Optimizing Security Compliance in Bring Your Own Device (BYOD) Through a Hybrid Approach

Norkhushaini Awang[1*], Noor Sabariah Salleh[2], Nurul Huda Nik Zulkipli[3] and Omar Zakaria[4]

[1] College of Computing, Informatics, and Mathematics, Universiti Teknologi MARA 40450 Shah Alam, Selangor, Malaysia
[2] The Inland Revenue Board of Malaysia, Jabatan Teknologi Maklumat, 63000 Cyberjaya Selangor, Malaysia
[3] College of Computing, Informatics and Mathematics,Universiti Teknologi MARA Melaka (Jasin Campus) 77300 Merlimau, Melaka, Malaysia
[4] Faculty of Defense Science and Technology, Universiti Pertahanan Nasional Malaysia, 57000 Kuala Lumpur, Malaysia
shaini@tmsk.uitm.edu.my

Abstract. Bring Your Own Device (BYOD) is a work environment that allows employees to use their devices to access the organization's resources to complete their tasks. However, BYOD has raised some security concerns because it presents organizations with more significant challenges in protecting their data assets. As a result, a well-managed BYOD policy and guidelines should be established and enforced in Malaysia, particularly in the public sector. Hence, the purpose of this study is to identify the risk of information security in BYOD faced in the Malaysian Public Sector (MPS) due to non-compliance behaviour of security policy. After that, this study proposed countermeasure strategies for handling the identified risks. In this research study examined the elements that impact employees' willingness to comply with the BYOD security policy based on Protection Motivation Theory (PMT). The process of reviewing current and past research on information security is carried out. A mixed-method research approach has been applied in this study, with the main data collection method including interviews, document analysis, and surveys. A specific group, which consists of 21 respondents from the Malaysian public sector, has participated in the survey. It is expected that organizations in MPS are more prepared to establish the BYOD security policy by studying employees' behaviour in complying with BYOD security policy requirements.

Keywords: Bring Your Own Device, Security Compliance, PMT Model, PPT Model

N. A. S. Abdullah et al. (eds.), *Proceedings of the International Conference on Innovation & Entrepreneurship in Computing, Engineering & Science Education (InvENT 2024)*, Advances in Computer Science Research 117,
https://doi.org/10.2991/978-94-6463-589-8_43

1 Introduction

The rapid technological change makes it more challenging to use security and privacy theories and models to secure personal data. The successful usage and deployment of information and communication technology (ICT) systems throughout the world and the continued dependence on them have given ICT firms more confidence in developing and introducing technological advancements like mobile computing technologies. Employees in modern firms are increasingly using their technical gadgets or applications for work-related tasks. This "IT consumerization" of the workplace, also known as "consumerization of IT," represents a significant shift in modern work life and has several advantages, including improved innovation, increased productivity, and increased employee satisfaction [2]**.** The consumerization of IT and known as Bring Your Own Device (BYOD) encourages employees to use their personally owned mobile devices to do work, whether inside or outside their workplaces. The BYOD phenomenon mainly changes the operational procedures and methods organizations use to conduct business. Under the BYOD concept, employees can use personal mobile devices to access business data, apps, records, managed networks, the web, and other enterprise content. Employees are given the power and opportunity to choose the technology that best suits their needs. BYOD also boosts employee happiness, productivity, and flexibility [6]**.** BYOD aims to increase productivity and speed of work by creating an atmosphere where workers may work from anywhere at any time. Furthermore, bringing your own device (BYOD) is meant to provide new business and service options [8]. BYOD usage in the public sector has not been widely adopted because of a lack of understanding and acceptance of its advantages. According to Ovum's study "BYOD: an emerging market trend in more ways than one," management of BYOD is a problem in several countries, including Malaysia, with just 20.1 percent of BYOD being correctly managed **[6].** Therefore, the comprehensive BYOD policy and guidelines for well managed should be established and enforced in Malaysia, primarily in the Public Sector. As a strong defense against these threats, many organizations have information security policies (ISP) in place to control employees' behavior when using information technology (IT) [7]**.** Employees that are oblivious to adherence to the security policy are common. Humans are seen as the weakest link in the security chain. Thus, organizations have faced significant hurdles when dealing with compliance concerns **[7].**

2 Literature Review

In today's environment, new technology is critical as a tool to aid employees in completing their jobs. As a result, new trends have evolved to boost employee productivity by allowing them to readily access data and information via smartphones, tablets, and phablets. As a result, bring your own device (BYOD) is a strategy that allows workers, business partners, and other users to use and access data and information to run workplace apps that are becoming increasingly common throughout the world [3]**.** In the literature, there are several definitions of BYOD. BYOD is defined as a policy

that allows employees to use their own mobile devices, such as smartphones, laptops, and tablet PCs, to access various applications or company information, whether on their network or the corporate network. As a result, they are allowed to work on their business premises or while working outside, for either official or personal purposes. Therefore, BYOD can boost agility and productivity in executing duties entrusted to employees in the organization [5]. In most circumstances, Bring Your Own Device (BYOD) principles benefit both organizations and employees. BYOD is a cost-cutting approach for the company since it avoids expensive hardware purchases while allowing employees to use a device they are acquainted with. The commercial benefits of using BYOD in the workplace include increased worker productivity, cost savings, increased employee happiness, and simplified corporate system administration [9]**.** Because it provides information security, BYOD deployment in the public sector requires intense observation [4]**.** The most crucial aspect of implementing BYOD for an organization is to provide a computing platform that is efficient, secure, and friendly to portable devices. The BYOD platform should incorporate an organization's full infrastructure.

3 Research Methodology

This study is based on a mixed-method research approach whereby both qualitative and quantitative data collection techniques are used. The qualitative method's result assists in developing the quantitative data gathering instrument. In the public sector, the use of mixed techniques helps researchers better comprehend their research problems and anticipate and accept study results. At an exploratory stage, a semi-structured interview assists researchers in extracting the key information [1]**.** To study the security behavior among employees, the Protection Motivation Theory model is used. Threat appraisal components include Perceived Vulnerability (PV), which is an individual's estimation of the likelihood of a threat occurring, and Perceived Severity (PS), which refers to the seriousness of the threat (Johnston & Warkentin, 2010; Liang & Xue, 2009). Coping appraisal components consist of Self-Efficacy (SE), which is the employee's confidence in their ability to take the necessary action (Bandura, 1977, 1982); Perceived Effectiveness (PE), which is the subjective assessment of how effectively a safeguarding measure can prevent a security threat (Liang & Xue, 2009); and Perceived Cost (PC), which is the physical and cognitive effort required to comply with BYOD security policies. Therefore, the constructs in the PMT model, including PV, PS, SE, PE, PC, and CI, along with BYOD's unique features such as Mixed Usage (MU) and Surveillance Visibility (SV), are tested. According to PMT, an individual's reaction to a threat is the result of two appraisal processes: threat appraisal and process of coping appraisal. It's one of the most effective hypotheses for predicting individual intentions to take preventative measures. Based on PMT, a study model was built proposing that both threat and coping assessments influence an employee's intention to follow the organization's BYOD security policy. Specific BYOD characteristics, such as surveillance visibility and mixed usage, minimize some relationships. People assess a threat based on their own perception of the severity of the

threat, susceptibility to the threat, and its probability of occurrence. Once an employee is conscious of the security threat, they will establish beliefs about the probability of personally experiencing the threat and its seriousness.

4 Findings and Discussions

This section presents the result of the data analysis in three sections and the discussion of those results. The first section presents the demographic information of the Malaysian public sector's respondents. The second section presents the implementation of the BYOD environment in the Malaysian public sector. The third section contains the results of the analysis by identifying factors that influenced the Malaysian public sector employees to comply with BYOD security policy. The last section discusses the results of the data analysis obtained by answering all the research questions that had been stated. Descriptive statistics are used as the main analysis method, which is appropriate for the questions being asked in this research. In this study, descriptive statistics described the data collection and summary of the data simply and easily such as a table, figure, frequency, percentage, mean and standard deviation. Thus, it involved the demographic profile of respondents and factors on BYOD Security Policy Compliance in the Malaysian public sector.

4.1 Reviews on BYOD Program

This section discusses the current BYOD practices and policies in the respondents' organizations as shown in Table 1. Most organizations allow employees to bring their own mobile devices to the workplace, with 95.2% of respondents indicating this practice. Additionally, 95.2% of respondents bring their personal mobile devices to work, although 76.2% of organizations do not support purchasing these devices for employees. The majority of personal mobile devices used are smartphones (90.5%), followed by laptops (85.7%) and tablets (42.9%), and 81% of respondents are allowed to connect these devices to the corporate network.

Table 1. Current Practice and Policies of BYOD in Organizations.

BYOD Program		Frequency	Percentage (%)
Do organization allow employees to bring their own mobile devices into the workplace?	Yes	20	95.2
	No	1	4.8
Bring your personal own mobile device to your workplace?	Yes	20	95.2
	No	1	4.8
Organization support in terms of finance to buy your own mobile device?	Yes	5	23.8
	No	16	76.2
Types of Personal Mobile Devices:			
Smartphone	Yes	19	90.5
	No	2	9.5
Tablet	Yes	9	42.9
	No	12	57.1
Laptop	Yes	18	85.7

Meanwhile, Table 2 showed a list of applications which were allowed to access from mobile devices. Based on the result showed that most respondents choose email applications with 17 respondents (81%) followed by video conferencing applications with 15 respondents (71.4%), company application, and calendaring & scheduling with 11 respondents (52.4%). Meanwhile, the minority of the respondents choose directories and file servers with 3 respondents (14.3%).

4.2 BYOD Security Policy Compliance in Malaysian Public Sector

Table 3 showed the finding of the extent to which one uses own device for work for mixed usage. These findings showed a majority of the respondents choose "*I occasionally use my own device for work and do not store organization data in my own device"* with 12 respondents (57.1%) followed by "*I sometimes use my own device for work and store a little organization data in my own device"* with 7 respondents (33.3%) and "*I use my own device for work in most time work and store a lot of organizational data in my own device"* with 2 respondents (9.5%).

Table 2. Allowed Application in the Organization

Application Organisation Allow on Devices		Frequency	Percentage (%)
Email	Yes	17	81.0
	No	1	4.8
Company Application	Yes	11	52.4
	No	7	33.3
Document Access	Yes	7	33.3
	No	11	52.4
Intranet	Yes	8	38.1
	No	10	47.6
Video Conferencing	Yes	15	71.4
	No	3	14.3
Calendaring & Scheduling	Yes	11	52.4
	No	7	33.3
Databases	Yes	7	52.4
	No	11	33.3
Directories	Yes	3	71.4
	No	15	14.3
File Servers	Yes	3	14.3
	No	15	71.4

Table 3. Mixed Usage

The extent to which I use my own device for my work.	Frequency	Percent
I occasionally use my own device for work and do not store organization data in my own device	12	57.1
I sometimes use my own device for work and store a little organization data in my own device	7	33.3
I use my own device for work in most time work and store a lot of organization data in my own device	2	9.5
I fully use my own device for work and store all working data in my own device	0	0.0
Total	21	100

Table 4 showed the finding of the extent to which organizations monitor employees' BYOD usage by surveillance visibility. These findings showed majority of the respondents choose "*My organization does not monitor employees' BYOD usage at all"* with 11 respondents (52.4%) followed by "*My organization requires employees to safeguard their BYOD usage by themselves, but no formal measures and controls for monitoring"* with 5 respondents (23.8%), "*My organization has some measures and controls to monitor employees' BYOD usage"* with 4 respondents (19%) and "*My organization has complete measures and controls to monitor employees' BYOD usage*" with 1 respondent (4.8%).

Table 4. Surveillance Visibility

The extent to which my organization monitors employees' BYOD usage	Frequency	Percent
My organization does not monitor employees' BYOD usage at all	11	52.4
My organization requires employees to safeguard their BYOD usage by themselves, but no formal measures and controls for monitoring	5	23.8
My organization has some measures and controls to monitor employees' BYOD usage	4	19.0
My organization has complete measures and controls to monitor employees' BYOD usage	1	4.8

Overall sample based on the intention to comply with BYOD security policies with the perceived vulnerability, perceived severity, coping action self-efficacy, perceived effectiveness, perceived cost, mixed usage, and surveillance visibility. The R2 (73.8%) of the intention to comply with BYOD security policies is mainly due to the perceived vulnerability, perceived severity, coping action self-efficacy, perceived effectiveness, perceived cost, mixed usage, and surveillance visibility, and the 26.2% indicates other factors. Based on the findings presented in Figure 1, the R^2 value of 73.8% indicates that the theoretical model moderately explains the variance in employees' intentions to comply with BYOD security policies. The analysis reveals that coping action Self Efficacy (SE) and Surveillance Visibility (SV) have a significantly positive relationship with compliance intentions, as evidenced by p-values less than 0.05. Surveillance Visibility (SV) emerges as the strongest predictor, with a beta coefficient of 0.032 ($p<0.05$), followed closely by Self Efficacy (SE), with a beta coefficient of 0.040 ($p<0.05$). These findings suggest that features such as SV have the potential to significantly influence employees' compliance with BYOD security policies. Additionally, the reliability test confirms the validity and reliability of the scales used, with Cronbach's alpha values exceeding 0.70 for all variables. The analysis also shows that Perceived Effectiveness (PE) has a greater impact on compliance intention when devices are used for both personal and professional purposes (M=4.678, SD=0.441), while Perceived Cost (PC) has a lesser impact when employees are under

closer surveillance (M=3.127, SD=1.275). Overall, respondents expressed strong agreement with the intention to comply with BYOD security policies (M=4.793, SD=0.401) and acknowledged Perceived Vulnerability (PV) (M=4.269, SD=0.997).

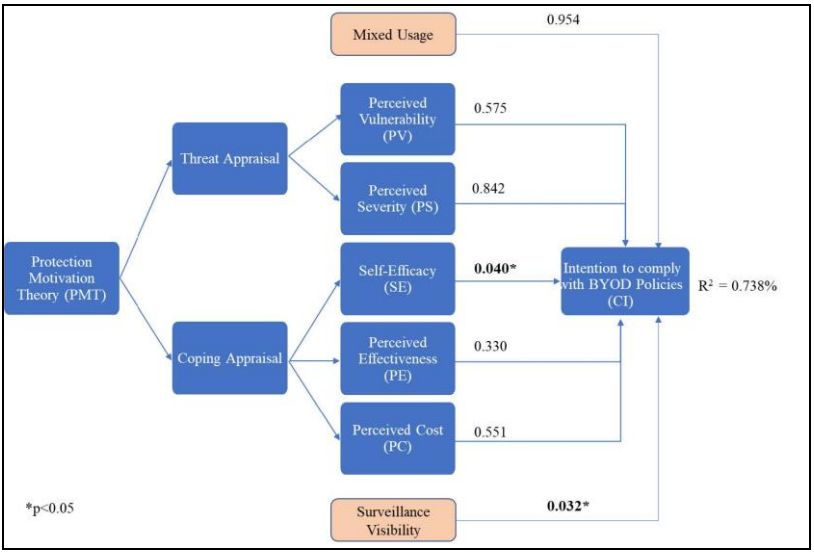

Fig.1 Feedback on Utilizing the Protection Motivation Theory (PMT) Model

A systematic literature review identified security risks arising from non-compliance with BYOD security policies, which were mapped according to the People, Process, and Technology (PPT) model. Under the "People" category, employees, particularly younger ones, were found to be vulnerable to phishing and often unaware of the risks associated with their actions, especially when using unsecured networks. The "Process" category highlighted issues such as inconsistent policy enforcement and a lack of BYOD security training, which leaves employees ill-equipped to handle security threats. The "Technology" category revealed that the management of personal devices poses significant risks, as these devices can easily be lost or stolen, and malware can exploit vulnerabilities, leading to potential breaches of the organization's network. Furthermore, the rise of shadow IT, where unauthorized devices and applications are used without the IT department's knowledge, exacerbates the challenge of securing the organization's data from external threats. Overall, the review underscores the critical need for comprehensive BYOD policies, effective employee training, and robust technological safeguards to mitigate security risks. The detailed findings of this systematic literature review are presented in Figure 2. This figure illustrates the identified security risks associated with non-compliance to BYOD policies, categorized under the People, Process, and Technology (PPT) model.

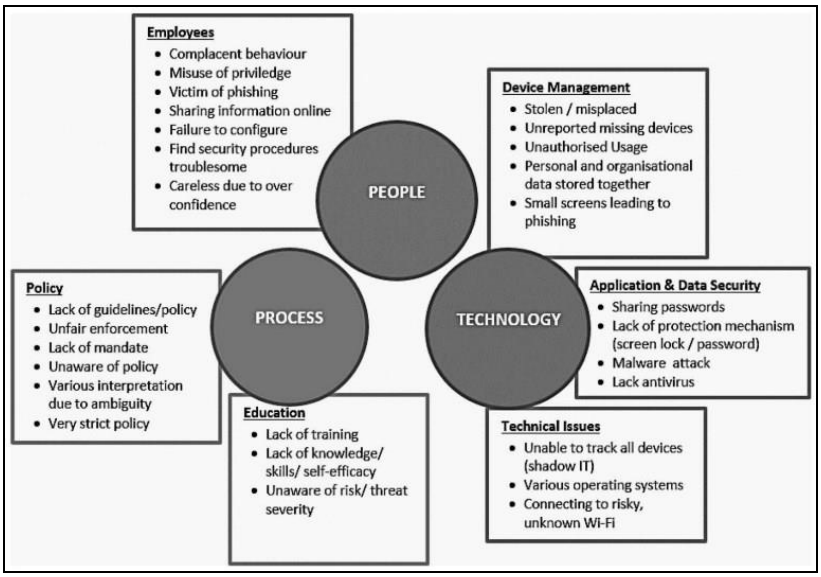

Fig.2 Findings from the People, Process, and Technology (PPT) Model

5 Conclusion

This study provides valuable insights into employee compliance with BYOD security policies, utilizing a moderation model based on the Protection Motivation Theory (PMT). The findings underscore the significance of threat and coping appraisals in influencing employees' adherence to BYOD policies and reveal that unique features of BYOD environments moderate this relationship. This research study contributes to the field by expanding the PMT framework to the largely underexplored area of BYOD security compliance and establishing new metrics to address the specific challenges of BYOD threats. The empirical validation of construct measures enhances the reliability and validity of the findings, offering a foundation for future research in this domain. Furthermore, the study has practical implications for management practices, highlighting the necessity for organizations to develop policies that address the additional security risks associated with BYOD usage. Given the growing trend of employees using various mobile devices for personal and work-related tasks, it is important to comprehend their behaviour and attitudes towards the security of Bring Your Own Device (BYOD) policies. The results demonstrate that organizational monitoring and surveillance can mitigate the negative impact of perceived costs on compliance intentions, suggesting that effective policy enforcement and monitoring are essential for improving adherence to security standards. The findings of this study will assist organizations in developing and implementing more efficient BYOD security policies, thereby strengthening the protection of important assets and improving the overall security position of the organization.

References

1. Ali, R. F., Dominic, P. D. D., & Ali, K. (2020). Organizational governance, social bonds and information security policy compliance: a perspective towards oil and gas employees. Sustainability (Switzerland), 12(20), 1–27. https://doi.org/10.3390/su12208576
2. Chen, H., Li, Y., Chen, L., & Yin, J. (2021). Understanding employees' adoption of the Bring-Your-Own-Device (BYOD): the roles of information security-related conflict and fatigue. Journal of Enterprise Information Management, 34(3), 770–792. https://doi.org/10.1108/JEIM-10-2019-0318
3. Chountalas P, Karagiorgos T. Bring Your Own Device philosophy from the user's perspective: An empirical investigation. InProceedings of the 2nd HOBA International Conference 2015 Mar 7 (Vol. 1, pp. 1-12).
4. In, R. (2016). Byod p. 323–326.
5. Mahat, N. B., & Ali, N. B. (2018). Empowering employees through BYOD: Benefits and challenges in Malaysian Public Sector. International Journal of Engineering and Technology (UAE), 7(4), 643–649. https://doi.org/10.14419/ijet.v7i4.35.23077
6. Ogie, R. (2016). Bring Your Own Device: An overview of risk assessment. IEEE Consumer Electronics Magazine, 5(1), 114–119. https://doi.org/10.1109/MCE.2015.2484858
7. Palanisamy, R., Norman, A. A., & Kiah, M. L. M. (2019). Bring your own device (BYOD) security policy compliance framework. Proceedings of the 23rd Pacific Asia Conference on Information Systems: Secure ICT Platform for the 4th Industrial Revolution, PACIS 2019.
8. Tanimoto, S., Yamada, S., Iwashita, M., Kobayashi, T., Sato, H., & Kanai, A. (2016). Risk assessment of BYOD: Bring your own device. 2016 IEEE 5th Global Conference on Consumer Electronics, GCCE 2016, 16–19. https://doi.org/10.1109/GCCE.2016.7800494
9. Zain, Z. M., Othman, S. H., & Kadir, R. (2017). Security-based BYOD risk assessment metamodelling approach. Proceedings Ot the 21st Pacific Asia Conference on Information Systems: "'Societal Transformation Through IS/IT'", PACIS 2017.