International Journal of Science Academic Research
Vol. 03, Issue 10, pp.4554-4558, October, 2022
Available online at http://www.scienceijsar.com

ISSN: 2582-6425

Research Article

CYBER SECURITY RISKS OF BRING YOUR OWN DEVICE (BYOD) PRACTICE IN WORKPLACE AND STRATEGIES TO ADDRESS THE RISKS

***Bilquis Ferdousi**

Information Assurance and Cyber Defense, Information Technology, School of Information Security and Applied Computing
Eastern Michigan University, Ypsilanti, MI 48197, USA

Received 09th August 2022; **Accepted** 12th September 2022; **Published online** 31st October 2022

Abstract

This paper provides an overview of the threats to cyber security of Bring Your Own Device (BYOD) practice in the workplace and the strategies can be taken to mitigate those threats. Many organizations are adopting the BOYD practice where employees can use their personal devices such as laptops, smart phones, etc. for job-related work. While the BOYD has many benefits from both employer and employee perspective, the practice may cause many cyber security risks too. Many organizations and their employees overlook the potential challenge the practice may create to data security, privacy, and confidentiality. This review-based paper focuses on the BYOD practice related to cyber security threats in the workplace. This article also addresses the strategies organizations can implement to reduce the cyber security risks in BYOD practice. This study may help organizations to effectively manage their employees' BYOD practice by developing and implementing appropriate BYOD policies in their organization.

Keywords: Bring Your Own Device (BYOD), Cyber security risks, Security Policy, Compliance, Role-based access.

INTRODUCTION

As mobile technology has become a part of everyday life, in many organizations, employees use their own devices to access organizational data to do their job-related work. Employees are increasingly using their personal devices for work (Gökçe and Dogerlioglu, 2019). This practice is known as Bring-Your-Own-Device (BYOD), which allows employees using their personal mobile devices such as laptops, smart phones, etc. to access organizations' data resources such as emails, files, databases, etc. for work connecting through the corporate network (Petersen *et al.,* 2020,Gökçe and Dogerlioglu, 2019, Zhiling *et al.,* 2019). A survey shows that 72% corporate businesses allow their employees using personal devices to connect to the corporate networks and 87% allow employees using personal devices for organizational works (Zhiling *et al.,* 2019). Globally about 75% organizations adopt BOYD practice. In some sectors, about 85% employees use their personal devices to access work-related sensitive data (Downer and Bhattacharya, 2022). It has been predicted that in 2022 around ten billion employee-owned personal mobile devices will be used for work (Palanisamy *et al.,* 2022)and the BYOD practice will reach nearly $367 billion (Blair, 2018). Emergency situations, such as Covid pandemics promote the BYOD practice even more when the organizational devices are not remotely accessible to employees to continue communication for work because of social distancing (Barlette *et al.,* 2021). However, although BYOD practice seems beneficial, there are some serious cyber security issues faced by both employers and employees (Blair, 2018, Gökçe and Dogerlioglu, 2019) from different perspectives.

Corresponding Author:** ***Bilquis Ferdousi
Information Assurance and Cyber Defense, Information Technology, School of Information Security and Applied Computing Eastern Michigan University, Ypsilanti, MI 48197, USA

For the organizations, BYOD practice can cause many cyber security risks including unauthorized access, data leaks, malware attacks, data compromise, loss of control over organizational data leading to complete data loss and confidentiality (Mitrovic *et al.,* 2014). From employee perspective, they are worried about keeping their expected privacy regarding the personal information on their device (Olalere *et al.,* 2015). Hence, the BYOD cyber security issue has become a point of focus for many organizations as BYOD has become prevalent in workplaces (Musarurwa *et al.,* 2018). In this context, this paper assesses the cyber security risks in BYOD practice and the organizational strategies to address the cybersecurity threats. Analyzing the available literature on BYOD practice, this study identifies the cyber security risks, challenges, and mitigating strategies of the cyber security risks caused by practicing BYOD policy.

Cyber security risks of BYOD

Although BYOD practice is beneficial for both organizations and employees, it can cause security risks too. The practice comes with a cost because if employee-owned mobile devices are lost, stolen, or hacked; it may cause security breaches with potential disastrous consequences as the device has access to the critical and sensitive corporate data (Yang *et al.,* 2019). In addition to the possibility that employee-owned mobile devices can be easily lost or stolen, those devices may not be properly equipped with security protections such as anti-virus software, patches, updated firmware and configuration (Zhiling *et al.,* 2019). Consequently, BYOD practice can create serious security risks for organizations as well as employees (Gökçe and Dogerlioglu, 2019). The security concern for organizations includes mobile device loss, data contamination and data leakage that may cause financial and reputational cost for an organization (Palanisamy *et al.,* 2022). In BOYD practice, one of the most serious security challenges for an organization is that organizational data is being delivered to employee-owned

devices that are not managed by the organization's IT department. This has effects on security such as data leakage, data theft, and regulatory compliance (Olalere *et al.,* 2015). The lack of control over employees' personal mobile devices, which may have sensitive organizational data, make it one of the serious cyber security challenges for organizations. The cyber security threats may also include lack of security features in employee-owned mobile devices, data leakage in shared media, infected data, and new forms of malware targeting mobile devices (Wani *et al.,* 2020). Employee personal mobile devices are not designed for business purposes and may not have a sufficient level of security features that added more security risks of malware attack and data loss (Hovav and Putri, 2016). A study shows that in 2017 employee-owned mobile devices were responsible for 51% of corporate data breaches (Barlettea *et al.,* 2021). From employee perspective, the BYOD practice can be intrusive that may interfere with their privacy and personal data security (Annansingh, 2021). In addition, BYOD related cyber security issues increase the threats to organizational data because employee-owned mobile devices can be connected to different types of networks including cloud computing that often located in public cloud computing;hence, become more vulnerable to malware, viruses, unauthorized access and cyber-attacks. Especially, employees' Internet of Things (IoT) connected mobile devices used for work may worsen the cyber security situation. Furthermore, since employees own the mobile devices, it is more difficult for employers to monitor employees' usages of devices and their compliance with organizational policies and regulations. All this can cause security failure in data level, functional and system level, and eventually service level of the organization (Barlette, et al, 2021).

Strategies to mitigate BYOD-based

Cyber security risks

In the face of such serious cyber security threats, appropriate technical, behavioral, and organizational measures need to be taken against any deliberate or accidental corporate data loss or damage (Annansingh, 2021). The reviewed literature on BOYD practice suggests different strategies to ensure secure BYOD practice in the workplace. Those include: device and application security, employee awareness and training, BYOD related cyber security policies.

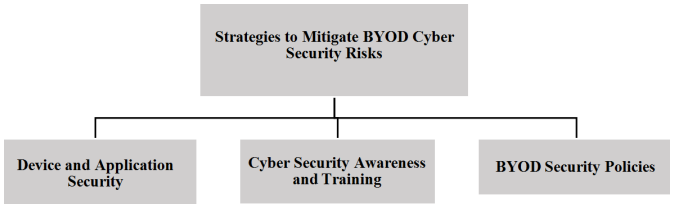

Figure 2. Strategies to Mitigate Cyber Security Risks in BOYD practice

Device and Application Security

Install and Update Security Tools: Despite the benefits, in BYOD practice, organizations have less control over employee-owned mobile devices that are used for accessing the corporate data and are more exposed to cyber-attacks. Consequently, employee-own devices that have access into the corporate network should be assessed for vulnerabilities (Annansingh, 2021). To ensure the mobile device and applications installed in it are secure, security tools such as antivirus, antimalware, antispyware, or anti-phishing tools needto be installed and regularly checked to protect organizational data (Wani *et al.,* 2020). Organizations must ensure that in BOYD practice, the device must meet the standard of authentication as well as protection against malware to prevent data leakage (Jamal *et al.,* 2020). A user's guide to BYOD security published in NIST reported that to secure employee-owned device used in BYOD practice, employees should use a combination of security software, such as antivirus software, personal firewalls, spam filtering, and popup blocking, to stop most attacks, especially malware. Employees must secure their personal devices based on the security recommendation from the device's manufacturer. The operating systems and important application software, such as web browsers, emails, instant messages, and security features in the device used in BOYD practice should be regularly updated on a weekly, if not daily basis (Souppaya and Scarfone, 2016).

Configurations: Configure primary applications can filter out the malicious content and activity; therefore,install configuration applications in the device used in BOYD practice to support security measures to block malicious attacks. Disable unnecessary network features and configure wireless networks securely on the device used in BOYD practice. Disable network connection when the mobile device used in BOYD practice is not in use. Configure remote access software following organizational requirements and recommendations stated in their policy. Also, to access the organizational data and resources, use an isolated, protected and encrypted network environment that is supported and managed by the organization (Souppaya and Scarfone, 2016).

Cyber Security Awareness and Training

People's knowledge, skills and understanding of cybersecurity, as well as their experiences, perceptions, attitudes and beliefs, are the main influencers of their behavior in this regard (Bada and Nurse, 2019). Developing awareness of cyber security threats and how to protect corporate data, is an essential component of organizational cybersecurity strategy. Organizations cannot assume employees will independently protect their mobile devices and the networks they connect to in BOYD practice, if there is an absence of training that specifies the basic security mechanisms and threats to be aware of (Downer and Bhattacharya, 2022). Literature shows that employee awareness of cyber security risks in BYOD practice has positive impacts**.** Therefore, it is important to develop training programs that raise employees' awareness of their rights, responsibilities, and procedures to follow in BOYD practice. The training program should also focus on the importance of cyber security and consequences of its threat (Hovav and Putri, 2016). But an organizational attempt to monitor employees' personal devices could be perceived by the employees as a threat to their privacy (Hovav and Putri, 2016). Therefore, in BYOD practice, organizations must involve their employees into their overall cyber security strategy as employees could be the weakest security link (Veljkovic and Budree, 2019). The employees should get regular training that includes the norm in social media usage, how to protect the personally identifiable information, creating strong password and privacy settings, etc. (Jonathan and Misra, 2016). The awareness training can be in-person, online, staff

meetings, newsletters, posters, team discussions, etc. (Wani *et al.,* 2020).

BYOD Security Policies

As with any cyber security policy, it is crucial in BYOD practice to have a cyber security framework that can reduce the risk of unauthorized access, intrusion and data leakage while limiting the impact on employee freedom, flexibility, convenience, and privacy. Developing a proactive and integrated security policy regarding BYOD practice helps organizations stay ahead of any risk of cyber-attacks (Annansingh, 2021). Therefore, as a strong measure to control security breach in BYOD practice, organizations should have appropriate policy regulating BYOD practice (Palanisamy *et al.,* 2022). Organizations adopting BOYD must have a clear security policy regarding BYOD practice based on their business requirements, productivity and the level of security required in the organization (Vorakulpipat *et al.,* 2017). The findings in current literature show that a practical approach to ensure cyber security is to develop a comprehensive BYOD related security policy that would balance between employees' convenience and their organizational data security (Kadimo *et al.,* 2018).Active and uniform enforcement of BYOD policy in the workplace is the best mechanism to mitigate legal or reputational risks of organization (Blair, 2018). However, there is a lack of effective cyber security policy regarding BYOD practice. A study shows that only 40% of employees were subject to regulations regarding personal devices used for work (Barlettea *et al.,* 2021). For that purpose, effective BYOD related cyber security strategy and policy are necessary in organizational, application, and device level for BYOD practice in the workplace (Zhiling *et al.,* 2019).

Effective BYOD practice is possible only with a comprehensive security policy that defines the devices and software to support, employee's role-based access to data resources, level of risk organization is willing to take, employee privacy, etc. (Jonathan and Misra, 2016). It may require organizations to review and change their existing IT policies (Musarurwa *et al.,* 2018). Organization should review whether its current cyber security policy addresses the BYOD practice. Otherwise, they must revise the policy to outline the rules, laws and practices that include the organizational right to check employee-owned devices, when necessary, in BOYD practice. As with any cyber security policy, it is crucial in BYOD practice to have a cyber security framework that can reduce the risk of unauthorized access, intrusion and data leakage while limiting the impact on employee freedom, flexibility, convenience, and privacy. Developing a proactive and integrated security policy regarding BYOD practice helps organizations stay ahead of any risk of cyber-attacks (Annansingh, 2021). Therefore, as a strong measure to control security breach in BYOD practice, organizations should have appropriate policy regulating BYOD practice (Palanisamy *et al.,* 2022). Organizations adopting BOYD must have a clear security policy regarding BYOD practice based on their business requirements, productivity and the level of security required in the organization (Vorakulpipat *et al.,* 2017).

The findings in current literature show that a practical approach to ensure cyber security is to develop a comprehensive BYOD related security policy that would balance between employees' convenience and their organizational data security (Kadimo *et al.,* 2018). Active and uniform enforcement of BYOD policy in the workplace is the best mechanism to mitigate legal or reputational risks of organization (Blair, 2018). However, there is a lack of effective cyber security policy regarding BYOD practice. A study shows that only 40% of employees were subject to regulations regarding personal devices used for work (Barlettea *et al.,* 2021). For that purpose, effective BYOD related cyber security strategy and policy are necessary in organizational, application, and device level for BYOD practice in the workplace (Zhiling *et al.,* 2019).

Effective BYOD practice is possible only with a comprehensive security policy that defines the devices and software to support, employee's role-based access to data resources, level of risk organization is willing to take, employee privacy, etc. (Jonathan and Misra, 2016). It may require organizations to review and change their existing IT policies (Musarurwa *et al.,* 2018). Organization should review whether its current cyber security policy addresses the BYOD practice. Otherwise, they must revise the policy to outline the rules, laws and practices that include the organizational right to check employee-owned devices, when necessary, in BOYD practice.

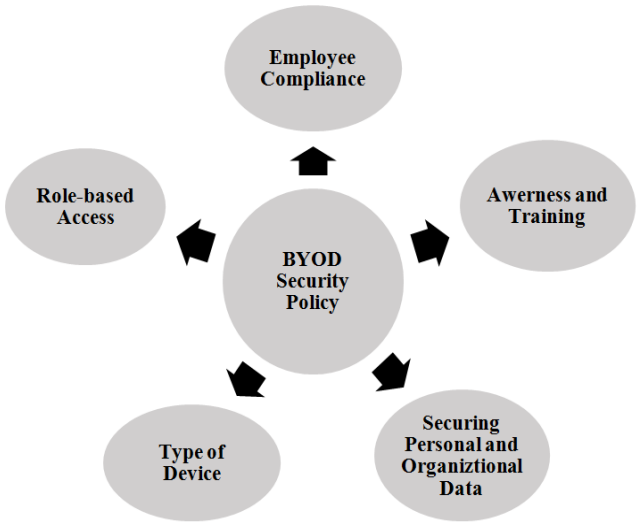

Figure 2. Comprehensive BYOD Security Policy

Employee Compliance: As cyber security concerns have become critical in BYOD practice, it is vital for employees to comply with the organization's cyber security policy (Tu *et al.,* 2019, Zhiling *et al.,* 2019). Prior studies highlight that compliance to BYOD policy can help ensure cyber security (Yang *et al.,* 2019). Therefore, employees must be familiar and comply with these policies (Mitrovic *et al.,* 2014). However, employees could be negligent toward adherence to the BYOD security policy (Palanisamy *et al.,* 2022). Hence, before BYOD practice, employees must sign a BYOD agreement that explains the responsibilities of employees as well as organization, defines consequences of noncompliance, etc. (Wani *et al.,* 2020). Also, in order to ensure fairness and employees willingly follow the security process, they should be consulted when deciding BYOD policy (Downer and Bhattacharya, 2022).

Role-based Access: The policy should include a detailed statement of authorized employers who can have access to the organizational resources. The degree of access by employees in organizational data and resources should be based on the responsibilities and roles they play in their organization (Jonathan and Misra, 2016). The policy must precisely specify the role-based access to the organizational data and resources from employee-owned devices. Ensure appropriate access to verified BYOD employees through strong authentication, authorization, and access control mechanisms (Wani *et al.,* 2020). To ensure restricted role-based access in BOYD practice, organizations should have a separate standard user account for each employee, assign a password to each user account, use the standard user accounts for daily use, and protect user sessions from unauthorized physical access. Safeguard restricted access to the mobile devices used in BOYD practice by setting a password or unique personal identification number (PIN), and device automatically locked after a certain idle period. Also, maintain the device security on an ongoing basis, such as changing passwords regularly and check the status of security software periodically (Souppaya and Scarfone, 2016).

Awareness and Training: The policy should include details for employee awareness and training with required guidelines on how to keep the sensitive data secured in BYOD practice for the best interest of both institution and employee. Policy needs to require training that should provide employees information regarding the appropriate and inappropriate use of their personal devices for job-related work (Jonathan and Misra, 2016). Policy of BOYD related cyber security awareness and training programs must be designed aligning with the organization's mission and supporting the business context and relevant to its culture of the organization (Bada and Nurse, 2019).

Type of Device: The policy should clearly describe the type of devices to be allowed in BYOD practice. A highly restricted devices policy specifies all the details of the devices to be used in organizational works. A flexible devices policy allows employees to bring any device of their choice provided it can serve for work (Jonathan and Misra, 2016). Device policy should allow employers to use security-compatible devices only to access the organizational resources for work (Zambrano and Rafael, 2018).

Securing Personal and Organizational Data: Detail guidelines separating organizational data and employee's personal data, enforcing employees to register their personal devices that will be used in workplace, enabling remote access using mobile devices through virtual private network (VPN), data encryption, etc. (Jonathan and Misra, 2016). Also, employees should not connect their mobile device used in BOYD practice in unknown unsecure public charging station (Souppaya and Scarfone, 2016).

Conclusion

BYOD practice allows employees using their personal devices to access organizational data and resources to perform their job-related work that enhance productivity, employee satisfaction, convenience, cut operational costs, and add value to the business of the organizations (Hovav and Putri, 2016). However, the literature on BOYD practice related to cyber security has highlighted that BYOD practice can increase the threat to cyber security at workplaces. The security risks can seriously hurt organizational reputation and business goal achievement. Therefore, it is very important for organizations to have standard policy regarding BOYD practice that their employees must comply with. The organizations need to ensure that employees are strictly compliant with the BOYD practice related security policies. This study will have significant implications on organizational management in designing and implementing BYOD practice related to cyber security awareness and training within their organizations following specific security policy.

REFERENCES

Annansingh, F. (2021). Bring your own device to work: how serious is the risk? *Journal of Business Strategy, 42*(6) 2021, pp. 392-398, © Emerald Publishing Limited, ISSN 0275-6668

Bada, M. and Nurse, J. R.C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information and Computer Security, 27*(3), pp. 393-410. DOI 10.1108/ICS-07-2018-0080.

Barlettea, Y., Jaouena, A., and Bailletteb, P. (2021). Bring Your Own Device (BYOD) as reversed IT adoption: Insights into managers' coping strategies. *International Journal of Information Management, 56*. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7484736/pdf/main.pdf

Blair, B. (2018). Contextualizing Bring Your Own Device policies. *The Journal of Corporation Law, 44*(1).

Downer, K. and Bhattacharya, M. (2022). BYOD security: A study of human dimensions. *Informatics, 9,* 16. https://doi.org/10.3390/informatics9010016

Gökçe, K. G., and Dogerlioglu, O. (2019). "Bring your own device" policies: Perspectives of both employees and organizations. *Knowledge Management and E-Learning, 11*(2), 233–246. https://doi.org/10.34105/j.kmel.2019.11.012

Hovav, A. and Putri, F. F. (2016). This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. *Pervasive and Mobile Computing, 32*, pp. 35-49.

Kadimo, K., Kebaetse, B. M., Ketshogileng, D., Seru, E. L., Sebina,B. K., Kovarik,C., and Balotlegi,K. (2018). Bring-your-own-device in medical schools and healthcare facilities: A review of the literature. *International journal of medical informatics,* 119, pp. 94-102.PMID: 30342692**.** DOI: 10.1016/j.ijmedinf.2018.09.013. Retrieved from: https://pubmed.ncbi.nlm.nih.gov/30342692/

Jamal, F., Taufik, M., Azizol A. A., and Hanapi, M. Z. (2020). A Systematic Review of Bring Your Own Device (BYOD). *Journal of Physics: Conference Series.* 1529 042071

Jonathan, O. and Misra, S. (2016). Policy framework for adoption of Bring Your Own Device (BYOD) by institutions of learning in Nigeria. https://www.researchgate.net/publication/312118956

Mitrovic, Z., Veljkovic, I., Whyte, G., and Thompson, K. Introducing BYOD in an organisation: the risk and customer services viewpoints. *The 1st Namibia Customer Service Awards and Conference,* 2014 - 3rd-5th November 2014, Windhoek, Namibia.

Musarurwa, A., Flowerday, S. and Cilliers, L. (2018). An information security behavioural model for the bring-your-own-device trend. *South African Journal of Information Management 20*(1), a980. https://doi. org/10.4102/sajim.v20i1.980

Souppaya, M. and Scarfone, K. (2016). User's guide to telework and Bring Your Own Device (BYOD) Security. *US National Institute of Standards and Technology (NIST).*http://dx.doi.org/10.6028/NIST.SP.800-114r1

Olalere, M., Abdullah, T. M., Mahmod, R., and Abdullah, A. (2015). A Review of Bring Your Own Device on Security Issues, *SAGE Open*, 1–11. DOI: 10.1177/21582440 15580372

Palanisamy, R., Norman, A. A., and Kiah, M. L. (2022). BYOD Policy Compliance: Risks and Strategies in Organizations. *Journal of Computer Information Systems*, *62*(1), 61–72. https://doi.org/10.1080/08874417.2019.1703225

Petersen, R., Santos, D., Smith, C. M., Wetzel, A. K., Witte, G. (2020). Workforce Framework for Cybersecurity (NICE Framework). NIST Special Publication 800-181 Revision 1. U.S. Department of Commerce. *National Institute of Standards and Technology.* https://doi.org/10.6028/NIST.SP.800-181r1. Retrieved from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

Tu, Z. C., Joni, A, and Zhao, Y. G. (2019). Complying with BYOD security policies: A moderation model based on protection motivation theory, *Journal of the Midwest Association for Information Systems (JMWAIS), 1*(2). DOI: 10.17705/3jmwa.000045 Available at: https://aisel.aisnet.org/jmwais/vol2019/iss1/2

Wani, A. T.,Mendoza, A., and Gray, K. (2020). Hospital Bring-Your-Own-Device security challenges and solutions: Systematic review of gray literature. *JMIR mHealth and uHealth 8*(6). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7333072/

Veljkovic, I., and Budree, A., 2019. Development of Bring-Your-Own-Device risk management model: Case study from a South African organisation. *The Electronic Journal Information Systems Evaluation, 22*(1), pp. 1-14.

Vorakulpipat, C. Sirapaisan, S., Rattanalerdnusorn, E., and Savangsuk, V. (2017). A policy-based framework for preserving confidentiality in BYOD environments: A review of information security perspectives. *Hindawi, Security and Communication Networks,* 2017, Article ID 2057260. https://doi.org/10.1155/2017/2057260

Yang, X., Wang, X., Yue, T. W., Sia, L. C. and Luo, X. (2019). Security Policy Opt-in Decisions in Bring-Your-Own-Device (BYOD) – A Persuasion and Cognitive Elaboration Perspective. *Journal of Organizational Computing and Electronic Commerce, 29*(4), 274-293, DOI: 10.1080/10919392.2019.1639913

Zambrano, R. R. F. and Rafael R. R. F. (2018). Bring Your Own Device (BYOD): a Survey of Threats and Security Management Models. *InternationalJournal of Electronic Business, 14*(2):146. DOI: 10.1504/IJEB.2018.094862

Zhiling, C, T., Adkins, Joni, A., and Yu, G., Z. (2019). Complying with BYOD security policies: A moderation model based on protection motivation theory. *Journal of the Midwest Association for Information Systems (JMWAIS), 1*(2). DOI: 10.17705/3jmwa.00004

****