International Journal of Computer Applications Technology and Research
Volume 9–Issue 11, 303-310, 2020, ISSN:-2319–8656

Adoption of Bring Your Own Device: Challenges and Risks in Higher Learning Institutions in Kenya

Oonge, O. Samuel
Department of Information Technology,
Maseno University Kenya
Kisumu, Kenya

Muhambe, T. Mukisa
Department of Information Technology,
Maseno University Kenya
Kisumu, Kenya

Ratemo, M. Cyprian
School of Computing,
Kisii University Kenya,
Kisii, Kenya

Abstract: In the digital world, consumerization of Information Technology has motivated individuals to privately acquire the latest mobile technology devices to access the organization/institution networks to perform their formal duties, a phenomenon also known as bring your own device (BYOD). The popularity of BYOD in learning institutions has been accelerated by perceived benefits of work flexibility, increased productivity and efficiency, dynamic student and employee preferences and technology trends and advancements. It has been noted however, that BYOD adoption compromises the general security of organizational information resources. This paper explores the challenges and risk factors of BYOD adoption in higher learning institutions and recommends mitigation strategies for the same.

Keywords: Bring your own device (BYOD), Risks, Security, point to point (P2P), Mobile Device Management (MDM) Mobile Application Management (MAM) and Identity Access Management (IAM).

1. INTRODUCTION

Information Technology (IT) has progressed from being a commodity service provider to a means for achieving greater efficiency and productivity [1]. The growth of IT adoption has been driven by the need for efficiency in operations, increased dependency on information for strategic and evidence-based decision making, online digital platform learning, the need to secure institutions information resources, and the growing phenomenon of collaboration between the institutions and other entities. The growth in uptake of mobile devices has greatly contributed to the use of information technology in enterprises. There is also a growth in the use of personal devices to execute enterprise applications and access data or information to perform their work related activities, a phenomenon known as Bring Your Own Device (BYOD), gradually becoming the norm. [2][3][4].

Studies [5][6] have established that powerful mobile operating systems, with capability to handle enterprise level applications, coupled with growing use of mobile internet connectivity provide advanced device capabilities allowing individuals to access information wherever they are and at whatever time. These devices, combined with business applications hosted in cloud-based environment means that organizational data and information or institutions learning resources are available to users no matter where, when or which devices they access the corporate networks with [7], which has led to increased access flexibility and availability of corporate information [8], hence increased efficiency and productivity.

Fortinet, [9] established that academic institutions' networks continue to be a favorite playground for cybercriminals because of their openness nature when it comes to information sharing. The report also highlighted the upsurge of attacks in these BYOD environments because of the users' cutting edge technologies and strategies, not forgetting pushing hard against network restrictions that make them employ workarounds to access information when in need. According to this report, in 2018, academic institutions had posted 13% of information security breaches compared to all other sectors in the United States of America (USA) resulting to a compromise of over 32 million records. Oregon University also suffered a breach that resulted in exposing students and their respective families' data. The PII of 636 students were compromised because of a BYOD user being compromised through a phishing email. The victims of this attack were majorly those who had interacted through email with the attack victim [10]

In [11] global risk management survey, cyber risk was ranked as the first risk facing academic institutions in Africa and is likely going to remain on top. In its 2016 report, [11] reported that the University of Limpopo's website was brought down, leaking exam papers and the details of over 18,000 students. The perpetrator also leaked login details for the University's intranet. This was suspected to be an insider with a BYOD device [10]

1.1 Objective of the Study

This study explores the challenges and risk factors that face higher learning institutions' information resources due to BYOD adoption and proposes mitigation strategies to counter the challenges and improve information security.

1.2 BYOD in Higher Learning Institutions

Institutions of higher learning have contributed towards the growth of the BYOD phenomenon. [12] revealed that "ownership and use" of mobile devices by higher education learners were on the ascendency. Cisco Networks [12] in their survey indicate that 85% of education institutions have allowed some form of BYOD on their institutions networks, a trend confirmed by the Bradford Networks global survey [13]. A survey by [14] on the use of personal devices established that 92% of students used laptops, 68% tablets, 44%, smart phones while 16% used e-readers for academic purposes. In another survey, [13] found that 85% of higher education institutions in US and UK, allow students, faculty and non-academic staff to access the institution's network using personally-owned mobile devices and predicted that by 2019, 90% of learning institutions would support BYOD [16], while the institutions that do not allow BYOD would receive ongoing requests to use personal devices on their networks [13].

Several factors have been identified as driving forces behind adoption of BYOD in the university. The higher learning institutions have allowed their employees and students to use their own devices for personal and official purposes on the same infrastructure instead of them maintaining a separate, work-dedicated device [17]. It is argued that this has been fuelled primarily by the limited budgets for purchasing computers for these institutions, dynamic employee preferences and technological trends and advancements that has spiked the number of smartphones and tablets on the network.

[18] argues that one of the main reasons for the sudden shift towards BYOD by institutions is students' determination to use their personal devices to access institutions and other information regardless of the institutions security policies in place. The students believe that it is their right to use their own devices within their institutions [19] , and will intentionally break any anti-BYOD policies introduced [20] [21] [22] established that students and staff prefer the use of education apps on their mobile devices to more efficiently handle their tasks, while using the same device to interact on social media, access cloud based storage and entertainment.

Currently, the world has experiencing significant economic and learning disruptions due to the effects of the Corona Virus (COVID-19) pandemic. COVID19 resulted in halting of most face to face interaction, with more emphasis being put on the online learning's as well as online transaction for most of the university activities. Higher learning institutions as indicated by national media houses have encouraged learning from home necessitating the use of BYOD to access course materials and examinations. This has accelerated the adoption of working from home, and made it necessary for employees and students to access learning and work-related applications from their personal devices.

While 95% of institutions allow the use of BYOD devices in the workplace in some way, two out of three employees use their personal devices at work, regardless of the company's BYOD policies. That means some employees are using their personal devices to access organization networks and applications irrespective of the policies in place.

Meanwhile, despite the institutions striving to establish and continually improve information security controls to adequately protect sensitive data and comply with a variety of laws and regulations [23] [1], note that this task has become difficult to achieve due to overdependence on BYOD. According to [24], organisations are struggling to manage remote workers' use of phones and other mobile devices. 52% of the respondents on the same survey indicated that personal mobile devices on the network were very challenging to protect from cyber threats. The institutions are tasked with balancing the expectations of users, reaping the benefits of mobile devices and applications, while protecting the Confidentiality, Integrity, and Availability (CIA) of the institutions' information [25]. [4] pointed out that attacks directed towards this information are on the rise.

2. METHODOLOGY

A survey was carried out across 3 Kenyan public universities that permit BYOD. A sample of 400 users was used in the study as recommended by [26]. The sample consisted of technical staff; Senior ICT administrators, covering system, network and operations and maintenance. In this category, the respondents were purposively selected and interviewed. The second category of respondents were other users; consisting of students, lecturers and non-academic staff who were randomly selected to participate in the study through a survey. It was a requirement for a user to have one or more years of BYOD experience to fill the questionnaire.

A mixed method research design was adopted allowing both qualitative and quantitative approaches [27] [28]. A five point structured Likert scale questionnaire was constructed based on comprehensive literature review. The questionnaire was sent out to four hundred (400) email addresses belonging to participants who included lecturers, non-teaching (administration) staff and students out of which three hundred and eightynine (389) responses were received representing approximately 97% response rate. The questionnaire was administered using google forms assuming high computer literacy among the respondents. A semi-structured interview schedule was also used to obtain precise but relevant BYOD risks and challenges information from the selected eleven (11) senior ICT administrators [28][29]. A qualitative and descriptive analysis of data was done to assist in establishing the challenges and risks experienced due to BYOD adoption within higher learning institutions.

2.1 Demographics

The participating universities were coded as U1, U2, and U3 representing university 1, university 2 and university 3 respectively. Out of the 389 responses received university U1 had a majority of respondents with 162 followed by university U3 with 126 respondents while university U2 had 101 respondents. Majority of the respondents were students representing 60%, lecturers 27% while non-academic staffs represented 13% of the respondents. The non-academic staff category comprised of ICT administrators, other administrative staff and top management cadre. Three ICT administrators were randomly selected and interviewed from U2 and U3 while five respondents were interviewed from U1 university for being an established and more populous university. There was 100% response rate for interviews.

2.2 Results and discussion

To identify the challenges and risk factors for BYOD adoption within higher learning institutions, a questionnaire and interview schedule containing nine questions were administered to the respondents. The responses for the questions were as follows;

2.2.1 Does your institution allow students and staff to use their own mobile devices on the institutions network?

The question was meant to establish whether BYOD adoption is in place in the respondent's institution. All the respondents were positive on this question. As indicated by one of the administrators

> *"The university has allowed own mobile devices into the institution hooking them up on the institutions network in order improve mobility and ease of information and academic material access by the students and researchers*".

This indicated that out of the three selected universities, none prohibits the use of BYOD on the institution's network, a confirmation that BYOD has been adopted to enhance student motivation and learning in higher learning institutions as also established by [30] [31] [32]

2.2.2 Do the ICT administrators control who to connect to the institution's network?

This question was meant to establish if there were any information security controls implemented to detect and deter any unauthorized access. Out of the 100 respondents, more than half (75%) denied knowledge of any implemented security controls that controls who connects to the network. 15% of the respondents slightly agreed while 10% strongly agreed of their administrators knowing who connects to the network.

Institutions of higher learning promote a culture of openness in order to promote access to information and learning materials therefore, they have a habit of using either one or two layers of security. Similarly, researchers, lecturers and students are committed to sharing information through collaboration, inside and outside the university, in order to facilitate their discoveries irrespective of information security policy flouting. These sentiments were also echoed by [33] [34] [35].

BYOD adoption overwhelms the universities' security teams since there is a lot of difficulty in controlling what the owners of the devices do with them. Since the institutions' focus is on getting users connected to ease learning, research and entertainment, this has deteriorated the general security of the network making it vulnerable to attacks and becoming easy targets or where targets anchor to launch attack against other targets [4].

2.2.3 Does your own mobile device have an active antivirus and a genuine operating system?

This question was meant to establish the security level of devices that constantly connect to the institution's network. The analysis revealed a sad state of operation since 83% of respondents had never protected their mobile devices, 11% of the respondents have an antivirus installed but not updated while only 6% had an updated antivirus. It was noted that 2% of the respondents used open source operating systems while 76% of the respondents used inactivated proprietary software. Variations in operating systems and physical platforms was encountered (e.g. Apple's iOS, Android, and windows mobile) on the institution's network posing a unique security challenge to IT resources, since every producer has customized security tools for their device. Getting the learning institution to implement all the security tools for different devices is a big challenge. [36] [37] also highlights on the security risk posed by variations of applications with different levels of trust installed on the varied devices.

2.2.4 Are there any security challenges that have come up by allowing BYOD in your institutions?

This open question to the respondents granted them an opportunity to list all challenges that they have experienced because of BYOD adoption in their respective universities. The responses were varied but classified in major topics as follows; Bandwidth constraints (8%), exposure of institution information to attacks (39%), device and data losses (13%), data ownership problems (25%), and spreading of malware (15%). With an increasing reliance on BYOD new and emerging software threats that target them specifically have also been on the rise. Viruses, for example, can infect one cellular phone and then spread to other devices via the network. Threats such as bluejacking and bluesnarfing where actual theft of data from Bluetooth enabled devices (including both mobile phones and laptops): contact lists, phonebooks, images are also on the rise.

Varied use of mobile devices within the organization network is likely to allow viruses and malware infections to proliferate the network, hence, exposing the institutions to information security incidents. [36][38] [39]; [40]. As pointed out by [41], protecting devices from infection of malware and viruses is a big challenge. A network admin in one of the institutions said; *"At our learning institution, blocking access to restricted applications is a challenge. Users exchange information through social media sites and share conference facilities using the institution's network. During this sharing, sometimes, institutions accounts are used".*

As much as staff and students may want to be secure while using institutions information [43] controlling downloaded information on BYOD devices is a challenge [39] because downloaded data can easily be accessed by friends who borrow the gadget. This introduces third party individuals or organization to the network who may try to gain unauthorized access to organizations' information depending hence, introducing a bridge to confidentiality [39] [45] [41] Likewise, users who grant permissions such as push notifications create another security loophole which enables installation of malicious applications onto the network [6]

Generally, as [47] puts it, there is a challenge in accounting for network access by BYOD devices for both students and staff and hence, protecting these devices from malware and viruses' infection is almost impossible. As one of the information security administrators reported,

"The learning institutions is not able to account for every device and its security status, this is because there is a big challenge to monitor who accesses these devices and what they do with them while connected on the network."

[41] suggest that theft and loss of mobile devices is rampant within learning institutions. These loses expose the institutions' information to CIA breaches (e.g. emails, financial information). Stolen information can also be used by malicious attackers to blackmail the victims especially if the gadget contained personal private information too. Users are the enemy within the organization. [43] argues that a bigger risk to institution's information is the insider. Insider threats emerge when an employee bypasses BYOD security controls to gain access to unauthorized areas. According to [4], curious and naughty students have always found themselves trying out their new learned skills on the institution's network. This activity is usually attempted remotely using their own gadgets with the help of open source hacking tools. This has brought down websites and corrupted information which would have been minimal without BYOD.

2.2.5 Are there any efforts from the institution's side to assist deal with the identified challenges?

The researcher sought to know whether the universities had put any measurer(s) to address the negative impact(s) brought by BYOD. 75% of the respondents indicated NO measurer(s) implemented while a mere 25% were positive about security controls implementation. For the positive response participants, it was noted that the main information security controls implemented included user authentication, system firewalls and antivirus software. NIST 800-30 guideline of information security recommend a layered approach to information security, which implies that the measures implemented in these environments were inadequate to fight against the challenges brought about by BYOD.

2.2.6 In the past six months, did you ever experience any information security attack(s) as a result of adopting BYOD within your institution?

The researcher sought to find out the recent and frequent attacks experienced on the university's information systems as a result of adopting BYOD. This was an open ended question posed to both questionnaire and interview respondents. The analysis indicated a high magnitude of malware attacks at 43% while student hackers who consistently tried to bring down websites and /or access the university's sensitive information followed closely at 40%. Theft of devices was at 10% while Denial of Service (DoS) attacks staggered at 7%.

With the introduction of BYOD in campus, young exploratory students always access inappropriate sites on the Internet, often engaging in illegal downloads from P2P, frequently visiting malware-infected sites and downloading questionable applications using personally owned devices on the institutions network with minimal oversight from the IT staff. As [48] puts it, these students are intelligent, curious, daring to use new tools and consistent in exploring the network. Their intrusive nature increases attacks on the network since their gadgets are not well protected

According to [49] the amount of malware for mobile devices keeps growing. Every quarter 1.5 to 2 million new malware variants are discovered. As of the end of 2019, there were over 30 million malware variants in total.

2.2.7 Do you receive any training from your institution on how to effectively protect yourself and the institution's information resources from attacks?

This question sought to establish whether BYOD users had been sensitized on security attacks and protection while using their devices on the university network. 58.5% of the respondents revealed that there was no form of training conducted with most of users citing major challenges on the use of the learning management system. The remaining percentage of respondents who acknowledged some form of training were university staff. Majority of users (71%) indicated their inadequacy in terms of user and technical skills when it comes to the use of ICT for Educational purposes. Due to limited budgets assigned to ICT improvement within institutions, users have been encouraged to acquire their own devices for use to keep up with the large number of students admitted in the universities. In the bid to achieve institutional objectives, institutions have invested in ICT infrastructure which includes allowing for Internet connectivity to other devices [50][51] but not training and awareness needs.

Respondents confirmed that despite the rampant BYOD security challenges and attacks within the campuses, there has been minimal training and sensitization on information security for users. Significant efforts have majorly been directed to policy and technical implementations. Statistics also indicate inadequate knowledge on information security for both staff and students despite the sophisticated BYOD device ownership. These condition calls for the need for capacity building for staff and running sensitization programs for students to improve the security of the information system with BYOD adoption in mind.

2.2.8 If attacked, is your institution able to continue with daily operations?

This question was posed to the ICT administrators because they are the ones in-charge of business continuity plans. Only 36% or 4 of the 11 respondents acknowledged having business continuity plans in place. This means that in case of an attack, most of the learning institutions are not be able to serve their clients and may not even continue operating because of loss of information and other resources.

University employees handle extremely sensitive details about students, staff members, research data and patients from institutions' clinics and hospitals. Use of personal digital devices in such environment requires that the organs meet compliance regulations of the information entrusted to the institution, backups of such data is paramount however efforts to comply with this goal has been hampered by the limited resources at hand, since the security teams tend to be perennially understaffed and underfunded. Given the kind of information acquired and stored by these institutions, this may be a very serious oversight. Continuity plans such as backing up data and having other redundant sites are crucial to every institution.

2.2.9 State any efforts and future plans by your institution to deal with other identified security challenges not currently addressed?

This question sought information from ICT administrators and management about the institution's commitment towards securing the information systems. Responses received pointed at improving the ICT infrastructure by increasing funding. This will ensure the learning institutions are able to implement adequate security controls. Training needs towards information security for both staff and students was highlighted. Policies, guidelines and procedures were also mentioned and management was keen on ensuring their implementation.

Higher learning institutions provide a wide range of information resources that attract hackers and other cyber criminals. BYOD adoption among these institutions has exposed student, staff and institution's information to major cyberattacks due to inadequate security controls. With the implementation of "traditional security controls" which include firewalls, antivirus and IDS, BYOD attacks have been on the rise because of their varied sources. Major information security challenges such as bandwidth inadequacy, information attacks due to malware, device losses and Denial of Service (DOS) attacks have been on the rise despite little security control implementation. Information gathered from this research reflect poor adoption of BYOD within these institutions; there has been neither sensitization and training for the users nor existent business continuity plans as outlined in [52] documentation.

3. PROPOSED INFORMATION SECURITY CONTROLS FOR A BYOD ENVIRONMENT

Information security controls are mitigation strategies implemented by an organization to detect, deter or correct attacks directed to the organization information system resources [53] The selection of information security controls plays a major role in ensuring business continuity in any information system environment.

Legacy information security strategies implemented in any computer networked environment usually involve physical, technical and administrative mitigation strategies which usually detect, deter and/or correct the security breach at hand of which are inadequate for the BYOD environment [54].

Due to the limited ICT infrastructure budgets, higher learning institutions' policy on information security allows the deployment of 'baseline' security measures, which has led to a continued increase in the number of security breaches. Literature indicate that over 60% of learning institutions have employed traditional security countermeasures which include anti-virus software, firewalls, anti-spyware software, virtual private networks (VPN's), vulnerability/patch management, encryption, and Intrusion Detection Systems [55] [56]. This has however not deterred the frequent BYOD targeted attacks due to increased internal and external activities.

[57] on recommendations for mitigation strategies in a BYOD environment start by proposing a unique security strategy for BYOD since it is "a project initiated by the users but not the organization" therefore posing unforeseen challenges. The authors state the importance of treating BYOD risks and challenges differently because most institutions have found themselves in them without much control. To secure information resources in a BYOD environment, simplicity with effectiveness should be combined.

3.1 BYOD Policy

A policy specifies an organization's security posture, defines and allocates functions and responsibilities, grants authority to security professionals, and identifies the incident response processes and procedures [58]. A BYOD policy should therefore be a well thought document that specify who, what, when, why and how of accessing, using, modifying and sharing information resources and educate employees on the best practice of data security.

A policy elaborates matters concerning eligibility, allowed devices, service availability, rollout, cost sharing, security, acceptable use, support and maintenance [59]. A BYOD policy according to [10] may cover Mobile Device Management(MDM), Mobile Application Management (MAM) and Identity Access Management (IAM). These three address the mobile device, mobile application and user access security strategies. MDM outlines the protocols for accessing data from within and remote locations, the applications manager monitors what application to be run on the mobile devices while IAM highlights user authentication. Mobile device management (MDM) solutions offer a balance between total control for employers and total freedom for employees, offering the ability to deploy, secure, and integrate devices into a network and then monitor and manage those devices centrally. Updating of BYOD devices and patching application systems, vulnerability checking to probe possible or potential weak points in the security infrastructure using "red teaming" or "penetration testing." Is another step towards prevention [60][61]; [62]; [63].

BYOD policy should be audited and tested regularly protect while serving the interests of both the user and information resources. The BYOD security specifies punishment of employees that fail to adhere to policy statements. The policy should also include and enhanced education and training program to inform students and staff of institutional policies and guidelines of using BYOD devices in order to make information security efforts more effective [64]

Encryption

Encryption addresses the security for data both at rest and in transit. Encryption technologies scramble data so that only people with the decryption keys can have access. Encryption can be applied in organizational emails, VPNs, passwords and even webpages. Encryption protects sensitive information from unauthorized people.

Encrypting information in transit within the BYOD environment prevent unauthorised access and hence enhances integrity and confidentiality [65] [66].

Risk assessment

Identifying the risks, threats and challenges that present themselves in a BYOD environment helps in alleviating these threats. A risk assessment will help in identifying assets and registration of devices that are allowed to access the network for easy authentication of the devices [58].

Risk assessment will help in identifying sensitive ICT resources that need limited access so that technological and human aspects of security are employed to protect them [67] [10]. also recommends in-depth risk assessment using methodologies such as ISO 27005 and NIST SP 800-30 to help determine appropriate controls for BYOD environments.

Remote Management and Surveillance

Loss of physical ICT storage devices are rampant in a BYOD environment. These devices mostly contain sensitive and private institutional information. Remote switching off and wiping of the devices should be made possible to protect the organizations' information [69].

Remote login should be restricted to a few individuals. SSO should never be allowed especially to individuals logging in remotely.

Surveillance involve monitoring of the security environment aimed at developing situational awareness to adapt to fast-changing BYOD circumstances and mobile threats [70]. Surveillance typically uses information generated from strategically placed 'sensors' augmented with visualization tools to increase security managers' understand ability of the situation [70] [69] [72]. Information collected is typically sourced from systems and applications software [73] including intrusion detection systems that report on the number of attacks, degree of attack propagation, and type of attack [70].

3.2 Other Information Security Control Strategies

Many more actions can be done to help protect information in a BYOD environment. Additional strategies include; consider implementing Enterprise Content Management (ECM) system, beware of vendor access, achieving compliance, WI-FI management/network segmentation, avoiding storage of sensitive information on mobile devices, having adequate technical support for ICT services, abandoning legacy systems, keeping track of inventory and containerization which separates the attacker and/or attacked area from other (unaffected) areas [75].

4. CONCLUSION

This study sought to identify the information security challenges and risks in higher learning institutions due to BYOD adoption. The study also proposes recommendations for information security controls in this environment. According to the respondents' views,

BYOD adoption is on the rise and has become inseparable part of today's academic and organizational system. Despite the convenience, BYOD is accompanied with lots of challenges and risks to institutional information resources.

In order to support and make BYOD adoption more beneficial, there is need for institutions to enhance their network infrastructure by implementing adequate security controls to counter the risks introduced on the network which can only be possible through top management support for these activities. It can also be noted that although insiders pose the biggest challenge to information systems security, implemented controls should embrace simplicity to users and security to technology. To sensitize users on the need to stay safe, regular training and awareness campaigns should be done. System audits are also crucial in establishing the weaknesses an information system. Top management should help in all these activities by taking information security as a key component and function of management. Structured approach to security implementation can be realized through formation of information security team adequately advice and protect the institution's resources

5. RECOMMENDATIONS FOR FURTHER RESEARCH

Due to the dynamic nature of BYOD within higher learning institutions, there is need to constantly identify the organization's sensitive information resources' security and highlight the needs for improving the same. Risk assessment as mentioned in the review is one of the best security control to secure a BYOD ecosystem. Further research is therefore recommended to develop a standard information security risk assessment model that will be used to identify threats and vulnerabilities within the BYOD academic environment. This will help prioritize security of sensitive areas because of the limited budgets allocated to ICT services within the learning

6. ACKNOWLEDGMENT

I would like to express my deep and sincere gratitude to my research supervisors Dr, Muhambe, T. Mukisa and Dr, Makiya, C. Ratemo for providing invaluable guidance throughout this research and my family for their support and valuable prayers during the time of writing this paper

7. REFERENCES

[1]. Van Leeuwen, D. 2014. "Bring Your Own Software," Network Security (3), pp.12-13.

[2]. Marcus, J. 2015. Is BYOD Trend Fading. Technivorz. Retrieved from https://technivorz.com/is-byod-trend-fading.

[3]. Gartner. 2013. Employees to Supply Their Own Device for Work Purposes. Retrieved May 28, 2020, from Gartner: http://www.gartner.com/newsroom/id/2466615

[4]. Khan Rahat Afreen. (2014). Bring Your Own Device (BYOD) in Higher Education: Opportunities and Challenges. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), 233-236.

[5]. Michael E. Whitman, Herbert J. Mattord. 2011. Cengage Learning, Jan 1, 2011 - Computers - 656 pages.

[6]. Armando A, G. Costa, A. Verderame, and A. Merlo, 2014. "Securing the 'bring your own device' paradigm," Computer, vol. 47, no. 6, pp. 48–56, 2014.

[7]. Power, D. 2012. BYOD: is Bring your own Devise" good for enterprise business. sprout.

[8]. Beckett, P. 2014. BYOD – popular and problematic. Network Security, 7-9.

[9]. Neo Sesinye 2018. Cyberattacks on educational institutions n the rise. Retrieved from https://www.itnewsafrica.com/2018/10/cyber-attacks-on-educational-institutions-on-the-rise on 12/7/2020

[10]. Brook Chris, 2020. The ultimate guide to BYOD security: overcoming challenges, creating effective policies, and mitigating risks to maximize benefits. Retrieved from https://digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating 2/11/2020

[11]. Cisco. 2012b. Cisco Bring Your Own Device. Retrieved May 21, 2020, from http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unifi ed_Access/byoddg.html

[12]. Cisco. 2012a. BYOD Security Challenges in Education: Protect the Network, Information, and Students. Retrieved march 22, 2020, from https://www.cisco.com/web/strategy/docs/gov/security_challenges.pdf

[13]. Bradford Networks. 2013. The impact of BYOD in education. Retrieved August 27, 2020, from http://th-ebooks.s3.amazonaws.com/The_Impact_of_BYOD_in_Education.pdf

[14]. ISDecisions (n.d). Network security in Universities, Colleges and Schools. Retrieved from https://www.isdecisions.com/blog/it-management/network-security-in-universities-colleges-and-schools/ on 21/10/2020

[16]. Thomas, S. M. 2014. Bring your own Devise. Benefits, risks and control techniques, pp. 1-6.

[17]. Gimenez, O., & Wang. 2015. Remote Mobile Screen (RMS): an approach for secure BYOD environments. *CSE Conference and Workshop Papers*, (p. 238). Nebrasca.

[18]. Negrea, S. 2015. *BYOD boundaries on campus*. Retrieved october 11, 2020, from UB University Business: https://www.universitybusiness.com/article/byod-boundaries-campus

[19]. Fortinet 2018. Top Cybersecurity Threats Active in the Education Sector Today – and Why You Should Care. Retrieved from https://www.csoonline.com/article/3250862/top-

cybersecurity-exploits-active-in-the-education-sector-today-and-why-you-should-care.html on 21october 2020

[20]. Ounza, J. E., Liyala, S., & Ogara, S. 2018. Emerging Security Challenges due to Bring Your Own Device Adoption: A Survey of Universities in Kenya. *International Journal of Science and Research (IJSR)*, 345-350.

[21]. Brian, T. 2013. *The security implication of BYOD*. Network Security, , 12-13.

[22]. Stavert, B. 2013. Bring your own device (BYOD) in schools. NSW Department of Education and Communities

[23]. Koh, E. B., Oh, J., & Im, C. 2014. A Study on Security Threats and Dynamic Access Control Technology for BYOD, Smart-work Environment. International Multi-conference of Engineers and Computer Scientists, 2, pp. 1-6. Hong Kong.

[24]. Brian, T. (2013). The security implication of BYOD. Network Security, , 12-13.

[25]. Kang D, Oh J, and C. Im, 2013. "A study on abnormal behavior detection in BYOD environment," Int. J. Env. Ecol. Geol. Geophys. Eng., vol. 7, no. 12, pp. 612–615

[26]. Israel, Glenn D. 1992. Sampling the Evidence of Extension Program Impact. Program Evaluation and Organizational Development, IFAS, University of Florida

[27]. Wilknison, D., & Birmingham, P. 2003. Using Research Instruments: A Guide for Researchers. Psychology Press.

[28]. Elizabeth A Buchanan Erin E Hvizdak 2009. Online Survey Tools: Ethical and Methodological Concerns of Human Research Ethics Committees. Journal of Empirical Research on Human Research Ethics 4(2):37-48.

[29]. Chris Brook 2020. The ultimate guide to BYOD security: overcoming challenges, creating effective policies, and mitigating risks to maximize benefits. Retrieved on 21/10/2020 from https://digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating

[30]. Shneiderman, B., & Plaisant, C. 2005. Designing the User Interface. Chapter 14.5: Information Visualization (pp. 580–603). Boston: Pearson

[31]. Akin-Adetoro, Kabanda 2015, Contextualizing BYOD in SMEs in developing countries. Proceedings of the **2015** Annual Research …, **2015** - dl.acm.org.

[32]. Attewell, J. 2005. Mobile technologies and learning: A technology update and m-learning project summary. London: Learning and Skills Development Agency http://www.lsneducation.org.uk/user/order.aspx?code=041923&src=XOWB

[33] French, A. M., Guo , C., & Shim, J. P. (2014). Current Status, Issues, and Future of Bring Your Own Device (BYOD). Communications of the Association for Information Systems, 10, 192-197.

[34] Gessner, D., Girao, G., & Li, W. (2013). Towards a User Friendly Security enhensing BYODSolution,. Nec Tech J, 7, 113.

[35]. H. Holm, K. Shahzad, M. Buschle and M. Ekstedt, 2015. Predictive, Probabilistic Cyber Security Modeling Language," in *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 6, pp. 626-639, doi: 10.1109/TDSC.2014.2382574

[36]. Coleman, L., and B. Purcell. 2015. Data breaches in higher education. Journal of Business Cases and Applications. 15: 1–7

[37]. Gajar P, A. Ghosh A, and. Rai S, 2013."Bring your own device (byod): Security risks and mitigating strategies," J. Global Res. Comput. Sci., vol. 4, no. 4, pp. 62–70,

[38]. A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner 2011. A survey of mobile malware in the wild. In Proc. of ACM Worksgop on Security and Privacy in Smartphones and Mobile Devices (SPSM), pages 3– 14,

[39]. Francis A. Kwansa, Katerina Berezina, Cihan Cobanoglu, Brian L. Miller, 2012. The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth International Journal of Contemporary Hospitality Management ISSN: 0959-6119,

[40] Eilertson EE, Ertoz L, Kumar V 2004. MINDS: A New Approach to the Information Security Process. Paper presented at the 24th Army Science Conference, Dec.

[41]. Shumate T, Ketel M- 2014. 2014 - Bring your own device: Benefits, risks and control techniques, ieeexplore.ieee.org;

[42]. Wang Y, Wei J., and Vangury K. 2014, "Bring your own device security issues and challenges," in Proc. IEEE 11th Consumer Communications and Networking Conference (CCNC), Jan. 2014, pp. 80–85.

[43]. Lampson BW 2004. Computer Security in the Real World. Computer 37 (6):37-46

[44]. Potts, M. 2012. The state of information security. Network Security, 2012, 9-11. doi:10.1016/S1353-4858(12)70064-8

[45]. A. Armando, R. Carbone, L. Compagna, &Lt 2014 SATMC: A SAT-Based Model Checker for Security-Critical Systems", In the Proceedings of the 20th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2014), pp. 31--45, Springer, France, April 2014

[49]. Kumari, Debbarma and Shyam 2015. Security Problems in Campus Network and Its Solutions , www.researchgate.net › publication › 224771078_Security_problems_in_campus_network_and_its_solutions.

[50]. McAfee Labs. 2018a. *McAfee Labs Threats Report, December 2018*. Santa Clara, CA: McAfee Labs.

[51]. Gikas, J., & Grant, M.M. 2013. Mobile computing devices in higher education: Student perspectives on learning with cellphones, smartphones and social media. The Internet& Higher Education, 19(1), 18-26.

[52]. Salaway G, Caruso JB. 2007. The ECAR study of undergraduate students and information technology, : key findings. At: www.educause.edu/library/EKF0706. Accessed: June 26, 2009

[53]. ISO/IEC 27001, 2013 Information technology — Security techniques — Information security management systems — Requirements. https://www.iso.org/standard/54534.html accessed on 21/10/2020

[54]. Souppaya m, Scarfone K (2015) - NIST special publication, - telehealthtechnology.org

[55]. Stanford Musarurwa, Attlee M. Gamundani and Fungai Bhunu Shava 2019. An Assessment of BYOD Control in Higher Learning Institutions A Namibian Perspective. ResearchGate.

[56]. Richardson, J. T. E. 2011. "Eta Squared and Partial Eta Squared as Measures of Effect Size in Educational Research." *Educational Research Review* 6: 135–147

[57]. Debar H, Tombini E 2005. Accurate Detection of HTTP Attack Traces in Web Server Logs. Paper presented at the European Institute for Computer Antivirus Research (EICAR) 2005 Conf. Best Paper, Saint Julians, Malta, Apr

[58]. Hamill JT, Deckro RF, Kloeber-Jr. JM 2005. Evaluating Information Assurance Strategies. Decision Support Systems 39:463-484

[59]. Park S, Ruighaver AB, Maynard SB, Ahmad A 2011 Towards Understanding Deterrence: Information Security Managers' Perspective. Paper presented at the International Conference on IT Convergence and Security 2011, Suwon, Korea,

[60]. Franklin, Onyechere and Ismail, Mohamed 2015. The future of BYOD in organizations and higher institution of learning. International Journal of Information Systems and Engineering VL – 3

[61]. Forcht KA 1994. Computer Security Management. Boyd and Fraser, Danvers, MA

[62]. Arce I, McGraw G 2004. Why Attacking Systems Is a Good Idea. IEEE Security & Privacy 2 (4):17-19

[63]. Evans S, Kyle DH, Piorkowski J, Wallner J 2004. Risk-Based Systems Security Engineering: Stopping Attacks with Intention. IEEE Security & Privacy 2 (6):59-62

[64]. Ray HT, Raghunath, Kantubhukta HR 2005. Toward an Automated Attack Model for Red Teams. IEEE Security & Privacy 3 (4):18-25

[65]. Graham D 2003. It's All About Authentication. SANS Institute,

[66]. Dunn TS 1982. Methodology for the Optimization of Resources in the Detection of Computer Fraud. University of Arizona

[67]. Kankanhalli A, Teo H-H, Tan BCY, Wei K-K 2003. An Integrative Study of Information Systems Security Effectiveness. International Journal of Information Management 23:139-154

[68]. Liu S, Sullivan J, Ormaner J 2001. A Practical Approach to Enterprise IT Security. IEEE IT Professional 3 (5):35-42

[69]. Klete H (ed) 1975. Some Minimum Requirements for Legal Sanctioning Systems with Special Emphasis on Detection. Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates. National Academy of Sciences, Washington, D.C.

[70]. Brand RL 1990. Coping with the Threat of Computer Security Incidents: A Primer from Prevention through Recovery, CERT, Pittsburgh, Pa., June 1990.

[71]. Doyle J, Kohane I, Long W, Shrobe H, Szolovits P 2001. Agile Monitoring for Cyber Defense. Paper presented at the 2001 DARPA Information Survivability Conference & Exposition II (DISCEX '01).

[72]. Ohno K, Kike HK, Koizumi K 2005 IPMatrix: An Effective Visualization Framework for Cyber Threat Monitoring. Paper presented at the Ninth Int'l Conf. on Information Visualisation (IV5), London, England,

[73]. CSSP 2009. Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-InDepth Strategies. Control Systems Security Program, National Cyber Security Division, Department of Homeland Security,

[74]. Dourish P, Redmiles D 2002. An Approach to Usable Security Based on Event Monitoring and Visualization. Paper presented at the 2002 Workshop on New Security Paradigms, Virginia Beach, Virginia, USA, Sep.

[75]. Grance T, Kent K, Kim B 2004. Computer Security Incident Handling Guide (trans: Computer Security Division ITL). NIST Special Publication. National Institute of Standards and Technology, Gaithersburg, MD