International Journal of Engineering & Technology, *7 (4.35) (2018) 643-649*

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Empowering Employees through BYOD: Benefits and Challenges in Malaysian Public Sector

Norhazilah binti Mahat[1]*, Nor'ashikin binti Ali[2],

[1 2]College of Graduate Studies, Universiti Tenaga Nasional, 43000 Kajang, Selangor, Malaysia
**Corresponding author E-mail: norhazilahmahat@gmail.com*

Abstract

In today's world, the development of new technologies has transformed the way employees perform their tasks without the limit of time and place. Bring Your Own Device (BYOD) is a concept to enable employees to perform their tasks with the limitless infrastructure, which allows mobility and access to anyone, anywhere using their own devices. The growing trends of BYOD have many benefits including increased employees' productivity, increased employee satisfaction, and reduced costs. Despite the benefits, companies are also facing challenges such as security, loss and stolen of device and data, as well as malware attacks. One of the reasons for these challenges is that the BYOD policy is still not established and enforced in the public sector. Failure to create BYOD policy will have a negative impact on the organisation. However, issues and benefits are only anecdotes and they are not empirically studied in the public sector. Therefore, this study aims to identify benefits and challenges in Malaysian Public Sectors (MPS). Through literature review, benefits and challenges were extracted to list out the construct by measuring the frequency of constructs appearing in the literature. For that purpose, the quantitative survey will be conducted.

Keywords: *BYOD; Public Sector; Benefit; Challenge*

1. Introduction

Bring Your Own Device (BYOD) is a concept that allows employees to utilize their technology personally using own devices, which they will be connected to access data with, from, or perform tasks for their organisations [1]. By adopting BYOD, users will be able to access employer-provided services and data using their personal tablets, smartphones, e-Readers and other devices [1]. Mobile devices, for example, cell phones and tablets offer flexibility to employees to perform their work from anywhere and anytime. As a result, BYOD gives a better accessibility, openness, versatility of information and cost saving for organisations.

Due to growing number of employees having mobile devices, some organisations are taking the opportunity to exploit this technology as a means to improve employees' productivity, job satisfaction, and mobility. These gadgets are used by employees as the method for interfacing, connecting with others, and progressively utilising their cell phones for business-related purposes. Research by CISCO as mentioned by Miller, Voas, and Hurlburt [2] in their study of BYOD security and privacy revealed that 95 percent of organisations in the United States allow employees to bring and use their personal devices for organisational purposes.

A growing literature has clearly stated the benefits of embracing the BYOD such as employees becoming more productive, improved employees' satisfaction and increased mobility. Despite these advantages, there are a few issues that need to be addressed. One of the main concerns is information security issues. Without the security measures and without any appropriate planning in BYOD implementation, organisations might expose their data to threats. This has been agreed by Olalere et al. [3] who emphasized the importance of security in BYOD implementation. In addition to security, other issues such as loss of stolen data and devices, data privacy violation, malware attack are also among the concerns of BYOD owners [4]–[6]. The stated issue is due to too much activity by BYOD is unmanaged properly. The survey by Ovum revealed that 18 per cent of organisations' IT department is oblivious of BYOD activity, while a further 28 per cent of organisations' IT department actively ignore it as it happens [7].

Studies by Ovum on "BYOD: an emerging market trend in more ways than one," found that, management of BYOD is an issue in many countries including Malaysia, at an average of only 20.1 percent of BYOD being managed properly [8]. Therefore, the comprehensive BYOD policy and guideline for well managed should be established and enforced in Malaysia, primarily in the Public Sector. The use of BYOD in the public sector has not been fully adopted due to lack of awareness and acceptance of BYOD's interests and benefits. In order to explore the current practice of BYOD among employees in the public sector, it is important to understand the issues and benefits of BYOD. However, the issues and benefits are only anecdotes and they are not empirically studied in Malaysian Public Sectors. Outside from Malaysia, the existing studies are mostly focused on private industries, Small, Medium and Micro Enterprises (SME), school and higher education [9]–[13], while in Malaysia existing study mostly focus on higher learning institutions, and organization as a whole [14]–[17]. Therefore, this study aims to fill this gap by investigating the current practices of BYOD as well as benefits and challenges in Malaysian Public Sectors (MPS).

2. Methodology

This study was implemented in two (2) steps. The first step, the BYOD benefits and challenges perspective were derived through an extensive literature review on content from high quality information systems journals databases was limited to those published between the years of 2012 – 2018. High quality information journals databases including:

- Emerald Insight (https://www-emeraldinsight-com.ezproxy.uniten.edu.my)
- IEEE Xplore Digital Library (https://ieeexplore-ieee-org.ezproxy.uniten.edu.my/Xplore/dynhome.jsp?tag=1)
- Science Direct (https://www-sciencedirect-com.ezproxy.uniten.edu.my/)
- Scopus

In addition, Google Scholar and online article were utilized to find suitable articles and journals based on the searching keyword. Based on the research question, the searching keywords are used to seek literature using a combination of Boolean operators (AND / OR). The pattern used in the keywords are:

- Bring Your Own Device AND Organisation
- BYOD AND Benefit AND Challenge
- BYOD AND Public Sector
- BYOD AND government

As a result, a total of 176 articles were downloaded for further examination and twelve (12) articles were selected for further study based on the title of papers and abstracts to answer the research questions.

The second step, benefits and challenges were extracted to list out the constructs by measuring the frequency of constructs appearing in the literature. For this study, the quantitative survey will be conducted among the staff of the category in management and professionals as well as the implementation team in various categories of IT and Non-IT schemes in the Malaysian Public Sector. The questionnaire will be submitted using the online survey form for one month.

3. Literature

3.1. Definition of BYOD

In today's world, the evolution of new technology is important as a tool to assist employees to carry out their tasks. As a result, new trends have emerged to increase employees' productivity through smartphones, tablets and phablets to easily access data and information to organize. Therefore, BYOD is a strategy that enables employees, business partners and other users to utilize and access data and information to execute enterprise applications that are becoming ubiquitous across the globe [11] .

Various definitions of BYOD are found in the literature. For the purpose of this research, BYOD is defined as the policy that enables employees to use their own mobile devices such as smartphones, laptop and tablet PCs to access various applications or company information whether using their own network or corporate network. Accordingly, they are able to work at their workplace or while working outside either for official or personal use. Therefore, BYOD can increase agility and improve productivity in carrying out the tasks entrusted among employees in the organisation.

The use of mobile devices for work purposes is generally considered unavoidable across all industries and that includes government employees. Now many governments implemented BYOD in their country to cater to digital technology in workplace activities. For the successful implementation of BYOD, some organisations have provided financial support, by offering BYOD toolkit and policy draft to ensure the BYOD implementation is on track [1], [13]. For instance, the Australian Federal Government in 2008 - 2013 provided funding to Victorian secondary schools to buy laptops to their students for a new era of 21st-century learning achieved a 1-to-1 computer to student ratio [13].

In Malaysia scenario, the use of the mobile device by employees in the workplace has shown an increase. Fig. 1 from StatCounter's has shown that the increase in demand for mobile equipment versus desktops has seen an increase from May 2017 to April 2018 [18]. It is a clear indication of the use of mobile equipment in Malaysia has been widespread and become a trend among employees.

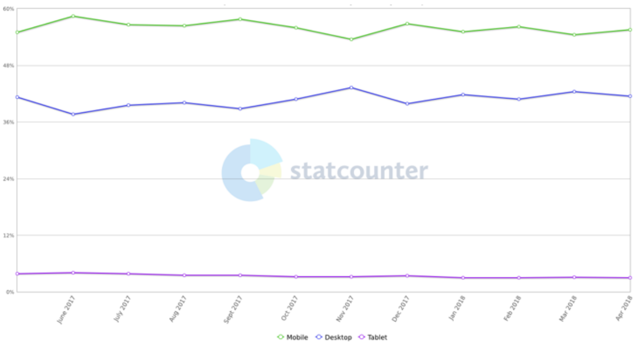

Fig. 1: Desktop vs Mobile vs Tablet Market Share Malaysia From May 2017 – Apr 2018

3.2. BYOD in Malaysian Public Sector

In Malaysia, BYOD captured the attention of Malaysian organisations whereby it has become a trend in Higher Learning Institutions. Onyechere Ugochukwu and Ismail [14] reported that various aspects of BYOD in Higher Learning Institutions include the level of BYOD awareness, the use and purpose of BYOD, the problems faced by users and the level of user satisfaction in college while using the BYOD. The study found that using personal devices at workplace provide benefits in terms of increased productivity and flexibility. Furthermore, this study claims that employees and students in organisations with regulated BYOD policy are productive, blissful, and collaborative. Despite many benefits, they found that data security is a major risk that threatens BYOD's implementation [14].

In another study by Majid and Mansor [16], it was indicated that a BYOD policy is a critical step in maintaining organisations' security if the employees are allowed to bring their own personal devices. They believe that the absence of BYOD's policies in the organisation may lead to problematic security issues such as organisational data safety and privacy when employees' devices are used [16]. Therefore, Majid and Mansor [16] concluded that BYOD security framework is also considered necessary as a solution to explicitly address and clarify device ownership, provide guidelines for management of policies and maintenance of employees' devices. Meanwhile, in another study of BYOD in private higher learning institutions, it was suggested that the BYOD policy should be proposed to help the public sector in adopting BYOD trend [15]. The importance of BYOD policy is also supported by government initiatives in Public Sector ICT Strategic Plan (PSICTSA). PSICTSA is a five year plan (2016 – 2020) that declares the strategic direction of ICT practices and policies in the public sector [19]. One of the strategic thrusts in PSICTSA, the Strategic Thrust 3 indicates that BYOD usage policy needs to be outlined to strengthen a secure cyber environment.

In Malaysian Public Sector (MPS), what available is only Information Security Policy document or officially named as *Dasar Keselamatan* ICT (DKICT). DKICT contains rules that must be read and adhered to in using Information and Communication Technology (ICT) assets but does not explicitly address BYOD policies. This policy only explains to all users about their responsibilities and roles in protecting the organisation's ICT assets.

Failure to create BYOD policy will have a negative impact on the organization. Among them are security issues, loss of data and data privacy violations. When employees use BYOD, the data and organisational information can be accessed through the employee's personal devices. Access to organisational information can be done in the organisation or anywhere. It is more dangerous if the employee has moved or stopped working, but the data and information are still on their personal devices. Furthermore, employees will face the risk of data loss because the device may be lost or stolen from or outside of the workplace due to its small and mobile size [5]. In any event of loss of device, the employees may have the risk of losing personal data information that is combined with employer data, and for security reason, the organization has the control measure to wipe out data on the device remotely. This has become a concern for employees in losing their personal data [20].

Despite many issues and challenges, a number of studies on BYOD have shown that organisations have acknowledged the benefits of BYOD and thus, have begun to embrace this trend. Employees are allowed to utilize their personally-owned technology to complete tasks for their organisations. As mobile technology permeates the workplace, public sectors are also under pressures to embrace this new trend; however, they are still at the early stage and still exploring BYOD [21]. Thus, the studies on the implementation of BYOD in public sectors are limited, and require further investigation. For public sectors to truly understand BYOD and implement BYOD successfully, they should have an understanding of the benefits that BYOD can bring and what challenges they have to face if this new trend was brought in to their employees. To date, research findings has provided very limited benefits and challenges. In addition, the research using empirical evidence is insufficient. It is critical to look at a broad set of benefits and challenges simultaneously that involve comprehensive analysis. As there is no such guideline being prepared before for public sectors specifically Malaysian Public Sectors, this study is expected to contribute to the process of adopting BYOD in a better and informed manner. Therefore, this study aims to explore and examine the benefits and challenges of BYOD in **Malaysian** P**ublic Sectors.**

4. Benefits of BYOD

The introduction of BYOD has offered many potential benefits to both employers and employees including increased productivity, employees' satisfaction, lower corporate IT costs, job flexibilities and increased mobility among the most frequently mentioned in literature. These benefits were among the findings in previous studies as summarised in Table 1. Altogether, there were sixteen (16) benefits retrieved from twelve articles. However, only five (5) were considered the most important based on the frequency as shown in Table 2.

4.1 Increased Productivity

According to a survey conducted by Forrester Consulting [29] for Trend Micro revealed that 70 percent of respondents said increasing worker productivity was the primary driver for the BYOD deployments. As mobile technology is transitioning from an amenity to a necessity, BYOD has been a new trend to be embraced by organisations to improve their productivity. BYOD gives employees and employers more flexibility to complete their tasks at home, at work, during outstation or while waiting for a meeting. Chountalas and Karagiorgos [11] reported that employees can interact and respond directly to business tasks notwithstanding of where they are either outside of office hours or outside their office. Moreover, the employees working with their personal devices are more likely to work outside of office hours, to perform basic administration tasks or check email even weekend or vacation [5], [11]. Generally, BYOD enhances operational efficiencies and indirectly increases the productivity of the organisation.

4.2. Employee Satisfaction

Employee satisfaction is the satisfaction of employees with their jobs or the degree to which employees like their jobs [30]. It is an important element for organizational development. Based on the two-factor theory by Herzberg, motivators (achievement, recognition, the work itself, advancement and growth) can lead to satisfaction [31], [32]. Among the effects of using BYOD are it can help employees achieve good working condition that helps their advancement and growth in their jobs that can boost productivity and thus, increase employees' satisfaction [23]. According Shumate and Ketel [25] claimed that their job satisfaction has increased when working with their own device. Employees' satisfaction is achieved as the effect of BYOD when employees feel comfortable and enjoy using their devices. The consequences of job satisfaction include better performance and improves stability of an employee's dedication to the organization [33]. According to a survey by CCMI [34], the use of BYOD in business was seen as a means of enabling the employees satisfaction by 19 percent. Thus, as observed from prior studies, employees working with their devices and appropriate technology feel more comfortable at the workplace and satisfied with their work accordingly.

4.3. Lower IT Costs

The implementation of the BYOD strategy introduces a measure of cost saving to organisations where the cost purchasing and maintenance of devices have been shifted to employees [20], [22], [23]. According to Chountalas and Karagiorgos [11], the cost can be reduced because employees are willing to bear the cost of purchasing, maintaining and upgrading their own devices that they use for working. In addition, Mitrovic et al. [4] in their study of the use BYOD in ICT organisation reported that cost reduction also includes the cost of exclusion of software and hardware, which also means less expenses from the organisational budget for maintenance. Therefore, this finding highlights that BYOD's implementation requires time and initial investment to create support infrastructure but in the long run, it reduces IT procurement and IT costs.

4.4. Job Flexibility

Work flexibility is to give employees the control and the freedom to carry out their work based on the suitability of the place and time. Employees can access company resources such as e-mail, calendar and scheduling, documents, applications and so on with their personal devices either for work or for personal use anytime and anywhere [35], [36]. Besides that, previous studies by Hinks [37] have reported that if employers allow their employees to use BYOD to complete their task at home, they can improve communication and cooperation among employees.

Additionally, this flexibility is appealing to employees who have the constraints of family members or community members with disabilities to work [24]. Furthermore, this flexibility allows employees to be able to communicate to solve critical problems even if they are out of the office or when they are stuck with traffic conditions [24]. Therefore, flexibility in a job can help employees perform tasks smoothly without affecting the organisation's business.

4.5. Increased Mobility

As defined by Abowd et al. [38], mobility basically means not being tied to a geographic location. It is often related to making information available whenever and wherever is needed [39]. From an organisation's perspective, the most foremost benefit that BYOD can bring is it can improve mobility as employees are now able to work whenever and wherever they like, using their personal mobile devices [4]. Consequently, organisations will have an advantage of higher productivity among employees which stems from the improved employee satisfaction and worker mobility [11]. BYOD strategy provides the flexibility and the mobility to respond immediately to requests even if the employees are not working at that specific moment [11]. The BYOD trend is also expected to grow in developing countries, such as Indonesia. Research by the International Data Corporation, Putri and Hovav [40] reveals that the BYOD trend in Indonesia is predicted to increase by 52 percent and they planned to increase mobility at work with their mobile device. Hence, mobile services on employee-owned devices can allow employees to work efficiently and increase productivity regardless of their time or location.

5. BYOD Challenges

Various challenges exist in the implementation of BYOD in organisations. For the purpose of this study, we have identified four (4) challenges based on the frequency obtained in the literature as shown in Table 3. Among them are security issues, loss and stolen data and device, data privacy violation, and malware.

Table 1: List of Benefits and Challenges BYOD

BIL	**SOURCE**	**1.** [22]	**2.** [5]	**3.** [4]	**4.** [23]	**5.** [24]	**6.** [25]	**7.** [26]	**8.** [27]	**9.** [6]	**10.** [11]	**11.** [28]	**12.** [20]
	BENEFITS												
1.	Increased productivity	√	√	√	√	√		√		√			
2.	Employee satisfaction	√	√		√	√	√						
3.	Lower corporate IT costs			√	√		√	√		√			
4.	Job flexibility					√		√		√	√		√
5.	Increased mobility			√			√	√			√		
6.	Innovation benefits	√											
7.	Enjoyment												√
8.	Enhanced job collaboration					√							
9.	Employees efficient						√						
10.	Convenient, user friendly									√			
11.	Technology empowerment												√
12.	Accessibility to data		√										
13.	Technology familiarity, agility							√					
14.	Time savings									√			
15.	Monitoring of system can be done remotely									√			
16.	Performance enhancement					√							
	CHALLENGES												
1.	Security							√	√	√		√	√
2.	Lost and stolen data and device		√	√			√			√			
3.	Data privacy violation									√	√	√	√
4.	Malware			√			√			√			
5.	Extensions of working hours					√					√		
6.	Losing control in managing information and data			√		√							
7.	Lack of policies				√	√							
8.	Cost											√	
9.	Work family conflict												√
10.	Technology burden												√
11.	Work product created on personal device						√						
12.	Access and permissions						√						

BIL	SOURCE	1. [22]	2. [5]	3. [4]	4. [23]	5. [24]	6. [25]	7. [26]	8. [27]	9. [6]	10. [11]	11. [28]	12. [20]
13.	Insecure Connections						√						

Table 2: List of Benefits BYOD via Frequency

BYOD Benefits	Number of cited	Source
Increased productivity	7/12	[22], [5], [4], [23], [24], [26], [6]
Employee satisfaction	5/12	[22], [5], [23], [24], [25]
Lower corporate IT costs	5/12	[4], [23], [25], [26], [6]
Job flexibility	5/12	[24], [26], [6], [11], [20]
Increased mobility	4/12	[4], [25], [26], [11]
Innovation benefits	1/12	[22]
Enjoyment	1/12	[20]
Enhanced job collaboration	1/12	[24]
Employees efficient	1/12	[25]
Convenient, user friendly	1/12	[6]
Technology empowerment	1/12	[20]
Accessibility to data	1/12	[5]
Technology familiarity, agility	1/12	[26]
Time savings	1/12	[6]
Monitoring of system can be done remotely	1/12	[6]
Performance enhancement	1/12	[24]

5.1. Security

The perceived security risk is defined as individuals' evaluation of the security risk that may be caused by violation of security policies and rules [41]. BYOD increases the risk of data security breaches as it is difficult to monitor due to its mobility. For instance, when employees leave the organisation, they do not have to return their own devices. Therefore, organisational applications and others are still accessible on their devices. This can lead to the intrusion of some confidential company data. In addition, advanced features of smart devices, such as high-definition cameras, recording functions, and large data storage capacity, can avoid many traditional IT security measures [11], [42]. For instance, during attending meetings or using them outside of work, the possibility of employees accidentally exposing their devices and the sensitive information to malicious attacks becomes serious risks [42] [28]. Thus, organisations that operate in regulated environments can ensure the security of privately owned devices with solutions to be available in a corporate environment.

5.2. Lost and Stolen Data and Devices

Loss of data due to devices being lost or stolen at work or outside the workplace is one of the most crucial risks associated with BYOD [5]. Most mobile devices are small in size, easy to carry everywhere and are easy to use and have the risk of being misplaced or dropped very high. According to IDC Research, more than 3 million mobile devices were stolen in 2013, and 44% of devices were left in a public area [43]. The implication when devices are lost or stolen is that sensitive organisation data can fall into the hands of a stranger. Besides that, in the US every 3.5 seconds mobile phone was lost [44]. Although a lost mobile phone does not contain confidential data, it might include apps or cached credentials to penetrate an organisation network by criminals [45].

Additionally, according to the study by Osterman Research [46] which is a UK-based study found that negligence from employees who sell their equipment to acquire new ones without clearing the information available on each device causes confidential and sensitive information to be exposed to unauthorized users. Therefore, there are needs to have a clear policy for employees and organisations to handle a loss of mobile device and data loss.

Table 3: List of Challenges BYOD via Frequency

BYOD Challenges	Number of cited	Source
Security	5/12	[26], [27], [6], [28], [20]
Lost and stolen data and device	4/12	[5], [4], [25], [6]
Data privacy violation	4/12	[6], [11], [28], [20]
Malware	3/12	[4], [25], [6]
Extensions of working hours	2/12	[24], [11]
Losing control in managing information and data	2/12	[4], [24]
Lack of policies	2/12	[23], [24]
Cost	1/12	[28]
Work family conflict	1/12	[20]
Technology burden	1/12	[20]
Work product created on personal device	1/12	[25]
Access and permissions	1/12	[25]
Insecure Connections	1/12	[25]

5.3. Data Privacy Violation

Weeger, Wang, and Gewald [47] define privacy risk as to what extent individuals, who use BYOD can compromise with their personal lives. In the context of BYOD, Miller et al. [2] found that privacy issues were considered more important than security issues. The research study by Chountalas & Karagiorgos [11] also found that the data privacy infringement is a threat to employees who are difficult to use BYOD. This is because employees use their own device to work, where the device contains personal data and employers' data. Employees are worried about organisations that implement control their devices such as monitoring the use of personal data and can wipe out their personal data if their device is lost or stolen [20].

Therefore, the privacy data infringement issue is becoming more critical to employees than employers as they are more likely to lose in terms of equipment as well as personal data which do not have the backup data.

5.4. Malware

Among the risks and challenges of using mobile devices is malware attacks [4]. Malware is specifically designed to disrupt, damage, or gain authorized access to a computer system. There has been a parallel growth in malicious software with the growth of the mobile device market specifically targeting those devices as a targeted. Viruses and worms intended to access confidential data from various mobile platforms are always being developed. According to the report by Shumate and Ketel [25], in 2011, there was 155% increase in malicious software targeted towards mobile devices and particularly true for Android devices, which comprise approximately by 51 % of all of the smartphones in the United States. Additionally, most of the mobile devices are exposed to these security challenges by unknowing users. Some organisations will certainly fail to manage with such challenges especially for a small-scale organisation due to budget constraints to manage all the types of mobile devices [27]. Therefore, organisations need to study, access and evaluate before mindlessly embracing the practice.

6. Discussion

This study was explored the various of benefits and challenges of BYOD and identified the benefits and challenges are related. By reviewing twelve (12) literature, sixteen (16) benefits and thirteen (13) challenges are extracted. However, only five (5) benefits and four (4) challenges are identified by measuring the frequency of constructs appearing in the literature.

The results from the literature reveal that increased productivity, employee satisfaction, lower IT costs, job flexibility and increased mobility are the mostly benefits of BYOD. Meanwhile, the issue of security, lost and stolen data and devices, data privacy violation and malware are the mostly challenges of BYOD. Thus, the benefits and challenges of BYOD will be tested to examine in MPS.

7. Conclusion

Understanding the benefits and being aware of the challenges of BYOD is crucial for organisations considering BYOD at workplace. This paper discussed the benefits and challenges of BYOD that were found in previous studies. The selected benefits and challenges will be empirically tested in MPS.

To strengthen a secure cyber environment in the organisation, these benefits and challenges will help organisations in developing a more comprehensive BYOD usage policy. From these findings, organisations can focus on key benefits and challenges to be considered when developing the policy. Therefore, the comprehensive BYOD's use policy for a public sector will be created as a guide and will be enforced to the MPS.

Acknowledgement

I would like to thank the Public Service Department of Malaysia who sponsored me for studying and completing my research.

References

[1] CIO Council, "Bring Your Own Device - A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs," 2012.

[2] K. W. Miller, J. Voas, and G. F. Hurlburt, "BYOD: Security and privacy considerations," *IT Professional*, vol. 14, no. 5, pp. 53–55, 2012.

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

[4] Z. Mitrovic, I. Veljkovic, G. Whyte, and K. Thompson, "Introducing BYOD in an organisation: the risk and customer services view points," in *The 1st Namibia Customer Service Awards & Conference*, 2014, pp. 1–26.

[5] A. Pillay, E. Nham, G. Tan, H. Diaki, S. Senanayake, and S. Deshpande, "Does BYOD increase risks or drive benefits?," *Dtl.Unimelb.Edu.Au*, pp. 1–8, 2013.

[6] U. M. Yabubu, "Cloud Computing and BYOD : Benefits and challenges in Modern Healthcare," no. November 2013, p. 24, 2014.

[7] I. Cook, "BYOD - Research Finding Released," *OVUM*, 2012. [Online]. Available: http://cxounplugged.com/2012/11/ovum_byod_research-findings-released/. [Accessed: 23-Aug-2018].

[8] Ovum, "BYOD: an emerging market trend in more ways than one," *Logicalis white paper*, 2012. [Online]. Available: http://www.us.logicalis.com/globalassets/united-states/whitepapers/logicalisbyodwhitepaperovum.pdf. [Accessed: 22-Aug-2018].

[9] R. Afreen, "Bring Your Own Device (BYOD) in Higher Education: Opportunities and Challenges," *Int. J. Emerg. Trends Technol. Comput. Sci.*, vol. 3, no. 1, pp. 233–236, 2014.

[10] G. Cheng, Y. Guan, and J. Chau, "An Empirical Study towards Understanding User Acceptance of BYOD in Higher Education," *Australas. J. Educ. Technol.*, vol. 32, no. 4, pp. 1–17, 2016.

[11] P. Chountalas and A. Karagiorgos, "Bring your own device philosophy from the user's perspective: an empirical investigation," in *Proceedings of the 2nd HOBA International Conference*, 2015, vol. 1, pp. 1–12.

[12] N. Fani, R. von Solms, and M. Gerber, "A framework towards governing 'Bring Your Own Device in SMMEs,'" in *2016 Information Security for South Africa (ISSA)*, 2016, pp. 1–8.

[13] K. C. Janssen and S. Phillipson, "Are we ready for BYOD?: An analysis of the implementation and communication of BYOD programs in Victorian schools," *Aust. Educ. Comput.*, vol. 30, no. 2, 2015.

[14] F. Onyechere Ugochukwu and M. Z. Ismail, "The Future of BYOD in Organizations and Higher Institution of Learning," *Int. Journals Accounting, Bus. Manag.*, vol. 1, no. 1, pp. 1–5, 2015.

[15] V. Jayaseelan, N. Ganthan, M. Nurazean, M. Norziha, S. Bharanidharan, and M. Pritheega, "Adopting Factors of Bring Your Own Device (BYOD) at the Selected Private Higher Learning Institution in Malaysia," *J. Adv. Res. Soc. Behav. Sci. ISSN*, vol. 2, no. 1, pp. 24–32, 2016.

[16] M. A. Majid and Z. Mansor, "Pelaksanaan BYOD di Organisasi: Pemerhatian ke atas Penguatkuasaan Polisi BYOD," in *3th International Conference on Information Technology & Society*, 2017.

[17] A. Hamza and M. F. Noordin, "BYOD usage by postgraduate students of International Islamic University Malaysia: An analysis," *Int. J. Eng. Sci. Invent.*, vol. 2, no. 4, pp. 14–20, 2013.

[18] statcounter, "Desktop vs Mobile vs Tablet Market Share Worldwide," *statcounter*, 2018. [Online]. Available: http://gs.statcounter.com/platform-market-share/desktop-mobile-tablet/malaysia/#monthly-201705-201804. [Accessed: 23-Aug-2018].

[19] MAMPU, "Pelan Strategik Sektor Awam 2016-2020," 2016.

[20] L. Zhang, M. Mouritsen, and J. Miller, "Role Of Perceived Value In Acceptance Of Bring Your Own Device (BYOD) Policy," *J. Organ. End User Comput.*, 2017.

[21] P. Fiorenza, "Exploring Bring Your Own Device In The Public Sector," 2013. [Online]. Available: https://www.td.org/insights/exploring-bring-your-own-device-in-the-public-sector. [Accessed: 30-Mar-2018].

[22] J. Harris, B. Ives, and I. Junglas, "IT Consumerization: When Gadgets Turn into Entreprise IT Tools," *MIS Q. Exec.*, vol. 11, no. 3, pp. 99–112, 2012.

[23] S. Kabanda and I. Brown, "Bring-Your-Own-Device (BYOD) practices in SMEs in Developing Countries – The Case of Tanzania," in *25th Australasian Conference on Information Systems (ACIS 2014)*, 2014, pp. 1–9.

[24] V. Omwenga and H. Mwenemeru, "Towards the adoption of bring your own device concept in an organization," *Int. J. Soc. Sci. Entrep.*, vol. 1, no. 11, 2014.

[25] T. Shumate and M. Ketel, "Bring Your Own Device: Benefits, risks and control techniques," in *IEEE SOUTHEASTCON 2014*, 2014, pp. 1–6.

[26] M. Gali, V. Barayuga, and W. Yu, "BYOD: Connectivity Option for Alaminos City Hall," in *International Conference on challenges in IT, Engineering and Technology (ICCIET'2014)*, 2014.

[27] K. Madzima, M. Moyo, and H. Abdullah, "Is bring your own device an institutional information security risk for small-scale business organisations?," in *2014 Information Security for South Africa - Proceedings of the ISSA 2014 Conference*, 2014, pp. 1–8.

[28] A. Gustav, "BYOD adoption concerns in the South African financial institution sector," in *International Conference on Information Resources Management(CONF_IRM) 2016*, 2016, pp. 59.

[29] Bell Techlogix, "The real benefits of BYOD," 2012.

[30] D. Bakotić, "Relationship between job satisfaction and organisational performance," *Econ. Res. Istraživanja*, vol. 29, no. 1,

pp. 118–130, Jan. 2016.

[31] F. Herzberg, B. Mausner, and B. B. Synderman, *The motivation to work*. New York, USA: John Wiley & Sons, Inc, 1959.

[32] J. R. Hackman and G. R. Oldham, “Motivation through the design of work: test of a theory,” *Organ. Behav. Hum. Perform.*, vol. 16, no. 2, pp. 250–279, Aug. 1976.

[33] A. M. French, M. Schmidt, C. Guo, and J. P. Shim, “An Exploratory Study on BYOD in Class: Opportunities and Concerns,” in *Twenty-first Americas Conference on Information Systems, Puerto Rico*, 2015.

[34] X. CCMI, “Research Shows Enterprises Continue to Control Employees’ Mobile Device Choice,” *Business Wire*, 2012. [Online]. Available: https://www.businesswire.com/news/home/20120717005172/en/Research-Shows-Enterprises-Continue-Control-Employees’-Mobile. [Accessed: 25-Jun-2018].

[35] P. K. Gajar, A. Ghosh, and S. Rai, “Bring Your Own Device (Byod): Security Risks and Mitigating Strategies,” *J. Glob. Res. Comput. Sci.*, vol. 4, no. 4, pp. 62–70, 2013.

[36] E. O. Yeboah-Boateng and F. E. Boaten, “Bring-Your-Own-Device (BYOD): An Evaluation of Associated Risks to Corporate Information Security,” *Int. J. IT Eng.*, vol. 04, no. 08, pp. 12–30, 2016.

[37] G. Hinks, “Join the mobile revolution,” *Financ. Manag.*, vol. 14, no. 7, pp. 30–32, 2012.

[38] G. Abowd, C. Atkeson, J. Hong, S. Long, R. Kooper, and M. Pinkerton, “Cyberguide: A mobile context aware tour guide,” *Wirel. Networks*, vol. 3, no. 5, pp. 421–433, 1997.

[39] H. van Der Heijden and P. Valiente, “The value of mobility for Business process performance: Evidence from Sweden and The Netherlands,” in *ECIS*, 2002, no. 2002, pp. 1144–1153.

[40] F. Putri and A. Hovav, “Employees’ Compliance with BYOD Security Policy: Insights from Reactance, Organizational Justice, and Protection Motivation Theory,” *ECIS*, pp. 1–17, 2014.

[41] K. H. Guo, Y. Yuan, N. P. Archer, and C. E. Connelly, “Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model,” *J. Manag. Inf. Syst.*, vol. 28, no. 2, pp. 203–236, Oct. 2011.

[42] Cognizant, “Making BYOD Work for Your Organization,” *Futur. Work*, pp. 1–16, 2012.

[43] B. Giorgio, “What Is BYOD? Challenges and Opportunities,” 2014. [Online]. Available: https://www.parallels.com/blogs/ras/what-is-byod/. [Accessed: 09-Jul-2018].

[44] Quentin Fottrell, “Lost Phones Cost Americans $30 Billion a Year,” *Market Watch*, 2012. [Online]. Available: http://blogs.marketwatch.com/paydirt/2012/03/23/lost-phones-cost-americans-30-billion-a-year/. [Accessed: 22-Jul-2018].

[45] H. Romer, “Best practices for BYOD security,” *Comput. Fraud Secur.*, vol. 2014, no. 1, pp. 13–15, Jan. 2014.

[46] Osterman Research, “Putting IT back in control of BYOD,” *White Pap.*, no. June, pp. 1–10, 2012.

[47] A. Weeger, X. Wang, and H. Gewald, “IT Consumerization: BYOD-Program Acceptance and its Impact on Employer Attractiveness,” *J. Comput. Inf. Syst.*, vol. 56, no. 1, pp. 1–10, 2015.