Enhancing Bring Your Own Device Security in Education

Article *in* Journal of Science and Technology · January 2021

DOI: 10.55662/JST.2021.2401

3 authors, including:

Richard Ntwari
Mbarara University of Science & Technology (MUST)
2 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Fred Kaggwa
Mbarara University of Science & Technology (MUST)
15 PUBLICATIONS **19** CITATIONS
SEE PROFILE

ENHANCING BRING YOUR OWN DEVICE SECURITY IN EDUCATION

Author(s): **Richard Ntwari*, Annabella E. Habinka** & Fred Kaggwa*****

* PhD Scholar, Mbarara University of Science and Technology, Mbarara, Uganda

** Associate Professor, Makerere University, Kampala, Uganda

*** Lecturer, Mbarara University of Science and Technology, Mbarara, Uganda

DOI: doi.org/10.55662/JST.2021.2401

ABSTRACT

Background: The acceptance and use of personal devices at educational institutions is on the rise, resulting in the education sector's adoption of Bring Your Own Device (BYOD). The institutions benefit from cost reduction in buying and managing IT devices as users purchase and bring their own devices. Users benefit by accessing learning materials and collaboration anytime, anywhere while on the move via institutional network. However, literature on BYOD indicates that various challenges are faced with usage of BYOD such as loss/stolen devices, malware, lack of policy, user negligence among others. This paper examined the literature in order to identify BYOD challenges, solutions, and guidelines that would inform secure BYOD usage in education.

Methods: Beginning with a search of selected databases, a systematic review of the literature was conducted. The database and back search generated 1594 items, 14 of which were deemed eligible for inclusion. The People Policy Technology (PPT) approach was used in identifying challenges from literature through grouping them under the Technology challenges, People challenges and Policy challenges. The BYOD security framework was utilized to develop a mitigation strategy.

Results: Various risks and threats were identified under the People, policy and technology themes. They include lost/stolen device, lack of policy, inadequate controls, connecting via

unsecure networks, malware such as virus, data leakage. The BYOD security framework was followed to give systematic guidelines and controls in overcoming the challenges. The guidelines included BYOD policy development and implementation with in the institution, device enrolment and management using the MDM, scanning for malware, software updates, and regular backups among others.

Conclusion: BYOD phenomenon is on the raise and here to stay. It has various benefits but these can be shadowed by threat identified in this review. Before implementing BYOD, educational institutions should ensure that an acceptable BYOD policy is in place to instruct users on how to behave while using BYOD. Users should be trained sufficiently on how to secure their devices and data while using BYOD. Technological solutions such as MDM, antivirus software and NAC should be deployed to manage both devices and data in the BYOD environment. However these solution should be used in a balanced manner that does not hinder usability.

Keywords: Bring your own device (BYOD), mobile devices, security, education, Controls

INTRODUCTION

Bring Your Own Device (BYOD) is a policy that allows employees to access the organization's data and services using personal devices such as a computer or mobile device across a network (Akande & Tran, 2021). BYOD allows the organization to extend its infrastructure without investing much more in its own equipment (Alotaibi & Almagwashi, 2018; Gupta et al., 2019). Employees benefit from BYOD adoption because it eliminates the need for separate personal and professional devices (Harris & Patten, 2014). Other employee benefits include higher productivity, job satisfaction, and mobility due to the ability to access information instantly using a mobile device (Alotaibi & Almagwashi, 2018). According to Ontech (2022), employees who use their own devices are more productive, according to 49% of them. Using a single mobile device for data access, according to 78% of employees, helps them balance their personal and professional lives.

As technology advances, it becomes increasingly important for students to learn from the wide range of educational apps and programs available to them. A BYOD program allows students to access classroom materials using their own laptop, tablet, or smartphone (Afreen, 2014;

Miller & Welsh, 2017). Students can access course content and communicate with lecturers and classmates from anywhere using mobile computing devices (Gikas & Grant, 2013). Similarly, educators have begun building learning environments that take use of students' devices/technologies in order to improve students' learning experiences and outcomes (Hakami, 2020). Due to the use of mobile devices in learning, BYOD applications are strongly linked to mobile learning (Sundgren, 2017). Allowing students to use their own gadgets during and after lectures, such as cell phones and iPads, has the primary benefit of increasing interaction between lecturers and students (Hakami, 2020).

Various studies have explored the application of BYOD in education. For example, (Masilo et al., 2021) investigated students' intentions to use a mobile device and the factors that influence actual use of the relevant application, as well as how their views regarding the device influence the intention. (Ziemba & Eisenbardt, 2021) conducted research to determine how academic work, particularly teaching and research, changed during the pandemic, as well as the use of ICT to support this work, and what academics' expectations are for their work following the epidemic. Allowing students to use their own devices in classroom activities has been found to create a more comfortable learning environment in general. The BYOD strategy enhances students' productivity because they were already comfortable with their personal devices.

Over the years, the usage of personal devices in education (BYOD) has increased. However, because personal devices are outside of school control and may lack essential security protections, BYOD puts schools at risk of disclosing sensitive information assets such as students' Personal Identification Information (PII). According to (Palanisamy et al., 2022), the key threats in BYOD include lost or stolen devices, malware, data leakage, network interceptions, and a lack of policy. These threats are present in education settings, as literature review indicates that most schools consider adoption without taking security into account. As a result, the purpose of this study is to come up with mitigation methods that will solve these security risks.

METHODOLOGY

A three-step methodology was employed. To begin, the researchers conducted a thorough literature analysis to determine the main concerns about BYOD security and the appropriate

solutions to improve them (Kitchenham et al., 2009). The People Policy and Technology model (Schlarman, 2001) was then used to identify risks from literature, and a BYOD security framework by (Zahadat et al., 2015) was implemented to align the mitigation strategy with the identified risks. The following steps were taken during the systematic literature review:

Search Methodology and Eligibility Criteria

IEEE Explorer, ACM Digital Library, Taylor & Francis, Emerald Insight, and Science Direct databases were searched to find peer-reviewed journal publications published between 2010 and 2020 using a keyword search. Some of the keywords included "mobile device security", "Bring Your Own Device", "Bring Your Own Technology", "BYOD", "Smartphones", "BYOD policy" and "Education". Because BYOD security technology has improved greatly since 2011, only publications published between 2011 and 2020 were evaluated. A total of 1594 papers that resulted were subjected to inclusion/exclusion criteria before any undesirable findings were eliminated. To eliminate a number of irrelevant results, the study only considered peer-reviewed articles from a conference or journal. As a result, non-academic publications including journals and white papers were left out of the study. In the second step, only papers written in English and with the complete text were considered. Following that, a preliminary scan of the contents of the papers was performed for screening purposes. Finally, publications that explored into extensive detail about the risks and controls associated with BYOD were chosen. The research looked at a total of 14 papers.

Data Extraction and Synthesis

The findings were organized using a deductive theme analysis based on the People Policy Technology (PPT) paradigm(Schlarman, 2001). The three core elements of the PPT model are 1)People that are in charge of carrying out and supporting the security procedure, 2) Policy, which is used to describe supporting procedures and provide clear guidance for good security behavior, and, 3)Technology, which comprises security-related items, technologies, and resources. The alignment of technological and social factors is essential to maximize cyber security measures, necessitating a holistic approach to fully appreciate the security process. As a result, the PPT model is particularly valuable because it emphasizes the importance of all three security criteria in a balanced manner.

Controls are mapped to risks using a BYOD security model defined by (Zahadat et al., 2015). This approach is a seven-step iterative procedure for managing the security risks associated

with BYOD. Its goal is to provide a step-by-step risk management process for BYOD security that spans the whole lifecycle of the device (which is divided into seven phases, beginning with an employee requesting permission to allow his or her device to access company resources and ending with the device being de-provisioned). The phases are Plan, Identify, Protect, Detect, Respond, Recover, and Assess and Monitor. As a result, in this work, this model was used to build a modular and sequential mitigation technique. Finally, the two models were used to describe the mitigation options that were discovered..

FINDINGS

The identified risks were mapped using the PPT Model as follows;

People

It must be assumed that when personal gadgets are utilized in the office, users' careless or reckless behavior in private will be carried over (Disterer & Kleiner, 2013). Inadequately secured mobile devices allow for unauthorized data use and modification as a result of intentional or unintentional actions. Human carelessness is at blame for majority of security concerns and breaches. This frequently happens when an employee is not aware of the company's policies, especially about the importance and specificity of device security. Furthermore, poor or no training will almost likely result in unnecessary personnel errors, jeopardizing the security of your firm (Harris et al., 2012).

Policy

Mobile device use in schools without a Bring Your Own Device (BYOD) policy is a concern, as it can lead to unsecure and inappropriate mobile device use. The insecurities are due to a lack of network controls, education, and communication technologies and systems (Kadimo et al., 2018). Data leak is a serious concern and a major factor in information security violations due to users' inability to follow policies while using personal mobile devices. (Giwah, 2018).

Technology

Devices: Because of the compact and portable nature of the devices, they are easily forgotten, misplaced, or stolen. This could put you in a risky scenario where your personal information is at risk (Palanisamy et al., 2022). Furthermore, since personal devices transmit and store data that is an organization's asset, and if hacked, might have terrible consequences, organizations

should be cautious about the intentions of BYOD users. Hackers take advantage of security flaws, misplaced mobile devices, unauthorized third parties applications, and companies' improper data disposal methods. (Giwah, 2018). Wearable devices used by employees on company premises, such as smart watches, have also been raised as a potential data security problem, with few solutions available (Al-Harthy et al., 2019). Because compromised websites and illegal programs are accessed via personal devices in BYOD, malware threats are introduced (Palanisamy et al., 2022). While these devices have built-in security safeguards, users often ignore them for convenience, the freedom to install unapproved software, and carrier migration (Wani et al., 2019). The "jailbreak" method disables the underlying security architecture, leaving devices vulnerable to security assaults at all times. Organizations find it incredibly challenging to manage mobile platforms due to their heterogeneity, particularly variances in how underlying security measures are handled. Rogue Access Points (RAP) are mobile devices that use tethering and Wi-Fi hotspot features to get around corporate security restrictions and access content that would otherwise be banned by company policy (Al-Harthy et al., 2019; Palanisamy et al., 2022). This opens the door for corporate data leaks, leaving standard security controls like firewalls ineffective.

Operating software and applications: Operating systems and applications on mobile devices must be updated on a regular basis (M. Ratchford et al., 2022). However, this may be the least concern for stakeholders in education domain. The implication is that these devices will become vulnerable to security problems due to a lack of software updates. Secondly, students and staff are free to load their smartphones with as many applications as they like. These could potentially install apps with undetected vulnerabilities or malware such as viruses (Madzima et al., 2014). As a result, BYOD exposes a business to information security threats, such as system malfunctions or malware infections, which affect data and information availability. Students utilize BYOD devices to access academic data, social networking sites, send emails, and download data from the internet, among other things. As a result, BYOD is likely to expose an institution to malware attacks that are difficult to detect in real time (Baillette & Barlette, 2018). Integrity, availability, and confidentiality can all be jeopardized by these security threats. Users' frequent downloading of mobile apps without considering underlying security risks; and the development of mobile platforms, which leads mobile devices to mimic traditional desktops and laptops, makes it easier for hackers to construct malware for them.

***Data*:** BYOD always changes the way a firm stores data and how non-corporate devices are likely to access it. As a result, BYOD and mobility provide new opportunities for individuals and data to be misused. Criminals might use a range of hacking tactics to gain access to network devices and compromise the complete data set (Madzima et al., 2014). Lack of appropriate security processes to detect and deter hackers could ruin the company's reputation and cause considerable financial loss. An organization's intellectual property and sensitive data can be easily lost or stolen if an insecure employee-owned device is lost or stolen (Madzima et al., 2014; Palanisamy et al., 2022; M. M. Ratchford & Wang, 2019). A device containing institution data can be readily stolen, or authorised users can provide unauthorised individuals access with the intent of sabotage. Mobile devices and BYOD become liabilities for institutions due to the possibility of theft and loss (Alotaibi & Almagwashi, 2018). As a result, corporate information stored on BYOD devices is very exposed to espionage.

***Network*:** It's challenging for businesses to decide which employees can access the workplace network using their own devices and what they can do once that is (Amoud & Roudies, 2017). Furthermore, the institutions may not have the resources to monitor the network.(Kadimo et al., 2018). As a result, cybercriminals will use these BYOD devices as a weak security link to launch attacks against an institution's information system. Some networked devices may be subject to security issues.(M. Ratchford et al., 2022). As a result, if an enterprise network contains a large number of operating devices, IT personnel will have a difficult time detecting those devices that have flaws. The device can also be used to create or connect to rogue wireless points, giving hackers access.

MITIGATION

Planning Phase:

Understanding the Business Environment is the first stage in the planning process. The planning process must be supported at the highest levels of management to guarantee that adequate time and human resources are available (Zahadat et al., 2015). The planning process necessitates extensive coordination among several disciplines and all stakeholders, as well as the identification of users and the resources they will use. A set of BYOD Specifications is necessary in the following phase to certify that BYOD devices meet functional and security

criteria (Souppaya et al., 2016). The standards should be revised on a regular basis to stay relevant. In consultation with all key stakeholders, develop a clear and comprehensive Bring Your Own Device policy. This should be done in compliance with any applicable rules or regulations. Organizational strategists must establish the rules, processes, and practices that will be utilized to administer and monitor the BYOD program (Baillette & Barlette, 2018). Statutory, regulatory, legal, security, environmental, and operational factors should all be factored into governance framework (Baillette & Barlette, 2018; Harris & Patten, 2014; Souppaya et al., 2016; Zahadat et al., 2015). When establishing which components of a BYOD security program are technologically enforceable and are enforced entirely through policy, it's critical to understand the limitations of mobile security solutions (Bello et al., 2015; Harris et al., 2012). Asset Management is the next phase, which needs organizations to specify what they are seeking to protect before they can expect to secure it. The correct technology, such as Mobile Device Management, must be adopted to provide adequate security control measures for the BYOD program.

Identify phase:

During the Identify phase, the devices are registered for the BYOD program, formally approved for use, and given appropriate security settings. The first stage in the BYOD Security Lifecycle's Identify phase is to register the devices that will require security (Wani et al., 2019; Zahadat et al., 2015). To be included in the organization's BYOD program, the user will bring their device to the registration procedure. As a result of the extra check, repeat offenders of BYOD or other security rules will not be placed in a position to jeopardize others. Before granting access to corporate resources or data, users should be taught on the system's rules and processes, as well as their specific role and responsibilities in implementing the system's security measures (Harris et al., 2013). This initial training helps to clearly communicate the standards of behavior expected of BYOD users while developing the business culture for BYOD. On a regular basis, user training should be examined for content updates, and users should be trained. Regular security training in a BYOD environment can help to reinforce security ideas and foster a culture of security responsibility and awareness (Harris et al., 2013; Palanisamy et al., 2022; Wani et al., 2019). The device will be evaluated by the company's designated department to confirm that it complies with the process's hardware and operating system requirements. Some companies might want to consider employee and device eligibility.

After that, the device should be provisioned according to the company's policies. Provisioning is the process of configuring all of the security setups, settings, apps, device profiles, and software certificates for the BYOD program (Zahadat et al., 2015). Depending on the organization's consent during the Plan phase, provisioning can take place over the air or in person.

Protect phase

The business must guarantee that the devices and data stored on them are appropriately protected throughout the BYOD life cycle after they have been provisioned and users have been correctly registered in the BYOD program. The following are the procedures used to safeguard the various layers:

Device level: A number of restrictions are in place on mobile devices to prevent illegal access and to aid in the eventuality of device loss or theft. Lock codes, sometimes known as passcodes, are the first type. A password, pin, or specified action is required to access a lock code on a mobile device. Passcode-protect all mobile devices (Souppaya et al., 2013). Requiring a passcode makes it more difficult for bad actors to gain access to the device. Allow devices to self-lock after a short period of inactivity(Harris & Patten, 2014; Souppaya et al., 2013). The most secure of these three options is a password. Geo-tracking can assist in the recovery of a misplaced smartphone. Geo-tracking is usually done with the help of an application that not only tracks the location of the phone using its Global Positioning System but also allows you to remotely lock and wipe it (Shumate & Ketel, 2014). A remote wipe enables for the total wiping of all data on a smartphone from a distance (Shumate & Ketel, 2014). Jailbreaking or rooting mobile device operating systems is not required. The risk of malware is greatly increased as a result of this (Harris & Patten, 2014; Wani et al., 2019). Update the device's operating system and applications as requested. The resolution of known vulnerabilities can be aided by updating software (Souppaya et al., 2013). Data on devices, especially removable memory cards, should be encrypted if at all practicable (Palanisamy et al., 2022). When data is encrypted, it is more difficult to access in the event of a breach.

Applications and data: Data stored on the device should be safeguarded by encrypting data communications and storage(Souppaya et al., 2016). Remote wiping is recommended in the case that the device is lost to prevent data from being recovered by an untrustworthy party (Harris et al., 2012; Souppaya et al., 2013). Wiping is especially important if the device is to

be reissued to another person or disposed off. To avoid malware, the organization should restrict which application stores a stakeholder can download applications from via the Mobile device manager (Alotaibi & Almagwashi, 2018; Palanisamy et al., 2022; Wani et al., 2019). Furthermore, the applications should be limited in terms of the data and services they can access on the device, such as the camera, contacts, location access, screenshots, and so on. Wherever possible, the technology team should vet these applications before recommending them to stakeholders, as this ensures policy compliance (Zahadat et al., 2015). After that, you can either whitelist (preferable) or blacklist which programs can be installed. To secure data against defects and vulnerabilities in the program, make sure the applications are updated on a regular basis.

Networks: Start by conducting a thorough review of your present technology network infrastructure and practices (Zahadat et al., 2015). This way, any potential cyber security flaws, difficulties, or conflicts with your present technological operations may be addressed before you start. To make your network more secure, you should use role-based access (Bello et al., 2015). That is, how much access each employee has is tied to their job role, and their access is limited to only the systems and information they need to do their job, limiting who can access your systems remotely and allowing restrictions on some applications or file sharing within your internal office network. Network Access Control (NAC) software guarantees that all devices connecting to your network meet basic requirements, such as having current software (Al-Harthy et al., 2019; M. M. Ratchford & Wang, 2019). Access to the network is prohibited to devices that do not match the standards until they are upgraded. Employ a VPN connection to connect to the network since it allows you to use secure protocols and encryption (Harris & Patten, 2014). Furthermore, connecting only devices with certain MAC addresses gives an extra degree of protection. MAC address filtering can be used by wireless access points and routers to control access (Zahadat et al., 2015).

***Users*:** Users can connect to the organization using their mobile devices in the expected areas and retain such relationships. Users have access to any resources that they are allowed to connect to within the organization, but they are not allowed to connect to any other resources. Employee education is critical (Harris et al., 2013). All staff should receive training on mobile device security issues and best practices. Training is critical, and it should be related to the policy about mobile devices.

Detect Phase

Changes in the technical environment frequently result in the formation of new attack vectors, even when equipment are effectively protected. As a result, in order for the organization to proactively prevent, respond to, and recover from intentional or inadvertent threat occurrences, numerous separate events must be identified. The detection process is multi-layered and can be accomplished in the following ways:

Vulnerability Detection: Software and configuration flaws can lead to unanticipated consequences, such as service outages, unauthorized access to business systems, and data loss or compromise (Harris et al., 2012). These flaws can be discovered by first ensuring that the device is operational, then probing it to check which services are active. The technical team of the organization must specify the criteria for vulnerability screening and detection while on the network (Zahadat et al., 2015). Vulnerability detection techniques or software can be used to test both systems and devices.

Malware Detection: Employee-owned devices pose a security risk since users have administrative control over them and are not always connected to secure networks as corporate devices (Baillette & Barlette, 2018). This might lead to the installation of malicious software on them, which could then be used to get access to employee-owned devices (Palanisamy et al., 2022). Anti-malware solutions can be implemented as a service within an enterprise. Signatures must be updated on a regular basis for these methods to operate (Souppaya et al., 2016). These solutions will ensure that enterprises' anti-malware is up to date; employees will no longer be responsible for keeping their antivirus up to date.

Attack Detection: Attackers may use vulnerabilities or malicious software that have not been identified, or that have been discovered but not fixed, to seize control of a network. The ability to detect a breach is crucial for guaranteeing a timely response that minimizes damage and makes recovery and risk mitigation easier (Scarfone et al., 2007; Zahadat et al., 2015). Intrusion detection systems (IDSs) enable detection of security breaches so that you can respond quickly. Intrusion prevention systems (IPSs) take it a step further by automatically activating network breach response steps to assist in the immediate containment of the attack (Zahadat et al., 2015). Security information and event management (SIEM) systems can assist in gathering data about

a network hacking attempt in order to identify the attack approach, which is valuable in preventing future attacks.

Respond

Mobile Device Manager establishes techniques and protocols for remote access of company data, as well as allowing IT access to any devices that may communicate with the business network, as well as the ability to terminate access or even delete data on stolen/lost device. (Alotaibi & Almagwashi, 2018; Baillette & Barlette, 2018; Palanisamy et al., 2022; Wani et al., 2019). For example, if particular applications are identified as the source of device infection, MDM should prevent them from being installed on BYOD-registered devices(Souppaya et al., 2016). Either the device's entire data is wiped, making it difficult for the thief to recover sensitive or medical information. Alternatively, data can be containerized and selectively deleted, leaving personal data undisturbed. Containerization is a practical solution because it just takes company data from the device while leaving personal data alone (Harris et al., 2012). The BYOD policy's list should also be updated, and all parties concerned should be informed as soon as possible. To eradicate the discovered vulnerabilities, use anti-virus, anti-malware, and firewall technologies (Souppaya et al., 2013). Furthermore, the IT department should provide appropriate training to stakeholders on standard operating procedures for responding to a security event or attack(Wani et al., 2019).

Recover

The recovery phase includes the measures necessary to avoid the loss of data saved on mobile devices. This phase begins with the identification of vulnerabilities or events, followed by the execution of corrective actions. If a device is lost, for example, IT may simply remove the data contained on the device and restore the deleted data to a new device from a backup(Palanisamy et al., 2022). In the case of network bleaching, replicas of your network environment are created in order to rapidly restore your company's network while you investigate the security breach. The next step is to investigate the attack strategy and determine how the attacker(s) gained access to the system(Zahadat et al., 2015). This assists in determining the cyber security gaps that caused the attack to occur, and measures may be put in place to prevent future attacks. In addition, ensuring that a Business Continuity / Disaster Recovery strategy is in place, which should harness the information gained in the aftermath of the disaster to discover methods to increase security measures(Baillette & Barlette, 2018). Investing in better security technology,

modifying laws, or increasing employee knowledge of their cyber security responsibilities are all options.

Asses and monitor

The BYOD program should be reviewed on a regular basis, taking into account organizational changes in the environment such as increased personal phone usage, changes in device specs, and device decommissioning(Souppaya et al., 2013; Harris & Patten, 2014; Bello et al., 2015; Zahadat et al., 2015). Maintain constant situational knowledge of the security and privacy postures of the system and organization to support risk management choices (Souppaya et al., 2016). One of the primary goals of monitoring is to ensure that the system and operational environment are monitored in line with the continuous monitoring strategy. Second, in accordance with the continuous monitoring strategy, continual evaluations of control efficacy are carried out(Souppaya et al., 2013). A security breach may occur if new organizational changes are not examined on a regular basis. Make sure that approved devices and apps are checked on a regular basis, and that any old devices, operating systems, or programs that fail to meet security standards are removed from the list. Those who have been affected should be notified as quickly as possible, and the process for transitioning to a new device should be examined into. Out-of-date software and operating systems should be prompted to be updated by employees. Devices that have been engaged in several security breaches should be decommissioned by the IT department (Souppaya et al., 2013). Decommissioning devices for leaving employees is also a vital step. Decommissioning devices for leaving employees is also a vital step. Decommissioning implies removing any access to services and privileges, as well as any security settings, software, or configurations put on the employee's device, in order to avoid data breaches. The results of ongoing monitoring operations are assessed and addressed, as well as a method for reporting management's security and privacy posture. Finally, continuing authorizations are provided based on the outcomes of continual monitoring methods.

CONCLUSION

Despite the fact that BYOD usage is expanding, the purpose of this article was to address a secure BYOD implementation gap in education. Several research on BYOD in education have

focused on the utilization of BYOD while ignoring the security component. To identify literature on security threats and issues in a BYOD environment, we did a systematic review. Using a PPT methodology, risks were identified in the literature. The papers examined revealed that risks exist at various network layers, most significantly lost devices, malware, insecure communication routes, malevolent users, and a lack of policy, among others. To patch the identified vulnerabilities, we employed the BYOD security framework. Implementing a BYOD policy as well as an MDM solution is essential because of the necessity for centralized management of all mobile devices that enter the network. User awareness training is a critical component of keeping organizations secure. Access to networks should be controlled using network access control technologies such as VPNs. Furthermore, intrusion detection and response tools should be used to detect any anomaly on the network. The organisation should ensure device decommissioning, so that company-sensitive data is removed from personal devices and networks for any exiting employee. This research based on a systematic BYOD approach due to requirement for a balanced combination of technology and policy management, which is critical in maintaining a desired level of security while providing various BYOD benefits to an educational institution.

FUTURE RESEARCH

The research's future objectives are to provide an integrated technological solution guided by policy to handle the inherent security challenges connected with the usage of mobile devices in education, particularly those that are not controlled by the organization, with a focus on resource-constrained environments. Many alternatives have been presented, however an assessment indicated that they are resource hungry, such as the need for continuous and rapid internet connectivity.

REFERENCES

Afreen, R. (2014). Bring your own device (BYOD) in higher education: Opportunities and challenges. *International Journal of Emerging Trends \& Technology in Computer Science*, *3*(1), 233–236.

Akande, A. O., & Tran, V. N. (2021). Predicting Security Program Effectiveness in Bring-Your-Own-Device Deployment in Organizations. *ICISSP*, 55–65. https://doi.org/https://dx.doi.org/10.5220/0010195800550065

Al-Harthy, I. M., Rahim, F. A., Ali, N., & Singun, A. P. (2019). Theoretical bases of identifying determinants of protection intentions towards bring-your-own-device (BYOD) protection behaviors. *2019 First International Conference of Intelligent Computing and Engineering (ICOICE)*, 1–9.

Alotaibi, B., & Almagwashi, H. (2018). A review of BYOD security challenges, solutions and policy best practices. *2018 1st International Conference on Computer Applications \& Information Security (ICCAIS)*, 1–6. https://doi.org/https://doi.org/10.1109/CAIS.2018.8441967

Amoud, M., & Roudies, O. (2017). Experiences in secure integration of Byod. *Proceedings of the 7th International Conference on Information Communication and Management*, 127–132.

Baillette, P., & Barlette, Y. (2018). BYOD-related innovations and organizational change for entrepreneurs and their employees in SMEs: The identification of a twofold security paradox. *Journal of Organizational Change Management*.

Bello, A., Armarego, J., & Murray, D. (2015). A policy-based framework for managing information security and privacy risks in BYOD environments. *International Journal of Emerging Trends \& Technology in Computer Science*, 189–198.

Disterer, G., & Kleiner, C. (2013). BYOD bring your own device. *Procedia Technology*, *9*, 43–53. https://doi.org/https://dx.doi.org/10.1016/j.protcy.2013.12.005

Gikas, J., & Grant, M. M. (2013). Mobile computing devices in higher education: Student perspectives on learning with cellphones, smartphones \& social media. *The Internet and Higher Education*, *19*, 18–26. https://doi.org/https://dx.doi.org/10.1016/j.iheduc.2013.06.002

Giwah, A. D. (2018). User information security behavior towards data breach in Bring Your Own Device (BYOD) enabled organizations-leveraging protection motivation theory.

SoutheastCon 2018, 1–5. https://doi.org/https://dx.doi.org/10.1109/SECON.2018.8479178

Gupta, R., Bhardwaj, G., & Singh, G. (2019). Employee Perception and Behavioral Intention to Adopt BYOD in the Organizations. *2019 International Conference on Automation, Computational and Technology Management (ICACTM)*, 73–78. https://doi.org/https://doi.org/10.1109/ICACTM.2019.8776815

Hakami, M. (2020). Using Nearpod as a Tool to Promote Active Learning in Higher Education in a BYOD Learning Environment. *Journal of Education and Learning*, *9*(1), 119–126. https://doi.org/https://dx.doi.org/10.5539/jel.v9n1p119

Harris, M. A., & Patten, K. P. (2014). Mobile device security considerations for small- and medium-sized enterprise business mobility. In *Information Management and Computer Security*. https://doi.org/10.1108/IMCS-03-2013-0019

Harris, M. A., Patten, K., & Regan, E. (2013). *The need for BYOD mobile device security awareness and training*.

Harris, M. A., Patten, K., Regan, E., & Fjermestad, J. (2012). *Mobile and connected device security considerations: A dilemma for small and medium enterprise business mobility?*

Kadimo, K., Kebaetse, M. B., Ketshogileng, D., Seru, L. E., Sebina, K. B., Kovarik, C., & Balotlegi, K. (2018). Bring-your-own-device in medical schools and healthcare facilities: a review of the literature. *International Journal of Medical Informatics*, *119*, 94–102. https://doi.org/https://dx.doi.org/10.1016/j.ijmedinf.2018.09.013

Kitchenham, B., Brereton, O. P., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering--a systematic literature review. *Information and Software Technology*, *51*(1), 7–15. https://doi.org/https://dx.doi.org/10.1016/j.infsof.2013.02.002

Madzima, K., Moyo, M., & Abdullah, H. (2014). Is bring your own device an institutional information security risk for small-scale business organisations? *2014 Information Security for South Africa*, 1–8.

Masilo, G. M., Simelane-Mnisi, S., Mji, A., & Mokgobu, I. (2021). Students' Behavioural

Intention and Challenges to Bring Your Own Device (BYOD) in Higher Education during COVID-19 and Beyond. *World Transaction on Engineering and Technology Education*, *19*(1), 10–15.

Miller, S., & Welsh, K. E. (2017). *Bring Your Own Device (BYOD) in higher education: Opportunities and challenges*.

Ontech. (2022). *15 BYOD Statistics that May Surprise You*. https://ontech.com/byod-statistics/

Palanisamy, R., Norman, A. A., & Mat Kiah, M. L. (2022). BYOD policy compliance: Risks and strategies in organizations. *Journal of Computer Information Systems*, *62*(1), 61–72. https://doi.org/https://dx.doi.org/10.1080/08874417.2019.1703225

Ratchford, M., El-Gayar, O., Noteboom, C., & Wang, Y. (2022). BYOD security issues: A systematic literature review. *Information Security Journal: A Global Perspective*, *31*(3), 253–273.

Ratchford, M. M., & Wang, Y. (2019). Byod-insure: A security assessment model for enterprise byod. *2019 Fifth Conference on Mobile and Secure Services (MobiSecServ)*, 1–10.

Scarfone, K., Mell, P., & others. (2007). Guide to intrusion detection and prevention systems (idps). *NIST Special Publication*, *800*(2007), 94.

Schlarman, S. (2001). The people, policy, technology (PPT) model: core elements of the security process. *Information Systems Security*, *10*(5), 1–6. https://doi.org/https://dx.doi.org/10.1201/1086/43315.10.5.20011101/31719.6

Shumate, T., & Ketel, M. (2014). Bring your own device: Benefits, risks and control techniques. *Ieee Southeastcon 2014*, 1–6.

Souppaya, M., Scarfone, K., & others. (2013). Guidelines for managing the security of mobile devices in the enterprise. *NIST Special Publication*, *800*, 124.

Souppaya, M., Scarfone, K., & others. (2016). User's Guide to Telework and Bring Your Own Device (BYOD) Security. *NIST Special Publication*, *800*, 114.

Sundgren, M. (2017). Blurring time and place in higher education with bring your own device applications: a literature review. *Education and Information Technologies*, *22*(6), 3081–3119. https://doi.org/https://dx.doi.org/10.1007/s10639-017-9576-3

Wani, T. A., Mendoza, A., & Gray, K. (2019). BYOD in hospitals-security issues and mitigation strategies. *Proceedings of the Australasian Computer Science Week Multiconference*, 1–10.

Zahadat, N., Blessner, P., Blackburn, T., & Olson, B. A. (2015). BYOD security engineering: A framework and its analysis. *Computers \& Security*, *55*, 81–99.

Ziemba, E. W., & Eisenbardt, M. (2021). The Effect of the Covid-19 Pandemic on ICT Usage by Academics. *Journal of Computer Information Systems*, 1–15. https://doi.org/https://dx.doi.org/10.1080/08874417.2021.1992806