World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:17, No:6, 2023

Organizational Data Security in Perspective of Ownership of Mobile Devices Used by Employees for Works

B. Ferdousi, J. Bari

Abstract**—**With advancement of mobile computing, employees are increasingly doing their job-related works using personally owned mobile devices or organization owned devices. The Bring Your Own Device (BYOD) model allows employees to use their own mobile devices for job-related works, while Corporate Owned, Personally Enabled (COPE) model allows both organizations and employees to install applications onto organization-owned mobile devices used for job-related works. While there are many benefits of using mobile computing for job-related works, there are also serious concerns of different levels of threats to the organizational data security. Consequently, it is crucial to know the level of threat to the organizational data security in the BOYD and COPE models. It is also important to ensure that employees comply with the organizational data security policy. This paper discusses the organizational data security issues in perspective of ownership of mobile devices used by employees, especially in BYOD and COPE models. It appears that while the BYOD model has many benefits, there are relatively more data security risks in this model than in the COPE model. The findings also showed that in both BYOD and COPE environments, a more practical approach towards achieving secure mobile computing in organizational setting is through the development of comprehensive cybersecurity policies balancing employees' need for convenience with organizational data security. The study helps to figure out the compliance and the risks of security breach in BYOD and COPE models.

Keywords**—**Data security, mobile computing, BYOD, COPE, cybersecurity policy, cybersecurity compliance.

I. Introduction

WITH rapid advancement of mobile computing and computer network technology, 85% of Americans now own a smartphone and 15% of American adults are "smartphone-only" internet users, who do not have home broadband service but own a smartphone [1]. Mobile computing provides employees access to the vital data resources in the workplace with flexibility to perform their job-related works from anywhere. There are significant increases in the remote and hybrid approach to conduct job-related work. The COVID-19 pandemic has transformed employees' in-person works to remote or hybrid works with the challenge of meeting cyber-security requirements in those environments [2]. Mobile computing can increase efficiency and productivity in the works, but can also leave sensitive data vulnerable. Therefore, securing the mobile devices, used for job-related work, is essential for ensuring data security [3].

The essential mobile devices include: smartphones (Android, iPhone, Windows Phone, Blackberry, etc.), laptops, tablets (Galaxy, iPad); PDA (Portable Digital Assistants); phablets (a combination of smartphone and tablets), etc. Mobile devices have become an integral component in people's daily lives. As a result, employees find it convenient to use their own mobile devices to connect to their corporate network, often for critical tasks for an extended time [4]

Mobile devices are an essential part in modern workplaces as an increasing number of employees are using these devices to perform job-related work. Consequently, organizations are increasingly challenged with ensuring that mobile devices process and store sensitive data securely since using those devices bring unique threats to the organizational data security that needs to be managed differently from desktop platforms [5].

The debate on whether employees should be allowed: 1) to use their own devices connecting to organizations' network and other vital resources for job-related works, or 2) to use corporate-owned devices for personal as well as job-related purposes, has made mobile device ownership a sensitive issue. The data security, privacy, cost, and supportability issues play an important role in this mobile computing ownership argument. Based on the ownership of the mobile computing, there are mainly two different models that leverage the employees to do their job-related work accessing the organizational data and network resources using mobile devices. Those models are: 1) COPE Model, and 2) BYOD Model.

Corporate Owned, Personally Enabled (COPE): The COPE model allows organizations as well as employees to install applications onto organization-owned mobile devices that are used for job-related works [3]. Instead of allowing employees to use their own personal mobile devices for job-related work, COPE model allows personal uses of organization's mobile devices. The organizations select mobile devices and own them, but the employees are reasonably allowed to install the applications they want on those devices. The organization also establishes usage and cost limits for employees.

Bring Your Own Device (BYOD): The BYOD model is defined as the adoption of employee's personally owned mobile

B. Ferdousi, Professor, School of Information Security and Applied Computing, Eastern Michigan University, United States (e-mail: bferdous@emich.edu).

J. Bari, Professor, School of Engineering, Eastern Michigan University, United States (e-mail: mbari@emich.edu).

devices to fulfill work-related activities. The low cost and ubiquitous nature of mobile devices and computer networks has led to the increasing popularity of BYOD [6]. The BYOD model is an environment in which employees use their personal mobile computing devices such as smartphones, laptops, tablets, etc. for job-related works [5], [7]. With advanced computer networking and mobile devices with applications, BYOD model emerged as a widespread practice since the 2010s [8], [9]. BYOD model allows employees to use their own personal mobile devices to access organizational data resources for job-related works [9]. Employees can work on any personal mobile device that they prefer to select, have access to organizations' network resources, download and view email, documents, etc. BYOD has significant implications for computer network security and IT support, as well as employee satisfaction and productivity [8]. However, the proliferation of mobile devices has brought the trend of BYOD practice in organizations along with serious challenges to data security, especially when employees fail to comply with the cybersecurity policies [8]. In this context, it is important to understand what level of threat to the organizational data security the mobile computing causes in BOYD or COPE models. It is also important to know how the employees' compliance with organization's data security policy can mitigate the threats. As more and more employees are using mobile devices for job-related work, especially after COVID pandemic, systematic literature analysis in this regard is significantly very important.

This paper focuses on: 1) the risks to data security in perspective of ownership of mobile devices used in the work remotely or onsite, especially in the BYOD and COPE models, 2) the compliance and legal issues arise as a result of allowing employees using mobile devices in BYOD and COPE models.

II. Related Works

A. Benefits of BYOD Practice

The benefits of BYOD practice include increase in productivity of employees, increased revenue, reduction organizational cost on mobile devices, data services, etc. [10]. BYOD practice allows employees to have access to organizational data, applications, records, networks, and other resources using their personal devices. This practice provides employees empowerment and privilege to decide the technology they will be using to fulfill their job responsibility. Many organizations are adopting BYOD practice as this practice has many positive effects such as increased job satisfaction, self-confidence, mobility, and flexibility for employees. The practice can also ensure better productivity, consumer services, and cost-cutting for organizations [8], [9]. According to a survey, 61% of employees prefer BYOD practice because they can perform their job-related tasks from anywhere and at any time using their own mobile devices [11]. In the BYOD model, the advantages are the lower hardware and service costs for organizations, enhancement of productivity and enablement, higher employee engagement and convenience, fast deployment time, etc. [8]. BYOD practice influences employees' job satisfaction, job performance, self-assessment, and commitment to their organizations [6].

Increased Productivity: BYOD practice can increase productivity gains, cost savings, innovation, business process improvement, and performance expectancy for organization. BYOD can increase productivity by 34%, management flexibility, and maximized employee contentment [12]-[14]. From employees' perspective, this practice can improve their productivity, efficiency, and workflow [15]. Employees prefer to use their own devices at work as they feel more comfortable while organizations want to improve the efficiency and productivity [16].

Reduced Costs: BYOD practice helps organizations to cut costs because they can purchase and maintain fewer mobile devices as employees use their own mobile devices for work [12], [14]. Many organizations adopt BYOD practice to increase their computer resources, especially the hardware devices [17]. Some organizations view this practice as an opportunity to increase productivity using their employees' software and hardware without investing their own resources on devices [18]. In BYOD practice, the employees can have access to the work from anywhere at any time using their own preferred devices rather than the organization provided devices out of its budget [19]. Consequently, the BYOD model increases organizational revenue by reducing the expenses for corporate-liable mobile device and data services [10].

Employee Satisfaction: Employees' freedom to use their own mobile devices for work, gives them more satisfaction as they can constantly improves their applications for convenience, comfortability, easy communication, and better functionality. Thus, BYOD practice increases employees' autonomy, motivation, satisfaction, innovation, and job performance. BYOD practice can help employees to easier assimilation, creativity, and more efficient use of their own devices for workplace tasks. In addition, BYOD allows employees to use their familiar and convenient applications on their own devices that increase their satisfaction [14].

Flexibility: BYOD practice is convenient for employees as it allows them to conduct their work from anywhere, and even any time in some cases [20]. The practice allows employees to work effectively from anywhere as they can install necessary apps in their mobile devices and take the advantage of increased functionality of the apps installed, which prompts flexibility. The flexibility to choose the device for their job-related work makes employees more mobile and productive [19].

Convenience: Along with the benefits of productivity, cost saving, employee satisfaction and flexibility, BYOD practice also provides a high level of convenience to the employees to perform their job-related works [19]. They can perform their organizational works from anywhere and/or anytime at their convenience.

B. Cost in BYOD and COPE Models

In the BYOD model, employees as owners are responsible for purchase, service, and maintenance costs of the mobile devices they use for their job-related work. With the fast pace of technology advancement, BYOD model may require employees to buy a growing number of sophisticated innovative applications. Thus, there are significant cost risks for employees in the BYOD model, especially if employees reach maximum data usage because of using personal applications, organizational applications, or a combination of both in their personal mobile devices. In the COPE model, mobile devices are owned by organizations and issued to employees, and both can install applications onto those devices; hence employees are not responsible for the mobile devices used for job-related works [5].

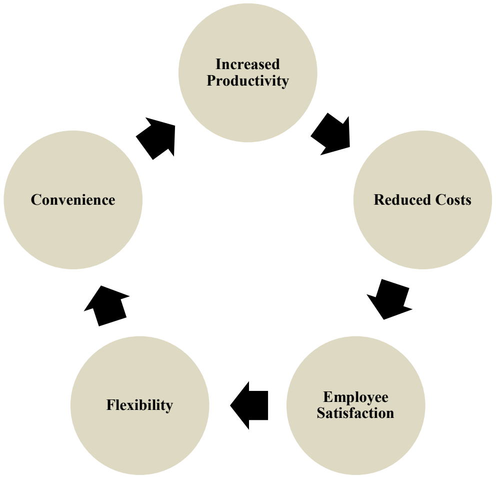

Fig. 1 BOYD benefits from employee and organizational perspective

From cost savings perspective, BYOD model may save on organizations' capital costs such as mobile device purchasing cost, but COPE model saves far more in operational costs (i.e., training, support, etc.) and other administrative costs to ensure less threat to data security. In addition to lowering mobile device acquisition cost, organizations may get better deals on application fees and data plans for more cost-effective usage. Compared to COPE, in BYOD model the configuration costs could be higher, legal implications and risks could be enhanced, enforcement of policy requirements could be more difficult, and support service for the mobile devices are more complex because those are personally owned by the employees, not by the organizations. Consequently, the security is much more difficult to enforce as it is much less centralized, replacement could be more problematic when an employee's personal device breaks or is lost, and there is no control without Mobile Device Management [8].

III. Methodology

The research in this study was conducted based on reviewing current literature on cyber security threats in practicing BOYD, COPE, and employees' compliance with data security policies in the work environment. An analysis of literature research was conducted that identifies the current consensus of BOYD and COPE. For that purpose, research articles, especially recently published in peer-reviewed journals and conference proceedings, have been collected from online libraries and Google Scholar. Articles were searched in online libraries using key terms *BOYD, COPE, data security, policy compliance*, etc., that are related to this research topic. Source literature utilized a wide array of methodologies, including survey analysis, field experiments, case studies, theoretical analysis, statistical analysis, literature analysis, and confirmatory factor analysis.

Collect Research Data: A collection of 50 articles with relevant topics was gathered and reviewed. Those articles were down selected to 39 based on a sampling of relevance to the research. Finally, 38 articles, published from 2015 to 2022, were systematically reviewed to fulfill the research purpose. This approach selected the studies that focus on the *BOYD, COPE, data security, policy compliance*. Target analysis data from the selected literature were compiled in tabular format for collective analysis. Tracked categories included study title, authors and date of publication, sample method, instrumentation of the research, and subsequent research findings or contributions to the body of knowledge. This paper analyzed the combination of research findings and contributions, identifying commonalities that indicate emergent best practices.

IV. Results and Discussion

A. Data Security Risks in BYOD and COPE

While the BYOD model increases convenience, efficiency, productivity, and flexibility; it also causes a number of cybersecurity risks such as ease of mobile device loss, data corruption, loss of control to organizational networks, etc. The BYOD model also makes it a challenge to ensure adherence to cybersecurity policy [9]. The cybersecurity risk in BYOD model cannot be solved applying regular policies designed to secure organizational devices. Finding an effective solution can be challenging due to the unique risks in practicing BYOD model. On the other hand, the practice in BYOD model can create risks for employees' privacy also. In the BYOD practice, employees may have to let their employers access private mobile devices used for organizational works. This access will allow employers to observe and even may control employee's private data [21]. In regular practices, employees do not have access to the employees' personal mobile devices. Therefore, there is no possibility for employers to observe employees' personal data or have control on those data that could be harmful for the employees. When employers get access to employees' personal data in their mobile devices, that may cause serious concern among employees regarding violation of their privacy. Although those employee-owned mobile devices are used for organizational work purposes, giving access and control on personal data stored in those devices may not be acceptable to the employees. Therefore, data security risk could be a concern for both employees and employers. Thus, BYOD can create threats to data security, particularly to data confidentiality, integrity and authenticity [6].

The COPE model can enhance the data security and privacy of organizations as well as employees [3]. In the COPE model, organizations have the right to disconnect mobile devices on the organization's network if necessary, such as in a situation of security breach. Thus, organizations can maintain their network

Open Science Index, Computer and Systems Engineering Vol:17, No:6, 2023 publications.waset.org/10013129.pdf

keeping sensitive data secure, which is one of the main challenges in the BYOD model.

In the COPE model, organization facilitates the mobile devices management and the mobile application management initiatives; consequently, has much greater technical and legal authority to being able to protect the organizational data. Also, in COPE the mobile device is the property of the organization and they own the line of its service. Therefore, an organization does have the authority to be able to choose which types of vendors of the mobile device to work with and which types of device models along with data plans to be provided.

Having personal and organizational data on mobile devices in BYOD models poses a great threat to the organizations due to the intended or unintended leak of sensitive data. The organizational data in mobile devices could be stored without proper security measures, which may expose the organization to the risk of data breach. Also, any personal file with malware may spread it to the organizational files and ultimately to the file servers and other internal resources in the organization. Finally, mobile devices, while used outside of the organization's network, could be connected to an unsecured wireless network and easily be victim of hackers [9].

In a BYOD environment it is risky also because employees could be careless or overconfident in sharing sensitive information online, failing to properly configure, and being the victim of phishing. BYOD is also unsafe due to data theft, malware infiltration, having the device stolen or lost, potential legal issues, lack of employee training, poor mobile management, etc. When it comes to the device being lost or stolen, the consequence can be from a big inconvenience to a disaster for the entire organization if recommended organizational data security protocols or policy not followed by the employee [22]. In addition to potential legal issues involved, an organization's reputation can be severely damaged if a security breach through an employee's device leads to a leak of crucial sensitive information of their customers or business partners. That may lead to the possibility of dealing with litigation from different parties [22]. In addition, the indistinct boundary between job-related works and personal uses of mobile devices may raise concerns regarding employers' possible access to employees' sensitive personal data and vice versa in BYOD model [8]. Denial of service attack can trigger unavailability of resources, network congestion, and bottle necks on organizational network. Unauthorized access to organizational resources with employee device can create problems of data breaches and data loss [23].

The larger organizations are more likely to employ the COPE model, as it maximizes control over device's mobility while retaining ownership of the mobile devices [24]. The advantages to COPE are the work-life balance on a single device, apps, enhanced control and authority over devices, while having relatively fewer security concerns compared to the BYOD model. The disadvantages are potential productivity issues because employee freedom is less in the COPE model as organizations are fully responsible for deploying, maintaining, and updating innovative mobile technologies.

B. Measures to Ensure Data Security

To maintain data security, organizations must balance restrictions on their sensitive data with productivity. With more than ever remote employees, especially since COVID-19 pandemic, having the right data security policy is crucial. However, given the challenges associated with mobile devices used in job-related works, managing the security of these devices and minimizing the risk can be very complex [5].

TABLE I
BYOD VS. COPE

BYOD	COPE
Employee is owner of mobile devices and apps	Organization is owner of mobile devices and apps
Employee is responsible for mobile device and service cost	Organization is responsible for mobile device and service cost
Higher employee control on mobile computing	Higher organizational control on mobile computing
Threat to data security is higher	Threat to data security is lower
Employee satisfaction higher	Employee satisfaction lower
Flexibility and convenience higher	Flexibility and convenience lower

Data security ensures the critical characteristics of information called CIA (confidentiality, integrity, authenticity) that can be established through technology, policy compliance, and human factors. When protecting data in the BYOD model, an additional security principle is required since a mobile device is not under the control of the organization but rather under the control of its employee [25].

Cyber Security Awareness and Training: Unlike the traditional environment, in BYOD model the security of the mobile device is completely in employees' control, which may open up more vulnerabilities. This is a huge risk, especially if employees are not aware of cyber security risks [8]. Employees' knowledge, skills, and understanding the importance of cybersecurity, as well as their experiences, perceptions, attitudes and beliefs play an important role in ensuring cybersecurity [26]. Developing awareness of cyber security threats and how to protect organizational data is essential to ensure data security. Therefore, organizations must provide cyber security training that specifies the basic security mechanisms and the threats to be aware of [27].

Literature shows that employees' awareness of cyber security risks has positive impacts, especially in BYOD practice. Therefore, it is important to organize training programs to raise awareness among employees regarding their responsibilities and procedures they need to follow in the BOYD model. The awareness training should focus on the importance of cybersecurity and consequences of security risk [27].

Security education training and awareness (SETA) programs via seminars and workshops are essential for employees to learn and prepare against threat to cybersecurity that may cause data breaches. Employee's participation in SETA program should be required so that they can be aware of cybersecurity policies and data protection of their mobile devices [28]. Modes of training can include classroom training, computer-based training, staff meetings, monthly newsletters, posters, and regular team discussions [15].

Data Security Policy: It is critical for organizations to have a robust data security policy and ensure that employees comply with the policy fulfilling organization's security expectations [29].

Organizations must regularly and routinely review and assess their cybersecurity policies and data protection for mobile devices [28]. Dedicated security policy provides complete guidance on authentication, access control, chain of responsibility, data ownership, devices allowed, acceptable use, training, legislation, and noncompliance [15].

Employee Compliance to Policy: As cybersecurity concerns in BYOD models have become critical to organizations, it is important that employees comply with organization's data security policies [30]. BYOD practice can create serious data security issues since organizational administrators have little controls over the mobile devices used for work and there have been concerns about regulatory compliance [31]. Organization must ensure that when employees use their personal mobile devices to access organizational data, the device must meet organization's standard of authentication as well as protection against malware to prevent from data leakage [17].

But the data security policy compliance in BYOD environment remains low [8]. When it came to compliance, the boundary of BYOD using both at home and work had raised concerns because employers may have access to employees' sensitive personal data and vice versa. It was found that compliance with the security policies has the utmost importance to address the factors that lead to the security risks. It was understood that organizations or businesses need to be able to adopt a much more holistic approach for improved security policy compliance. For that purpose, administrative support, security awareness and training, a comprehensive security policy development and review of current policy are important. In order to ensure fairness and employees willingness to follow the security process, they should be consulted in developing a comprehensive security policy [27].

Mobile Device Management Tools: Mobile devices, due to their unique capabilities, are vulnerable to specific cyber security challenges including: network-based attacks, compromise via malicious applications, phishing attempts, etc. [5]. The mobile device management (MDM) tools can address such vulnerabilities by ensuring secure access to organizational networks and other resources. These MDM tools are different from those required to secure computer desktops [3]. There are different settings in the MDM tools that can control, allow, restrict or disable features, run apps on dedicated devices, control security, and more in the COPE environment [32]. There are many MDM tools available to select and implement for data protection. These MDM, with constant protection capabilities, can identify threats to mobile devices and know how to mitigate those threats [5].

MDM is a comprehensive tool that can be efficient in addressing many cybersecurity threats associated with BYOD model. Security risks caused from weak passwords, data leaks, forfeit of management, and even complete device loss, etc. can be addressed using MDM. Furthermore, the MDM policy can also include additional policies to deal with risks to data by using mechanisms such as malware detection, encryption, PIN for access control and lockout control, jailbreak and root detection, remote wipe, etc. [33].

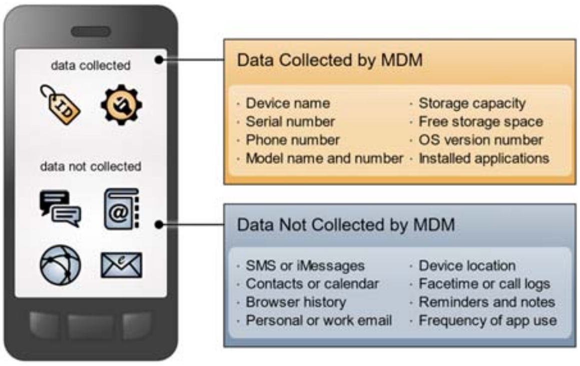

Fig. 2 Data collection process of mobile device management [21]

Finally, in the COPE model organizations need to consider the cost of a mobile device purchase, its data plan, warranty, IT management, and recycling. But in the BYOD model organizations can completely eliminate the cost of purchasing a mobile device and its management platform, and reduce the cost of the data plan [34].

V. Conclusion

This paper focused on understanding the advantages and disadvantages of BYOD and COPE models in terms of data security and costs of each. As increasing number of employees are using mobile devices for job-related work, knowing the level of threat to organizational data security causes in BOYD or COPE models, and employees' compliance with data security policies is significantly important. Comparing BYOD and COPE models, it has been found that BYOD would increase the data security risk at workplaces that may cause data security breaches. Research findings showed that in the BYOD model, a more feasible approach to achieve a secure mobile device environment is possible through the development of comprehensive security policies balancing employees' need for convenience with organizational data security [35]. To maintain data security in the BYOD model, organizations need to develop BYOD policy focusing on the type of mobile devices and apps are being used, employees' compliances with different regulations, data security measures taken, usage agreements about accessing organizational data, access to organizational resources, protection of employees' privacy, and data plans for the employees' mobile devices being used for works [34]. However, the recent studies on data security have also highlighted on organizational insiders' behavior as one of the factors of data security breaches because a large percentage of security incidents are caused by the insiders in the organizations. Therefore, to deter employees' misuse of data security policies, organizations must implement technical and procedural countermeasures. Organizations need to ensure that employees are strictly compliant with the data security policies [36].

This study reveals the unique features of mobile computing in BYOD and COPE environments in organizations. Both models show the ongoing trends toward the fluid boundaries in between the personal and the work-related usage of mobile technologies. The mobile devices in the COPE model are relatively much more secure to have at work since those are under the organization's control than in the BYOD model. The BYOD model provides benefits to both the organization and employees, but the adoption of this also can bring data risks [37]. With reduced cost and productivity BYOD model become increasingly popular [38].

Adopting specific technical measures, establishing and explaining additional data security policies to employees, and educating them to apply policy measures and to comply with the policies can ensure data security in organization, especially in the BYOD environment [9].

References

[1] Pew Research Center. (April 7, 2021). Mobile Fact Sheet. Retrieved from: https://www.pewresearch.org/internet/fact-sheet/mobile/.

[2] T. Pósa and J. Grossklags, "Work experience as a factor in cyber-security risk awareness: A survey study with university students," *J. Cybersecur. Priv.*, Vol 2, pp. 490-515, 2022. https://doi.org/10.3390/jcp2030025.

[3] NIST. (n.d.). Mobile device security: Corporate-Owned Personally-Enabled. *NIST - National Cybersecurity Center of Excellence.* https://www.nccoe.nist.gov/mobile-device-security/corporate-owned-personally-enabled.

[4] Veljkovic, and A. Budree, "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. 2019. ISSN 1566-6379

[5] M. J. Franklin, G. Howell, K. Boeckl, N. Lefkovitz, E. Nadeau, B. Shariati, G. J. Ajmo, J. C. Brown, E. S. Dog, F. Javar, M. Peck, F. Kenneth, and F. K. Sandlin, "Mobile Device Security: Corporate-Owned Personally-Enabled (COPE)," *NIST Special Publication 1800-21, NIST - National Institute of Standard and Technology. US Department of Commerce,* 2020.

[6] M. S. Doargajudhur and P. Dell. "The effect of Bring Your Own Device (BYOD) adoption on work performance and motivation," *Journal of Computer Information Systems,* vol. 60, no. 6, pp. 518-529, 2020. DOI: 10.1080/08874417.2018.1543001. https://doi.org/10.1080/08874417.2018.1543001

[7] S. H. Deba, L. K. Rohinia, D. Mishraa, K. R. Meenaa, and P. Bhattacharya, "BYOD supported crowd. interaction system," International Conference on Computational Intelligence and Data Science (ICCIDS 2018), *Procedia Computer Science, vol. 132*, pp. 1586–1591, 2018.

[8] R. Palanisamya, A. A. Normanb, and M. L. Kiaha, "Compliance with bring your own device security policies in organizations: A systematic literature review," *Computers & Security, Vol. 98,* 2020. https://doi.org/10.1016/j.cose.2020.101998.

[9] Z. Tu and Y. Yuan. "Coping with BYOD security threat: From management perspective," in *Twenty-first Americas Conference on Information Systems*, Puerto Rico, 2015. Retrieved from: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.897.2564&rep=rep1&type=pdf.

[10] L. Weber and R. J., Rudman, "Addressing the incremental risks associated with adopting Bring Your Own Device," *Journal of Economic and Financial Sciences*, vol. 1, no. 1, 2018. http:// dx.doi.org/10.4102/jef.v11i1.169

[11] F. R. R. Zambrano & G. D. R. Rafael. "Bring Your Own Device (BYOD): a Survey of Threats and Security Management Models," Int. J. Electronic Business, Vol. X, No. Y, pp.000–000, 2017.

[12] F. Annansingh, "Bring your own device to work: how serious is the risk?" *Journal of Business Strategy,* vol. 42, no. 6, pp. 392-398, 2021. © Emerald Publishing Limited, ISSN 0275-6668.

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

[14] C. T. Zhiling, A. Joni, & G. Z. Yu, "Complying with BYOD security policies: A moderation model based on protection motivation theory," *Journal of the Midwest Association for Information Systems (JMWAIS),* vol. 1, no. 2, 2019. DOI: 10.17705/3jmwa.

[15] A. T. Wani, A. Mendoza, and K. Gray, "Hospital Bring-Your-Own-Device Security Challenges and Solutions: Systematic Review of Gray Literature," *JMIR mHealth and uHealth,* vol. 8, no. 6, 2020. Retrieved from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7333072/.

[16] K. G. Gökçe and O. Dogerlioglu, "Bring your own device" policies: Perspectives of both employees and organizations," *Knowledge Management & E-Learning,* vol. 11, no. 2, pp. 233–246, 2019. https://doi.org/10.34105/j.kmel.2019.11.012.

[17] F. Jamal, M. T. Abdullah, A. Abdullah, and Z. M. Hanap. "A Systematic Review of Bring Your Own Device (BYOD) Authentication Technique," *Journal of Physics: Conference Series 1529.* 2020. 042071. doi:10.1088/1742-6596/1529/4/042071

[18] C. Vorakulpipat, S. Sirapaisan, E. Rattanalerdnusorn, and V. Savangsuk, "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.

[19] M. Olalere, T. M. Abdullah, R. Mahmod, and A. Abdullah, "A Review of Bring Your Own Device on Security Issues," *SAGE Open*, pp. 1–11, 2015. DOI: 10.1177/2158244015580372.

[20] A. Musarurwa, S. Flowerday, & L. Cilliers, "An information security behavioural model for the bring-your-own-device trend," *South African Journal of Information Management,* vol. 20, no. 1, 2018. https://doi.org/10.4102/sajim.v20i1.980.

[21] K. Boeckl, N. Grayson, G. Howell, N. Lefkovitz, J. G. Ajmo, M. McGinnis, K. F. Sandlin, O. Slivina, J. Snyder, and P. Ward. "Mobile Device Security: Bring Your Own Device," *NIST Special Publication 1800-22,* 2021. https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/bring-your-own-device

[22] G. Hollander, "The top 7 risks involved with bring your own device (BYOD)," 2019. Retrieved from: https://resources.m-files.com/blog/the-top-7-risks-involved-with-bring-your-own-device-byod-3.

[23] P. Shrestha and R. N. Thakur. Study on security and privacy related issues associate with BYOD policy in organizations in Nepal, Vol. 1, no. 2. 2019. ISSN: 2705-4683; e-ISSN: 2705-4748

[24] Calero. BYOD vs. CYOD vs. COPE - How to choose the right approach for your enterprise. Calero Software, LLC., 2020. Retrieved from: https://cdn2.hubspot.net/hubfs/430572/Content/Content%20Files/Calero_BYOD_vs._CYOD_vs._COPE_WP_10-29.pdf.

[25] M. Bada and J.R.C. Nurse. "Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs)," *Information & Computer Security,* vol. 27, no. 3, pp. 393-410, 2019. DOI 10.1108/ICS-07-2018-0080.

[26] M. Ratchford, O. El-Gayar, C. Noteboom, and Y. Wang, "BYOD security issues: A systematic literature review", *Information Security Journal: A Global Perspective,* vol. 31, no. 3, pp. 253–273, 2022. Retrieved from: https://doi.org/10.1080/19393555.2021.1923873.

[27] K. Downer, and M. Bhattacharya, "BYOD security: A study of human dimensions," *Informatics,* vol. 9, no. 16, 2022. https://doi.org/10.3390/informatics9010016.

[28] A. Koohang, M. T. Riggio, J. Paliszkiewicz, and J. H. Nord. Security Policies and Data Protection of Mobile Devices in the Workplace, Issues in Information Systems, vol. 18, no. 1, pp. 11-21, 2017

[29] X. Yang, X. Wang, W. T. Yue, C. L. Sia, and X. Luo. "Security policy opt-in decisions in Bring-Your-Own-Device (BYOD) – A persuasion and cognitive elaboration perspective," *Journal of Organizational Computing and Electronic Commerce*, vol. 29, no. 4, pp. 274-293, 2019. DOI: 10.1080/10919392.2019.1639913

[30] Z. C. Tu, A. Joni, and Y. G. Zhao, "Complying with BYOD security policies: A moderation model based on protection motivation theory," *Journal of the Midwest Association for Information Systems (JMWAIS),* vol. 1, no. 2, 2019. DOI: 10.17705/3jmwa.000045 Available at: https://aisel.aisnet.org/jmwais/vol2019/iss1/2.

[31] A. Alexandrou and L. Chen. "A security risk perception model for the adoption of mobile devices in the healthcare industry," *Security Journal*, vol. 32, pp. 410–434. 2019. https://doi.org/10.1057/s41284-019-00170-0.

[32] Microsoft. "Android Enterprise device settings list to allow or restrict features on corporate-owned devices using Intune," 2022. Retrieved from: https://learn.microsoft.com/en-us/mem/intune/configuration/device-restrictions-android-for-work

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

[34] IBM corporation. "Top 10m rules for Bring your own device (BYOD)," 2020. IBM Security. Retrieved from: https://www.ibm.com/downloads/cas/YK52D6GD.

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

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

[37] J. Ophoff and S. Miller. Business priorities driving BYOD adoption: A case study of a South African financial services organization, *Issues in Information Science and Information Technology,* vol. 16, 2019.

[38] M. S. Doargajudhur, "Impact of BYOD on organizational commitment: an empirical investigation," *Information Technology & People,* vol. 3, no. 2, pp. 246-268, (2019). © Emerald Publishing Limited 0959-3845 DOI 10.1108/ITP-11-2017-0378.