shows

[15] Chang, J., Ho, P., & Chang, T. (2014).Securing BYOD.*IT Professional*, *16*(5), 9-11.

[16] Garba, A., Armarego, J., Murray, D., & Kenworthy, W. (2015). Review of the Information Security and Privacy Challenges in Bring Your Own Device (BYOD) Environments. *Journal Of Information Privacy And Security*, *11*(1), 38-54.

[17] Phifer, L. (2013). *BYOD security strategies: Balancing BYOD risks and rewards*. *SearchSecurity*.[Online]. Available:http://searchsecurity.techtarget.com/feature/BYOD-security-strategies-Balancing-BYOD-risks-and-rewards

[18] Dedeche, A., Liu, F., Le, M., & Lajami, S. (2013). Emergent BYOD security challenges and mitigation strategy. *The University of Melbourne*, 1-17.

[19] Wang, Y., Wei, J., & Vangury, K. (2014, January). Bring your own device security issues and challenges. In *Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th* (pp. 80-85). IEEE.

[20] Ortbach, K., Walter, N., & Öksüz, A. (2015, May). Are You Ready to Lose Control? A Theory on the Role of Trust and Risk Perception on Bring-Your-Own-Device Policy and Information System Service Quality. In*ECIS*.

[21] Calder, A. (2013). Is the BYOD movement worth the risks. *Credit Control J*, *34*(3), 65-70.

[22] Fortinet,. (2012). Fortinet Global Survey Reveals First Generation BYOD Workers Pose Serious Security Challenges to Corporate IT Systems Fortinet Network Security, Enterprise and Data-Center Firewall. Fortinet.com.[Online]. Available: http:// www. fortinet. com/press_releases/120619.html

[23] Caldwell, T. (2012). Prepare to fail: creating an incident management plan. *Computer Fraud & Security*, *2012*(11), 10-15.

[24] Peraković, D., Husnjak, S., & Remenar, V. (2012, January). Research of security threats in the use of modern terminal devices. In *23rd International DAAAM Symposium Intelligent Manufacturing & Automation: Focus on Sustainability*.

[25] Dhillon, G. (2001). Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers & Security*, *20*(2), 165-172.

[26] Martins, A., & Elofe, J. (2002). Information security culture. In*security in the information society* (pp. 203-214).Springer, Boston, MA.

[27] Coopers, P. (2013). Key findings from the Global State of Information Security Survey 2013.*Changing the game*.

[28] Stanton, J., Mastrangelo, P., Stam, K., & Jolton, J. (2004). Behavioral information security: two end user survey studies of motivation and security practices. *AMCIS 2004 Proceedings*, 175.

[29] Commission of University Education [Online]. Available:http://www.cue.or.ke/index.php/services/accreditation/status-of-universities

[30] Kothari, C. R. (2004). *Research methodology: Methods and techniques*. New Age International.

[31] Morris, E. (2004). Sampling from small populations.*Websitehttp://uregina.ca/~morrisev/Sociol*

ogy/Sampling%20from%20small%20populations.htm.(Accessed 20 Sep. 2006).
[32] Saunders, M. L., & Lewis, P. (2009). P. and Thornhill, A. (2009). *Research methods for business students*, *4*.
[33] Research Randomizer.Randomizer.org. [Online]. Available: https://www.randomizer.org/
[34] J.E. Ounza, Secure Adoption For Bring Your Own Device in Universities in Kenya, Unpublished Jaramogi Oginga Odinga University of Science and Technology Thesis, 2017.
[35] Klassen, A. C., Creswell, J., Clark, V. L. P., Smith, K. C., & Meissner, H. I. (2012). Best practices in mixed methods for quality of life research. *Quality of Life Research*, *21*(3), 377-380.

Author Profile

Jairus E. Ounza is currently pursuing a M.Sc. degree in IT Security and Audit at Jaramogi Oginga Odinga University of Science and Technology, Bondo, Kenya. He holds a BTech degree in Industrial technology (2010) of Egerton University, Njoro, Kenya and a KNEC diploma in Electronics Engineering (1998) Kenya Institute of Mass and Communication, Nairobi, Kenya. He has over seventeen years experience in network design, implementation and maintenance. His area of interest include IT infrastructure deployment, IT security, and Cyber technology and data management.

Dr Samuel Liyala holds a PHD in information systems, De Montfort University, Leicester, England, B.Sc. in information systems management De Montfort University, Leicester, England. He has over fifteen years in academia and is currently a lecturer and the chair Department of Information and Technology at Jaramogi Oginga Odinga University of Science and Technology, Kenya. He has also served as a lecturer and researcher at De Montfort University, United Kingdom. Dr Liyala has also been engaged with social research and ICT4D where focus was on research and advocacy to make all voices count. He has also been engaged in design, implementation and evaluation of policies in developing nations.

Dr Solomon Ogara holds a Ph.D. in Computer Information Systems from the University of North Texas, USA, 2011, Post-Graduate Certificate from the University of North Texas, 2009, M.s. Computer Information Systems with specialization in Information Security and Networking from Dakota State University, USA 2005, B.S. Ag Economics with computer science courses, University of Arizona, USA, 2002 and B.sc. Ag Edu & Ext (1993) Egerton University, Njoro Kenya. He is currently a lecturer and the chair Department of Computer Science &Software Engineering, Jaramogi Oginga Odinga University of Science and Technology. Dr Ogara has interest in research and is currently working on a proposed comprehensive framework for securing mobile devices.