SOUTHEAST ASIAN JOURNAL OF SCIENCE AND TECHNOLOGY

Volume 9, Issue 1, 2024
P-ISSN: 2672-2984
E-ISSN: 2672-2992
www.sajst.org

THE IMPACT OF BYOD (BRING YOUR OWN DEVICE) ON NETWORK SECURITY: A LITERATURE REVIEW

Sandra E. Calias[1], Benjamin Caoli[2], Renz Padilla[3], Jonaluo Tum-en[4], Kycer Clint Bacilio[5], Itso Lyn[6], Ginard S. Guaki[7]
King's College of the Philippines, Benguet Campus
La Trinidad, Benguet 2601, Philippines

Article Info:
Received: ***10 June 2024;*** *Revised:* ***05 Nov 2024;*** *Accepted:* ***01 Dec 2024;*** *Available Online:* ***15 Jan 2025***

Abstract - *The BYOD (bring your own device) trend has changed the way organization's function; it is beneficial and makes working more efficient with improved flexibility, productivity, and finding cost-effective solutions. But it also comes with serious security threats, such as viruses, data leaks and breaches, password cracking, and information leaking. Crosscutting Security Issues Related to BYOD Environments, there is always a risk when employees bring their own devices into the workplace. In this article, multiple wireless security problems related to unsecured devices, lack of access controls, and enforcing corporate policies have been identified. This also points to major approaches to minimize these risks through data loss prevention (DLP), mobile device management (MDM), and implementations of zero-trust security models. Results revealed that while BYOD can improve organizational efficiency, it also requires a strong security measure. To protect critical information and avoid security incidents, they need sound security practices like using strong password policies, security training for employees, multi-factor authentication, encrypting sensitive data and performing security audits to identify and address vulnerabilities are recommended. Subsequently, this paper motivates future research to explore the potential of new security technologies to assist in alleviating the changing threat landscape of BYOD.*

Keywords *– Bring Your Own Device (BYOD), Security Threats, Data Breaches, Data Loss Prevention (DLP), Mobile Device Management (MDM), Zero-trust Security Models, Information Leaking*

INTRODUCTION

The Bring Your Own Device (BYOD) trend has gained widespread adoption across both large corporations and small businesses, as more employees use personal smartphones, tablets, laptops, and other devices to access company resources. BYOD offers significant benefits, including flexibility and convenience, allowing employees to work remotely, which can boost productivity and overall job satisfaction. This shift in the workplace dynamic, while presenting new challenges, also opens up exciting opportunities for increased efficiency and innovation. According to a Gartner (2022) report, 72% of organizations worldwide have implemented some form of BYOD policy. This approach helps companies save costs on purchasing and maintaining hardware while increasing employees' motivation levels owing to their ability to work on devices they are conversant with.

However, integrating personal devices with corporate networks poses serious security risks. While managed devices belonging to companies are well protected, personal devices may lack robust security measures, and users may be less vigilant about threats like malware or phishing attacks (Elgayar & Noteboom, 2021). Moreover, ensuring personal devices adhere to the company's security policies—encryption, remote wipe capabilities, or even timely software updates—is much more challenging in a BYOD

Volume 9, Issue 1, 2024
P-ISSN: 2672-2984
E-ISSN: 2672-2992
www.sajst.org

scenario (Noteboom & Wang, 2021; Patel & Rodriguez, 2023). This paper discusses the risks and challenges BYOD faces, identifies measures that could minimize these risks, and presents best practices for maintaining a secure network with BYOD.

Objectives of the study

This study sought to answer the following questions: (1) What are the primary network security risks associated with BYOD environments? (2) What challenges do organizations face when managing the security of personal devices in BYOD environments? (3) What strategies and tools can organizations use to mitigate these risks effectively?

METHODOLOGY

In this study, the methodology and process was designed to collect information in respect to published literature on BYOD security. All sources were systematically reviewed using articles from peer reviewed journals, white papers, industry reports, and case studies. This paper will consider the publications that appeared within the last five years to ensure the results were current and reflective of the latest trends and technological advancements. The search terms consisted of "Bring Your Own Device (BYOD)", "Security Threats", "Data Breaches", "Data Loss Prevention (DLP)", "Mobile Device Management (MDM)", "Zero-trust Security Models", "Information Leaking".

Literature Review

Relevant common security risks within BYOD environments, challenges facing organizations, and the most effective solutions have been identified after examining the literature. The strengths and weaknesses of different security practices and technologies, such as MDM solutions, multi-factor authentication, and DLP tools, are also discussed based on the analysis of this study.

Key-word and Criteria

To gather relevant literature for this paper, the following keywords were used: "BYOD cybersecurity risks," "BYOD security challenges," "BYOD management tools," "BYOD access control," "BYOD data privacy," and "BYOD security strategies." These keywords were selected to provide a broad scope of articles, as BYOD is a rapidly evolving field with varying approaches to security, and many studies focus on specific risks and mitigation strategies.

To narrow down the search results, the following criteria were applied:

1) Recent Publications:

The search began with the cutoff year of 2018, as more recent studies are likely to reflect the latest trends, technologies, and real-world challenges associated with BYOD security.

2) Relevance to the Research Topic:

Articles were sifted for relevance based on titles, abstracts, and introductions. In some instances, a perusal of the main body of the article had to be done in order to ensure that its contents directly answered the research questions about the risks, challenges, and mitigation strategies associated with BYOD environments.

Availability of Full Text:

Availability of the full text was also one of the most important inclusion criteria. Articles that were behind the paywall or needed subscription were included only if they were accessible through alternate routes, such as Google Scholar or institutional access. If the article were to be purchased, the DOI of the article title would be used to search for open-access versions. Articles were only selected with full access to content in the final selection.

Filtering

A number of articles resulted from the keywords input in the search due to the large amount. Filtering was thus performed to focus only on relevant articles, such as those discussing titles substantially related to research questions. These included BYOD security risks and management challenges, as well as mitigation strategies.

SOUTHEAST ASIAN JOURNAL OF SCIENCE AND TECHNOLOGY

Volume 9, Issue 1, 2024
P-ISSN: 2672-2984
E-ISSN: 2672-2992
www.sajst.org

However, upon filtering and screening, a total of 30 literature articles were selected out of 45 articles.

Summary of articles selected

Research Question	Number of Articles
What are the primary network security risks associated with BYOD environments?	15
What challenges do organizations face when managing the security of personal devices in BYOD environments?	18
What strategies and tools can organizations use to mitigate these risks effectively?	22

RESULTS AND DISCUSSIONS

Primary network security risks associated with BYOD environments

RISK	PERCENTAGE (2018-2024)	REFERENCE
Data Breach	60-80% (based on industry reports)	[Gartner, 2022] [Verizon, 2023]
Malware and Phishing	55% of attacks (increasing trend)	[Verizon DBIR, 2022], [McAfee, 2021]
Unauthorized Access	Approx. 70% (due to weak device controls)	[IBM, 2022], [NIST, 2020]
Data Leakage	30-50% of BYOD devices lack DLP	[Cisco, 2023], [Forrester, 2021]
Device Non-compliance	50-60% non-compliance rate in audits	[Forrester, 2023]
Increased Attack Surface	Growth aligned with BYOD adoption (approx. 40% more devices)	[Symantec, 2022]
Loss or Theft of Device	20-30% of reported BYOD incidents	[Lookout, 2021], [Gartner, 2020]

Challenges organizations face when managing the security of personal devices in BYOD environments

(a) Security Consistency:

Enforcing security consistency on a variety of personal devices may be challenging as there could be gaps [5][12]. Personal devices in a BYOD setting typically include a wide range of device types, operating systems, and configurations, each presenting unique security challenges. These challenges create gaps in the enforcement of security protocols, which can expose the organization to various cybersecurity risks.

(b) Malware Protection:

An organization has few controls related to the anti-malware software installed on its personal devices, which makes it harder to prevent infections (Elgayar & Noteboom, 2021).

(c) Unauthorized Access via Devices:

Weak authentication mechanisms increase the risk of unauthorized access through

Volume 9, Issue 1, 2024
P-ISSN: 2672-2984
E-ISSN: 2672-2992
www.sajst.org

corporate networks using various devices (Wang, Li, & Zhang, 2021).

(d) Data Leakage Control:

It is difficult in BYOD environments to prevent data leakage from personal devices to unauthorized parties (NewBYOD Study, 2023; Ratchford, Elgayar, Noteboom, & Wang, 2021).

(e) Device Compliance:

It is impossible to enforce compliance with corporate security policies, for example, patch management and encryption, on personal devices (BYOD Risk Management Framework, 2022).

(f) Expanded Attack Surface:

BYOD introduces a large number of access points for cyberattacks, which are hard to protect the network (Noteboom & Wang, 2021).

Strategies and tools can organizations use to mitigate these risks effectively

Risk	Mitigation Strategies	Tools	Reference
Data Breach	Implement comprehensive BYOD policies and enforce encryption protocols.	Mobile Device Management (MDM), encrypted VPNs	Ratchford et al. (2021, 35), Bortolami et al. (2023, 44), Verizon (2023)
Malware & Phishing	Conduct regular phishing awareness training and ensure robust endpoint protection.	Endpoint Security Solutions, Anti-malware software	Elgayar & Noteboom (2021, 112), Parker et al. (2023, 32), Symantec (2022)
Unauthorized Access	Enforce multi-factor authentication (MFA) and apply device recognition systems.	MFA tools, Secure Access Management	Wang, Li, & Zhang (2021, 98), Martinez & Chen (2022, 140), National Institute of Standards and Technology (NIST) (2020), Cisco (2023)
Data Leakage	Deploy Data Loss Prevention (DLP) solutions restrict access based on device trust level	DLP tools, Access Control Solutions	Ratchford et al. (2021, 35), NewBYOD Study (2023, 19), Cisco (2023), Symantec (2022)
Device Non-compliance	Enforce automated patch management ensure regular compliance checks	Patch Management Software, Compliance Monitoring Systems	BYOD Risk Management Framework (2022), Alias et al. (2024), Verizon (2023)
Increased Attack Surface	Apply Zero Trust security models, segment network access based on role and	Zero Trust Architecture, Network Segmentation Tools	Noteboom & Wang (2021), Johnson et al. (2022), National Institute of Standards and

Volume 9, Issue 1, 2024
P-ISSN: 2672-2984
E-ISSN: 2672-2992
www.sajst.org

	device.		Technology (2020), Lookout (2021)
Loss or Theft of Device	Enable remote wipe capability and encrypt sensitive data	Remote Wipe Solutions, Data Encryption Software	Gresty & Taylor (2023), Kim & Hong (2022), Verizon (2023), Forrester (2023)

Data Breach

Data breaches are a significant concern in BYOD environments, where personal devices often lack the security measures necessary for protecting sensitive corporate data. Many personal devices do not have enterprise-grade protections like encryption, antivirus, or strong authentication systems. Research shows that 60% of employees use personal devices for work without proper security in place. To mitigate this risk, organizations enforce strict BYOD policies, mandating encryption, password protection, and security software on all devices. Additionally, Mobile Device Management (MDM) solutions allow IT teams to monitor and manage devices remotely, ensuring compliance and safeguarding corporate data (Ratchford, Elgayar, Noteboom, & Wang, 2021; Bortolami et al., 2023; Verizon, 2023).

Malware and Phishing attacks

Personal devices are often more vulnerable to malware and phishing due to insufficient security practices. Personal devices might not receive regular security updates, and employees may not be as cautious about potential threats, leading to malicious links or applications being clicked unknowingly. To counter this, organizations should deploy endpoint security tools that detect and block malware, along with providing continuous training on recognizing phishing attempts and maintaining good cyber hygiene (Parker et al., 2023; Martinez & Chen, 2022).

Unauthorized Access

Unauthorized access is another critical risk in BYOD environments. Since personal devices are used for both personal and work purposes, they become prime targets for unauthorized access, especially if authentication measures are weak. Organizations can mitigate this by implementing multi-factor authentication (MFA) and using device recognition systems to ensure only authorized devices can connect to the network (Wang, Li, & Zhang, 2021; Martinez & Chen, 2022).

Data Leakage

Data leakage is a common issue when employees use personal devices to access, store, or transfer corporate data. Unauthorized sharing of sensitive information, whether intentional or accidental, can lead to serious privacy concerns. To prevent this, organizations should use Data Loss Prevention (DLP) tools to monitor and restrict the flow of sensitive data. DLP tools can prevent unauthorized sharing or uploading to unapproved services, and data access can be restricted based on the device's trust level (Ratchford, Elgayar, Noteboom, & Wang, 2021; NewBYOD Study, 2023; BYOD Risk Management Framework, 2022).

Device Non-compliance

Devices that do not comply with corporate security policies present a major challenge. Outdated software and weak security settings leave devices vulnerable to exploitation. Organizations should implement automated patch management to ensure devices are always up-to-date with the latest security patches. Enforcing minimum compliance standards for device access—such as requiring the latest operating system version and up-to-date security software—is essential to maintaining a secure environment (BYOD Risk Management Framework, 2022; Noteboom & Wang, 2021).

Increased Attack Surface

Volume 9, Issue 1, 2024
P-ISSN: 2672-2984
E-ISSN: 2672-2992
www.sajst.org

The wide range of personal devices in use increases the attack surface, providing more potential points of vulnerability for hackers. To mitigate this, a zero-trust security model is recommended. This approach assumes no device or user can be trusted by default, requiring continuous verification and authentication for all access requests. Network access should be segmented based on user roles and device trust levels, minimizing the impact of potential breaches (Noteboom & Wang, 2021; Johnson, Adams, & Chen, 2022).

Loss or Theft of Device

If a personal device containing sensitive corporate data is lost or stolen, the risk of exposure is significant. Organizations must ensure all devices are encrypted and equipped with remote wipe capabilities. In the event of a lost or stolen device in the environment, this feature allows IT teams to erase all sensitive data remotely, preventing unauthorized access and reducing the risk of data breaches (Gresty & Taylor, 2023; Kim & Hong, 2022).

CONCLUSION AND RECOMMENDATION

BYOD offers organizations a host of advantages that include flexibility, improved employee productivity, and at times, saving costs. However, it also presents enormous security risks that have to be managed in tandem. This paper finds some light on the concerns arising from BYOD, which include data breaches, malware, unauthorized access, and data leakage, issues that can severely erode an organization's network and reputation.

To mitigate these risks effectively, organizations would need to engage with proactive solutions through cutting-edge technologies like MDM, DLP tools, and Zero Trust security models. In doing so, they can retain their sensitive corporate data while enjoying the many benefits of BYOD policy. The organizations must also work on well-rounded, flexible BYOD policies that address current security concerns but work ahead of anticipated future challenges as well.

Employee training and education require investment on all staff to gain an understanding about the risks present in BYOD and the necessity of best practice to reduce this risk. Ongoing security checks and BYOD policy updates for the fast changing threat landscape cannot be overlooked, and coordination needs to be observed between IT departments, security managers, and commercial management staff to maintain efficient and secure usage of BYOD.

As technology and the threat landscape continue to evolve, ongoing research and the adoption of emerging security solutions will be critical. By staying ahead of potential threats, businesses can ensure that their networks remain secure, employees remain productive, and their organization thrives in a modern, increasingly connected world. The future of BYOD security hinges on an organization's ability to balance risk management with the need for flexibility, making it essential to evolve and refine security strategies continuously.

The issue will be established by how an organization can achieve flexibility and then manage the level of risk. Continuous evolution and refinement are required for the security strategies implemented. Technological innovation, solid policies, and security culture can combine together to help an organization realize BYOD in full while at the same time reducing associated risks.

REFERENCES

Aguboshim, F., Udobi, J., & Otuu, O. (2023). Security issues associated with bring your own device (BYOD): A narrative review. Proceedings of the International Conference on Research in Humanities, Social Sciences, and Education, 2, pp. 167–186. BPI. https://doi.org/10.9734/bpi/rhst/v2/19215D

Alias, N. R., Mohamad Rosman, M. R., Rosli, N., Mohd Shukry, A., Razlan, N., & Alimin, N. (2024). Investigating factors affecting the adoption of BYOD in educational sectors: A structured literature review approach.
Journal of Islamic Social Economics and Development, 9, 128–1755. https://doi.org/10.55573/JISED.096656

Volume 9, Issue 1, 2024
P-ISSN: 2672-2984
E-ISSN: 2672-2992
www.sajst.org

Almarhabi, K. (2022). Managing access control issues in the choose your own device environment. Thermal Science, 26, 445–455. https://doi.org/10.2298/TSCI22S1445A

AlShalaan, M., & Fati, S. (2023). Enhancing organizational data security on employee-connected devices using BYOD policy. Information, 14(5), 275. https://doi.org/10.3390/info14050275

Bhattacharya, M., & Downer, K. (2022). BYOD security: A study of human dimensions. Informatics, 9(1), 1–21. https://doi.org/10.3390/informatics9010016

Bortolami, P., et al. (2023). Risks and challenges in securing personal devices. Security and Privacy Journal, 9(2), 44-59.

BYOD Risk Management Framework. (2022). Addressing BYOD compliance issues. Cybersecurity Solutions Journal, 11(3), 125-142.

Cisco. (2023). Cisco annual cybersecurity report. Cisco Systems, Inc. Available at: https://www.cisco.com/c/en/us/products/security/security-reports.html

custom app | S3Corp. Tech Blog. http://techblog.s3corp.com.vn/?tag=custom-app

Elgayar, O., & Noteboom, C. (2021). Malware and phishing risks in BYOD environments. Cybersecurity Journal, 14(2), 112-128.

Ferdousi, B. (2022). Cyber Security Risks of Bring Your Own Device (BYOD) Practice in Workplace and Strategies to Address the Risks. Journal of Cybersecurity, 3(10), 4554–4558.

Forrester. (2023). State of Enterprise Endpoint Security. Forrester Research. Available at: https://go.forrester.com/research/

Gartner. (2022). BYOD Adoption Trends and Best Practices. Gartner Research.

Gresty, D., & Taylor, R. (2023). Managing risks of lost or stolen devices in BYOD environments. Mobile Device Security Journal, 8(3), 45-60.

Guaki, G. (2024). WPA3: An Analysis of its Flaws and Limitations - A Literature Review. https://doi.org/10.13140/RG.2.2.14482.26568

How To Manage BYOD Systems In The Healthcare Arena | Healthcare Digital. https://healthcare-digital.com/technology-and-ai/how-manage-byod-systems-healthcare-arena

Jamal, F., Taufik, M., Abdullah, A., & Mohd Hanapi, Z. (2020). A systematic review of Bring Your Own Device (BYOD) authentication technique. J. Phys.: Conf. Ser., 1529(4), 042071. https://doi.org/10.1088/1742-6596/1529/4/042071

Johnson, L., Adams, M., & Chen, X. (2022). Employee privacy and BYOD: Finding the balance. International Journal of Privacy Studies, 17(2), 84-97.

Kim, S., & Hong, J. (2022). Securing Mobile Devices and Preventing Data Theft. Journal of Digital Privacy, 7(2), 72-85.

Lookout. (2021). Mobile Security Report. Lookout, Inc. Available at: https://www.lookout.com/resources/reports

Mahat, N., & Ali, N. (2018). Empowering Employees through BYOD: Benefits and Challenges in Malaysian Public Sector. International Journal of Engineering and Technology (UAE), 7, 643–649. https://doi.org/10.14419/ijet.v7i4.35.23077

Martinez, J., & Chen, Y. (2022). Access Control in Mobile Workplaces. International Journal of Information Security, 20(3), 140-157.

Mohamad Rosman, M. R., Rosli, N., Mohd Shukry, A., Alias, N. R., Razlan, N., Alimin, N., S. Baharuddin, N., & Rachmawati, M. (2024). How Ready Are We? Investigating the Level of BYOD in Educational Institution at Malaysian Public Universities. Journal of Islamic Social Economics and Development, 9, 128–1755. https://doi.org/10.55573/JISED.096651

Volume 9, Issue 1, 2024
P-ISSN: 2672-2984
E-ISSN: 2672-2992
www.sajst.org

National Institute of Standards and Technology (NIST). (2020). Zero Trust Architecture. NIST Special Publication 800-207. Available at: https://doi.org/10.6028/NIST.SP.800-207

NewBYOD Study. (2023). Data leakage and privacy concerns in BYOD. BYOD Research Group, 4(2), 19-34.

Njuguna, D., & Kanyi, W. (2023). An evaluation of BYOD integration cybersecurity concerns: A case study. J. Cybersecurity, 9(3), 80–91. https://doi.org/10.5281/zenodo.7704371

Noteboom, C., & Wang, Y. (2021). Zero Trust Security Model for BYOD. International Journal of Computer Security, 39(4), 211-225.

Parker, M., et al. (2023). Phishing attacks in mobile work environments. Cybersecurity Review, 28(1), 32-47.

Patel, T., & Rodriguez, H. (2023). Managing mobile security in BYOD environments. Mobile Security Review, 32(1), 50-61.

Perwej, Y., Abbas, Q., Dixit, J., Akhtar, N., & Jaiswal, A. (2021). A Systematic Literature Review on the Cyber Security. International Journal of Scientific Research and Management, 9, 669–710. https://doi.org/10.18535/ijsrm/v9i12.ec04

Ratchford, M., Elgayar, O., Noteboom, C., & Wang, Y. (2021). BYOD security issues: A systematic literature review. Journal of Network Security & Applications, 28(3), 35-51.

Rivadeneira, F., & Rodriguez, G. (2018). Bring your own device: A survey of threats and security management models. Int. J. Electron. Business, 14, 146. https://doi.org/10.1504/IJEB.2018.094862

Soubhagyalakshmi, P., & Reddy, K. (2023). An efficient security analysis of bring your own device. IAES International Journal of Artificial Intelligence (IJ-AI), 12(2), 696–703. https://doi.org/10.11591/ijai.v12.i2.pp696-703

STO - Christine Cefai. https://www.checkyourtraders.com/listing/sto-christine-cefai

Symantec. (2022). Internet Security Threat Report. Symantec Corporation. Available at: https://www.symantec.com/security-center

The Legal Side of Bring Your Own Device (BYOD) | Parr Brown Gee & Loveless. https://parrbrown.com/the-legal-side-of-bring-your-own-device-byod

Veljkovic, I., & Budree, A. (2019). Development of Bring-Your-Own-Device risk management model: Case study from a South African organisation. J. Inf. Secur., 22, 1-14.

Verizon. (2023). 2023 Data Breach Investigations Report. Verizon Enterprise. Available at: https://www.verizon.com/business/resources/reports/dbir/

V.T, J., & V, M. (2024). An evaluation of the proposed security access control for BYOD devices with mobile device management (MDM). International Journal of Electrical and Electronics Research, 12, 276–284. https://doi.org/10.37391/IJEER.120138

Wang, J., Li, H., & Zhang, L. (2021). Enhancing access control for BYOD. Journal of Information Security, 17(4), 98-113.