Penerbit Akademia Baru

Journal of Advanced Research in Social and Behavioural Sciences
ISSN (online): 2462-1951 | Vol. 2, No. 1. Pages 24-32, 2016

Adopting Factors of Bring Your Own Device (BYOD) at the Selected Private Higher Learning Institution in Malaysia

J. Vejayon[1,a], *G. N. Samy*[*,1,b], *N. Maarop*[1,c], *N. Megat*[1,d], *B. Shanmugam*[2,e] *and P. Magalingam*[1,f]

[1]Advanced Informatics School, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia
[2]Charles Darwin University, Ellengowan Drive, Casuarina Campus, Australia
[a]*jayaseelan.vejayon@qiup.edu.my*, [*,b]*ganthan.kl@utm.my*, [c]*nurazean.kl@utm.my*, [d]*norziha.kl@utm.my*,
[e]*Bharanidharan.Shanmugam@cdu.edu.au*, [f]*mpritheega.kl@utm.my*

Abstract – *Bring Your Own Device (BYOD) is a term used for the new trend where employees bring personally-owned mobile devices into their workplace. This new trend is witnessed by the organizations to bring several advantages, including competitive advantage, reduction of cost, higher employee productivity and flexibility. The concerns or issues should be addressed so that the benefits of this trend can be achieved. Higher learning institutions are seen as organizations that have to adopt this trend as the new generation of students is computer-literate and technically-savvy. The objectives of this study are to identify factors those influence the adoption of BYOD and to identify the factors thus contribute to the success of BYOD in a selected higher learning institution in Malaysia. The factors are Security, Infrastructure, Cost, Policy, Privacy, Education and Applications. Surveys were conducted at the institution to gather data from students and staffs. The total number of 67 staffs and 202 students responded to the questionnaires. The collected data was then analysed to identify the factors that are deemed to have relevance and influence in the adoption of BYOD at the selected private higher learning institution. The results of the analysis show that there is a high percentage of mobile device ownership among staffs and students at the institution, and there are concerns identified relating to all the seven factors mentioned.*

Keywords: Bring Your Own Device (BYOD), Security, infrastructure, Cost, Policy, Privacy, Education, Applications, Private higher learning institution

1.0 INTRODUCTION

Garba et al [1] reported that the companies such as Gartner and Hewlett-Packard projected that, by 2015, approximately 4.5 billion personally owned mobile devices will be on the network. Along with this, the trend of Bring Your Own Device (BYOD) is also becoming more popular as smartphones and tablets are making their ways into the organizations. BYOD allows employees to use their own mobile devices to access the organization's network information systems [1].

According to [2] teachers utilizing BYOD in their classes may have better opportunity of enhancing student learning experience in their classes. Majority of teenage students own smartphones or other technologies which allow them to access the Internet via the means of wireless communication. Enhancing learning through technology and using social media for educational purposes are looked at as important factor in enhancing students' knowledge, creativity, collaboration and innovation. The skills they acquire here will also be taken to their future jobs [2].

The trend of BYOD is taking place in many organizations, regardless whether there is official approved implementation or not. In higher education institutions, BYOD is a trend that should be welcome because it will allow for wider utilization of the available information systems while also giving the flexibility to the users to use their own preferred devices. With the advances in information and communications technologies, we now have convenience devices with high computing power. However, there are factors and concerns that must be addressed in ensuring that the implementation of BYOD trend in higher learning institutions to become successful. Among the greatest challenges IT leaders identified in Educause Center for Applied Research (ECAR) interviews and focus groups were issues that pertained to faculty and staff use of their own devices for work-related purposes [3]. Those factors, concerns and issues need to be identified and addressed in order for adopting BYOD.

2.0 RELATED WORKS

Singh describes Bring Your Own Device as "a recent trend that has been observed where employees bring personally-owned mobile devices to their workplace to access company resources such as email, file servers, databases as well as their personal data" [4][1]. Bring Your Own Device (BYOD) is the term used for the trend where consumer devices are brought into the workplace. The concept of Bring Your Own Device is gaining momentum at the workplace. "BYOD" means the same with "consumerization", and therefore both the terms will be used interchangeably in this document. According to [5], the term BYOD is also being supplanted with BYOT (Bring Your Own Technology), which more broadly includes both hardware and software [5].

The studies conducted show that there are a number of factors discussed regularly in literature review. The categories highly mentioned in the literature review have been listed below:

[1] **Security** – matters about security concerns caused by BYOD. Examples are like security threats, security attacks and security solutions.

[2] **Infrastructure** – matters about requirements for improving the present infrastructure to support BYOD.

[3] **Cost** – matters about cost implications or cost-effectiveness if BYOD is enabled.

[4] **Policy** – matters about BYOD policies to include/implement.

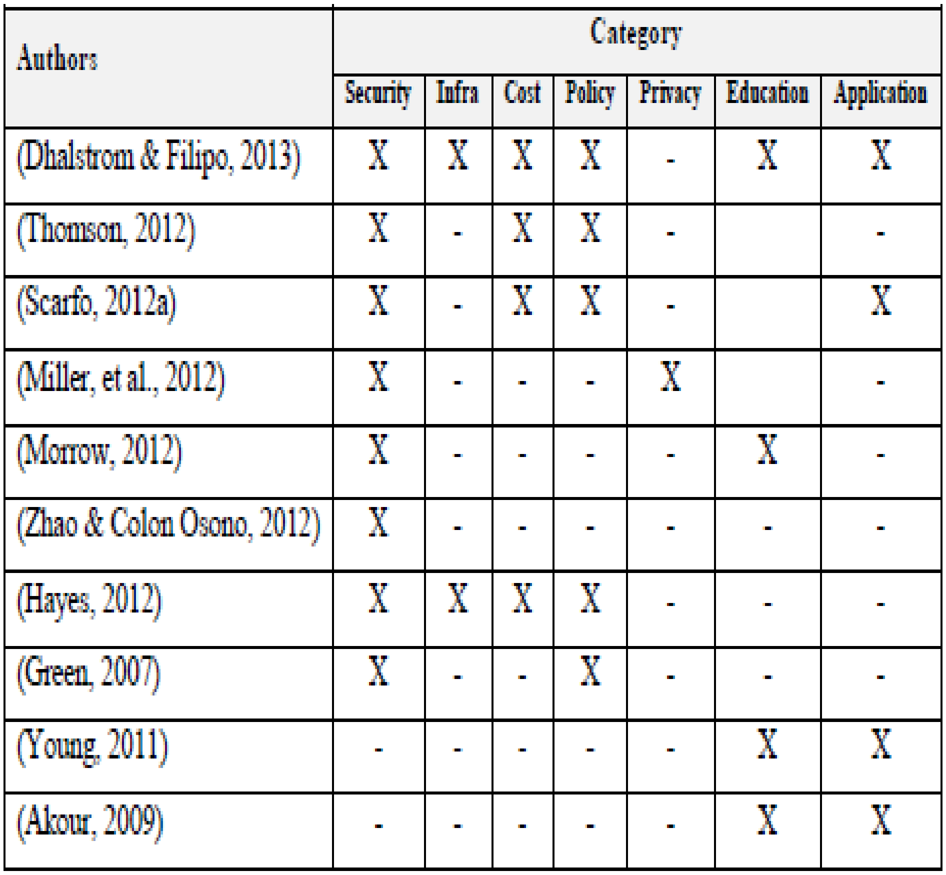
[5] **Privacy** – matters about individual privacy considerations if the devices are to be managed by the organizations.

[6] **Education** – matters about educating users about BYOD policies, security and awareness.

[7] **Applications** – this category discusses about the applications and types of applications (web-based/desktop-based) and how to access them with BYOD.

Literature review has been conducted to identify the categories of factors with regards to BYOD. The factors, issues and concerns identified in the literature review have been grouped into categories based on their relevance. Table 1 gives a summary on the categories mentioned in the literatures [3, 5-13].

Table 1: Categories of factors to consider in BYOD implementation



Authors	Category						
	Security	Infra	Cost	Policy	Privacy	Education	Application
(Dhalstrom & Filipo, 2013)	X	X	X	X	-	X	X
(Thomson, 2012)	X	-	X	X	-		-
(Scarfo, 2012a)	X	-	X	X	-		X
(Miller, et al., 2012)	X	-	-	-	X		-
(Morrow, 2012)	X	-	-	-	-	X	-
(Zhao & Colon Osono, 2012)	X	-	-	-	-	-	-
(Hayes, 2012)	X	X	X	X	-	-	-
(Green, 2007)	X	-	-	X	-	-	-
(Young, 2011)	-	-	-	-	-	X	X
(Akour, 2009)	-	-	-	-	-	X	X

3.0 RESEARCH METHODOLOGY

This study is conducted using quantitative research methodology. Quantitative research requires that one either simply study the counts of events/people/things or that numeric labels be created for meaningful events, experiences and actions.Survey questionnaires were used as the methodology for this research. The questionnaires were developed based on the literature reviews conducted and guided by the questionnaires that have been developed earlier by ECAR.

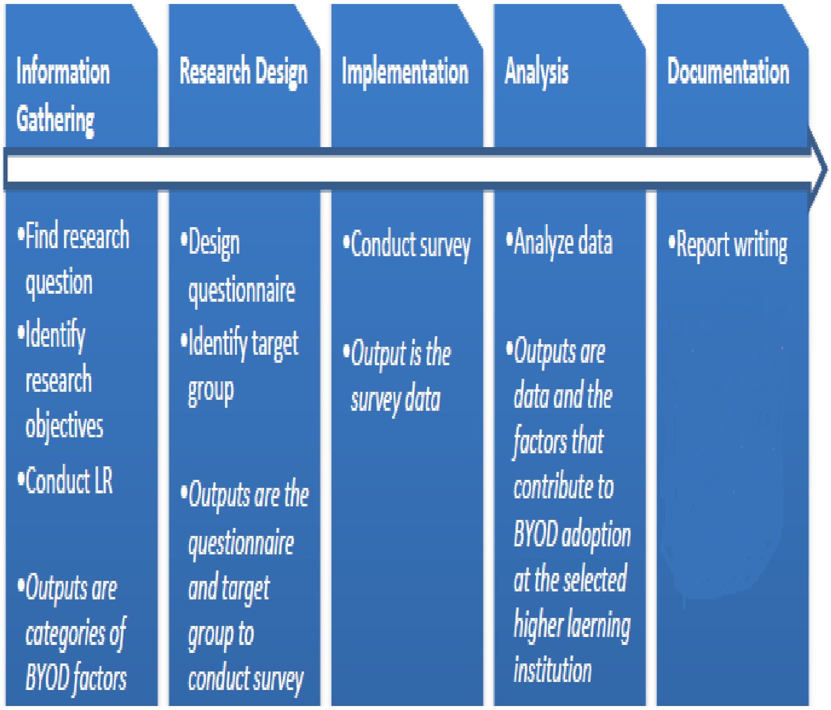

Information Gathering
Research Design
Implementation
Analysis
Documentation
•Find research question
•Identify research objectives
•Conduct LR
•Outputs are categories of BYOD factors
•Design questionnaire
•Identify target group
•Outputs are the questionnaire and target group to conduct survey
•Conduct survey
•Output is the survey data
•Analyze data
•Outputs are data and the factors that contribute to BYOD adoption at the selected higher laerning institution
•Report writing

Figure 1: Research Procedure

The research procedure is shown in Figure 1 above was used as the guide for the overall research. The research project was divided into 5 phases; Information Gathering Phase, Research Design Phase, Implementation Phase, Analysis Phase and Documentation Phase. The sections that follow describe each of the phases and the activities that were carried out.

3.1 Information Gathering Phase

The purpose of this phase was to identify the factors that are critical for the success of adopting BYOD at the selected higher learning institution. Information gathering included the understanding of previous researches that are related to BYOD factors. Sources of this information were from literature review and came from journals, textbooks, reports, and media electronics. This phase has set the scope determination and the direction of this study.

3.2 Research Design Phase

In this phase, 'how the research is to be conducted' has been outlined. In the first section of this phase, literature review was carried out and the factors that deemed important in BYOD have been identified. In the following section, the target groups have been recognized for the conduct of the survey.

3.3 Implementation Phase

In this phase, the questionnaire has been distributed to the identified groups at the selected higher learning institution. Data collection is done during this phase. There are two general groups that the questionnaires have been distributed to; the staffs and students. Outcome from the survey are the raw data collected which have been analysed in the following phase.

3.4 Analysis Phase

During the analysis phase, the raw data collected has been analysed using IBM SPSS Statistics 17.0. The tools were used to interpret the raw data and translate it into descriptive information. The tool was used to provide statistical information and the results are then presented in tables, charts and graphs. The outputs of these analyses are then documented.

3.5 Documentation Phase

The final phase is the documentation of all the phases. The product of this phase is a complete report for the preparation which can be used in the preparation of a guideline in adopting BYOD at the selected higher learning institution as a future research.

4.0 RESULTS AND DISCUSSION

One higher learning institution has been approached and approval obtained to conduct this survey. The survey is conducted where the target is a higher learning institution community members namely staffs and students. The target was divided into two groups as to cover the overall community of the institutions. Different sets of questionnaires were distributed to the groups. A total of 150 staffs and more than 700 students were approached to answer the questionnaires prepared. Emails were sent requesting for them to answer the online questionnaire forms. Out of the total numbers, 67 staffs and 202 students responded to the questionnaires.

4.1 Factors and Concerns in BYOD Adoption in the Selected Higher Learning Institution

The analyses of the studies identified that all the factors and concerns have significant contributions in BYOD adoption at this selected private learning institution.

4.1.1 Security

Staffs were questioned on the security measures available in the institution in preventing data loss, securing the devices and on securing the data. The result clearly indicates that staffs are not sure and answered ‘Don’t know’ whether the measures are available. For ‘Preventing Data Loss’ and ‘Securing Device’, staff responded ‘Don’t know’ with the percentages of 82% and 61%, respectively. However, they are aware that some measures have been put in place in securing data.

For BYOD to be successful, it is important that security measures are put in place accordingly. Therefore, the institution needs to make the right security controls and measurements put in place. Users of the institution are also to be made aware so that they comply with the security policies. The response from staffs is quite alarming when questioned whether they have antivirus installed on their mobile devices. 97% of the staffs indicated that they do download and install free mobile applications but only about 31% know and have installed antivirus on their smartphones. This shows that there is a need for the staff to be made aware on the importance of antivirus on their mobile devices. It is also important that they download and install freely available applications with caution. Staffs have responded very positively on locking their smartphones with screen lock/pin. This is the first layer of defense for a smartphone. About 76% of the staffs say that they protect their smartphones with screen lock/pin.

4.1.2 Infrastructure

Infrastructure to support BYOD at this institution is deemed to be sufficient as staffs find that they do not find difficulties in connecting their devices to Wi-Fi and the bandwidth of Internet access is sufficient. Staffs do however think that there will be a need to improve the infrastructure in the very near future to cater for more user-provisioned devices.

4.1.3 Cost

The responses from staffs show that they strongly believe that the institution can save cost by reducing the number of general-purposed computers provided. On the other hand, increase of cost is expected on infrastructure to support the widespread use of BYOD devices in the institution. For instance, staff were asked on their opinion whether the institution should plan to substantially reduce the number of general-purpose computers and provide better infrastructure for BYOD devices. The responses have been very positive that staffs feel the number of general-purpose computers should be reduced. 63% of the staffs 'Agree' and 28% 'Strongly Agree' that the institution should plan to reduce general purpose computers substantially.

4.1.4 Policy

Questions were asked on the policies available with regards to the use of their own devices at the institution. Based on staffs' responses, it was found that there are no formal policies for devices and applications that can run on the devices. More than 50% staffs have responded that there are no formal policies for 'Permitted Devices' and 'Permitted Apps'. Only about 22%-24% think that there are policies for the two items mentioned. It is therefore important that the institution looks into preparing policies to clearly guide the users on their use of personally-owned devices for the institution's work or while they use the institution's resources i.e the institution's network resources.

It is important to create supporting policies for security, privacy, confidentiality, and information sharing. By having proper policies in place, both students and staff of the institution will have clear guidance on what the 'Dos' and 'Don'ts' when they use the institutions IT assets, including information and infrastructure. The means of having agreements, i.e Data Use Agreements can be used to support the policies on data access by users.

4.1.5 Privacy

Trust is a vital element in making a successful BYOD program. However, most employees do not trust their employers with personal data. This is defined as 'Trust Gap' by Mobileiron and this causes user dissatisfaction and lack of support for IT initiatives. This has caused organizations difficulties to develop proper set of practical guidelines to address mobile privacy effectively. According to staffs' responded, 78% of them said they are concerned about their personal data privacy. This is highly significant. Only about 16% said they do not keep sensitive data on their phone and they are not so worried about their data privacy. moreover, based on the findings, it is notable that staffs are quite concerned on the personal data privacy on their mobile devices. This would need for proper policies put in place if mobile device management (MDM) software is to be installed on their devices. MDM has the capacity to remotely wipe and read the information on the mobile devices. Trainings and exposure to the monitoring software can be given to gain better confidence from the staffs.

4.1.6 Education

Students' responses were collected to find the relevance of this factor to BYOD implementation at the institution. 'Some' and 'Most' of their instructors effectively use technology, have adequate technical skills and provide the students with adequate training for the technology used in courses. BYOD is a phenomenon. In order to garner the benefits of BYOD, the right technologies and applications are needed. Those technologies and applications are then should be properly transferred to the instructors and students, via proper trainings. Analyses on staffs' need on training shows that staffs have recommended highly that they need trainings on the online productivity tools, digital library, security programs and ICT policies. These are only some of the areas covered under the trainings. However, staffs find that all these areas are important and that they need to be trained.

Based on the analyses conducted among staffs on the training needs, it was found that staffs have recommended highly that they need trainings on the online productivity tools, digital library, security programs and ICT policies. For productivity tools, 64.2% indicated that training is either "Very important" or "Extremely important". For the same responses, 79.1% of staffs indicated they need training for Digital Library, 47.7% of staffs indicated they need training for the institution's security programs and a high percentage of 83.6% indicated they need training on ICT policies.

4.1.7 Applications

The findings implicate that applications should be platform-free as students and staffs hold different types of devices with different operating systems. For example, the operating systems of the devices vary based on the devices used. 176 students out of 181 responded that they use laptop installed with Windows operating system. This is 93% of the total. 133 students responded that they use tablets, with 33% selecting iOS, 36% selecting Android, 12% selecting Windows and 16% indicated they do not know the OS used on their tablets. 181 students responded on the OS used on their smartphones where the breakdown is Android phone (69%), iPhone (13%), Windows phone (1%), BlackBerry (2%), other smartphones (7%) and 8% indicated they do not know the OS running on their phone.

Besides that, the findings also clearly indicates that Android devices (smartphone and tablet) have high ownership among students. This is followed by iOS and with a very small percentage by Windows phones (1%) and tablets (12%). As mobile applications are very OS dependent, it is important that development of mobile applications for academic purpose focus more on Android and iOS phones. Furthermore, students have also indicated the many applications that they consider important in their academic success. The applications should also be user-friendly enough to be used from handheld devices. To garner the benefits of BYOD, applications that are useful in teaching and learning should be made available.

5.0 CONCLUSSION

The main contribution of this study is on the identifications of the factors and concerns in adopting BYOD in the selected higher learning institution. Basically, there are none or very limited studies made on the adoption of BYOD at a higher learning institution in Malaysia. This study therefore contributes as a base for future studies on this same area. The study has also made a clear exposure that BYOD is a trend or phenomenon that is happening fast in the institution. High percentage of staffs and students are carrying their personally-owned computing devices such as laptops, tablets, and smart phones to the institution. The institution must look at catering for these devices so that higher satisfaction of users is achieved for better teaching and learning experiences.

Furthermore, the categories of factors have been identified namely security, infrastructure, policy, privacy, cost, application and education. It was found that all these categories are also relevant for adoption of BYOD at the selected higher learning institution. Moreover, based on the identified factors and concerns, guidelines can be proposed to help the institution to adopt the BYOD trend. As there is no such guidelines been prepared before for a higher learning institution, this study and outcome of the study are expected to contribute in the process of adopting BYOD in a better and informed manner.

REFERENCES

[1] A.B. Garba, J. Armarego, D. Murray, W. Kenworthy, Review of the information security and privacy challenges in bring your own device (BYOD) environments, Journal of Information Privacy and Security 11 (1) (2015) 38-54.

[2] M. Vanwelsenaers, Students using their own technology Device in the classroom: can “BYOD” increase motivation and learning, Master thesis, Northern Michigan University, 2012.

[3] G. Thomson, BYOD: Enabling the chaos, Network Security 2 (2012) 5-8.

[4] M.N. Singh, BYOD genie is out of the bottle - “devil or angel”, Journal of Business Management & Social Sciences Research 1 (3) (2012).

[5] K.W. Miller, J. Voas, G.F. Hurlburt, BYOD: Security and privacy considerations, IT Professional 14 (5) (2012) 53-55.

[6] H. Akour, Determinants of mobile learning acceptance: an empirical investigation in higher education, Master thesis, Oklahoma State University, 2009.

[7] E. Dhalstrom, S.D. Filipo, Consumerization of Information Technology/BYOD, Research Preview, 2013.

[8] A. Green, Management of security policies for mobile devices, Proceedings of the 4th Annual Conference on Information Security Curriculum Development, ACM, Kennesaw, GA, 2007.

[9] J. Hayes, The device divide, Engineering & Technology 7 (9) (2012) 76-78.

[10] B. Morrow, BYOD security challenges: Control and protect your most sensitive data, Network Security 12 (2012) 5-8.

[11] A. Scarfo, New security perspectives around BYOD, Seventh International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA), IEEE, Victoria, BC, 2012, pp. 446-451.

[12] J.R. Young, Top smartphone apps to improve teaching, research, and your life, Education Digest: Essential Readings Condensed for Quick Review 76 (9) (2011) 12-15.

[13] Z. Zhao, F.C.C. Osono, "TrustDroid™": Preventing the use of SmartPhones for information leaking in corporate networks through the used of static analysis taint tracking, 7th International Conference of Malicious and Unwanted Software (MALWARE), IEEE, Fajardo, PR, 2012, pp. 135-143.