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

JAYASEELAN VEJAYON
GANTHAN NARAYANA SAMY
NURAZEAN MAAROP
NORZIHA MEGAT
BHARANIDHARAN SHANMUGAM
PRITHEEGA MAGALINGAM
Advanced Informatics School (AIS),Universiti Teknologi Malaysia
&
Charles Darwin University, Casuarina Campus, Australia

Outline

Abstract

1.0 Introduction

2.0 Related Works

3.0 Research Methodology

4.0 Results And Discussion

5.0 Conclusions

References

Abstract

- ***Bring Your Own Device (BYOD)*** *is a term used for the new trend where employees bring personally-owned mobile devices into their workplace.*
- *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.*

1.0 Introduction

- 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.
- 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.

2.0 Related Works

- 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 “consumerisation”.

2.0 Literature Review (cont'd.)

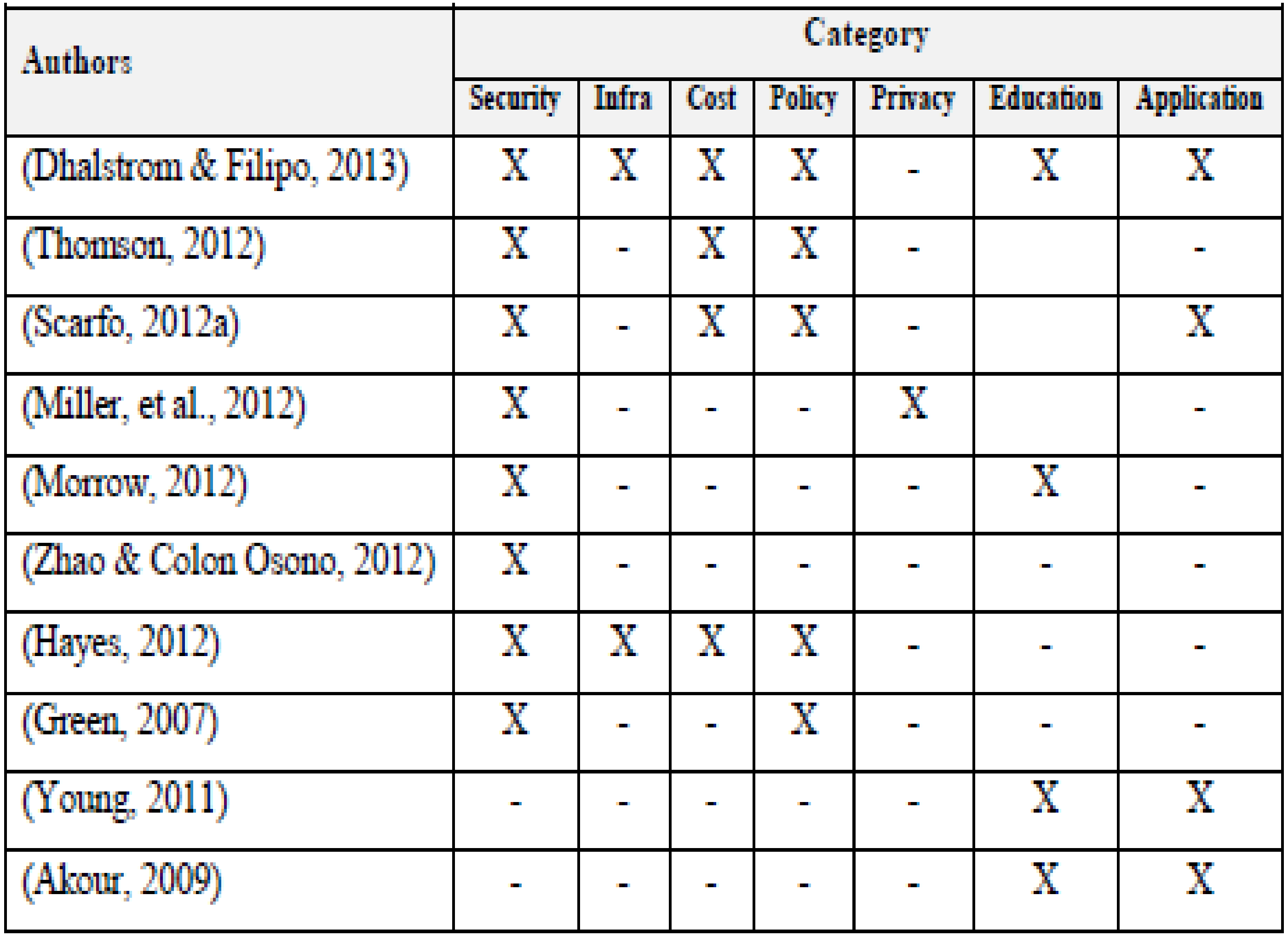
- The studies conducted show that there are a number of factors discussed regularly in literature review. The categories highly mentioned in the literature review have been listed below:
- **Security** – Matters about security concerns caused by BYOD. Examples are like security threats, security attacks and security solutions.
- **Infrastructure** – Matters about requirements for improving the present infrastructure to support BYOD.
- **Cost** – Matters about cost implications or cost-effectiveness if BYOD is enabled.

2.0 Literature Review (cont'd.)

- **Policy** – Matters about BYOD policies to include/implement.
- **Privacy** – Matters about individual privacy considerations if the devices are to be managed by the organizations.
- **Education** – Matters about educating users about BYOD policies, security and awareness.
- **Applications** – This category discusses about the applications and types of applications (web-based/desktop-based) and how to access them with BYOD.
- The factors, issues and concerns identified in the literature review have been grouped into categories based on their relevance in following slide.

2.0 Literature Review (cont’d.)

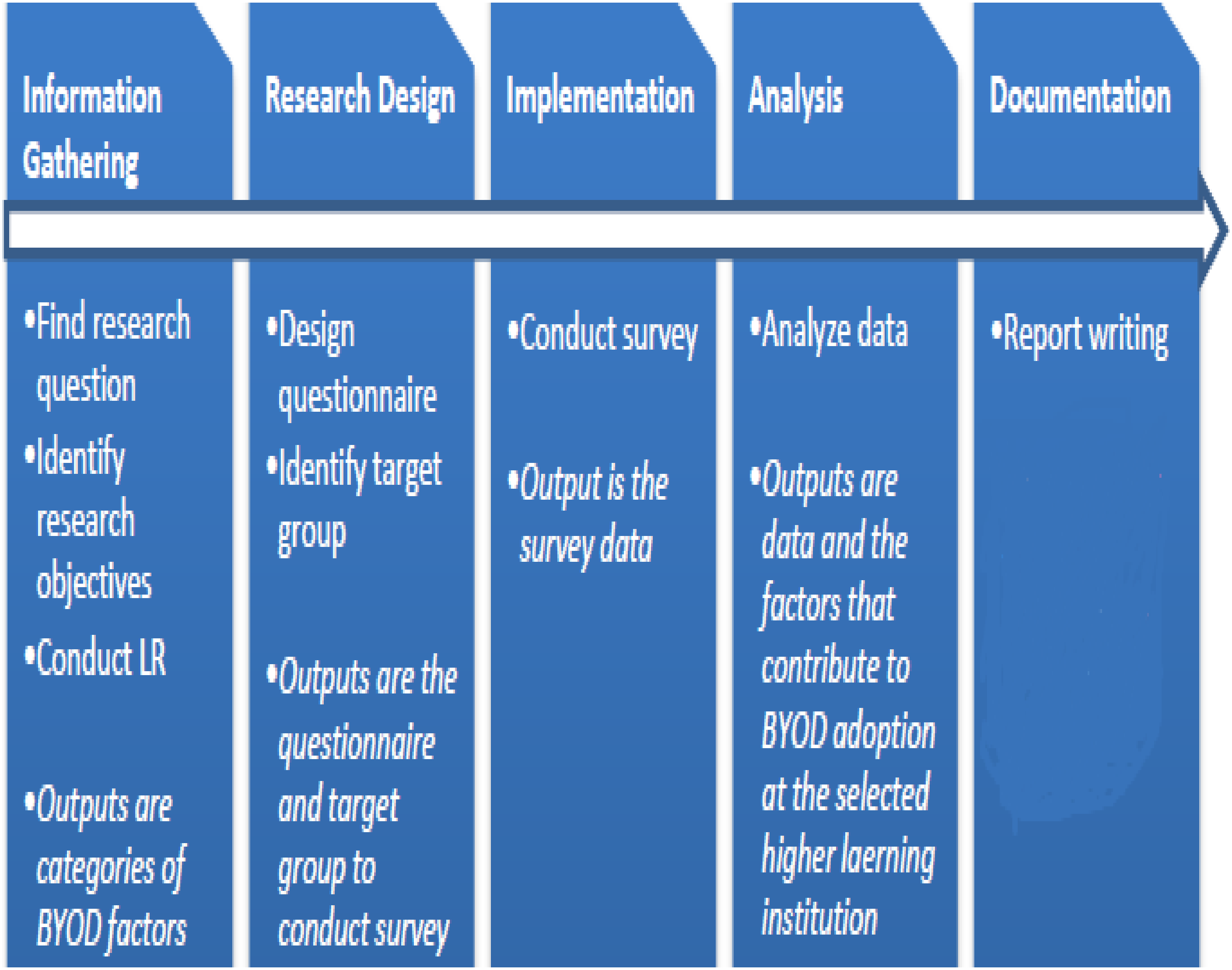
Table 1: Categories of factors to consider in BYOD implementation



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

Figure 1: Research Procedure



Information Gathering

- Find research question
- Identify research objectives
- Conduct LR

- *Outputs are categories of BYOD factors*

Research Design

- Design questionnaire
- Identify target group

- *Outputs are the questionnaire and target group to conduct survey*

Implementation

- Conduct survey

- *Output is the survey data*

Analysis

- Analyze data

- *Outputs are data and the factors that contribute to BYOD adoption at the selected higher laerning institution*

Documentation

- Report writing

4.0 Results And Discussion

- The survey is conducted where the target is a higher learning institution community members namely staffs and students.
- 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.
- Out of the total numbers, 67 staffs and 202 students responded to the questionnaires.

4.1 Factors and Concerns in BYOD

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.

4.1 Factors and Concerns in BYOD (cont’d.)

4.1.1 Security (cont’d.)

- 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 smart phones.
- This shows that there is a need for the staff to be made aware on the importance of antivirus on their mobile devices.
- Staffs have responded very positively on locking their smart phones with screen lock/pin.
- This is the first layer of defense for a smart phone.
- About 76% of the staffs say that they protect their smart phones with screen lock/pin.

4.1 Factors and Concerns in BYOD (cont'd.)

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 Factors and Concerns in BYOD (cont'd.)

4.1.3 Cost

- 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 Factors and Concerns in BYOD (cont’d.)

4.1.4 Policy

- 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’.
- 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.

4.1 Factors and Concerns in BYOD (cont'd.)

4.1.5 Privacy

- 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.
- 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.

4.1 Factors and Concerns in BYOD (cont'd.)

4.1.6 Education

- 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 Factors and Concerns in BYOD (cont'd.)

4.1.7 Applications

- 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.

4.1 Factors and Concerns in BYOD (cont'd.)

4.1.7 Applications (cont'd.)

- 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 smart phones (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%).

4.1 Factors and Concerns in BYOD (cont'd.)

4.1.7 Applications (cont'd.)

- 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.
- The findings implicate that applications should be platform-free as students and staffs hold different types of devices with different operating systems.

5.0 Conclusion

- The main contribution of this study is on the identifications of the factors and concerns in adopting BYOD in the selected higher learning institution.
- 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.
- Based on the identified factors and concerns, guidelines can be proposed to help the institution to adopt the BYOD trend.

REFERENCES

[1] Abubakar Bello Garba, Jocelyn Armarego, David Murray & WilliamKenworthy, 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] Vanwelsenaers, M, Students using their own technology Device in the classroom: can “byod” increase Motivation and learning, 2012.

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

[4] Singh, M. N., BYOD Genie Is Out Of the Bottle–“Devil Or Angel”, Journal of Business Management & Social Sciences Research 1(3) (2012).

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

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

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

[8] Green, A, Management of security policies for mobile devices, Proceedings of the 4th annual conference on information security curriculum development, 2007.

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

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

[11] Scarfo, A, New security perspectives around BYOD, Victoria, BC, (2012a).

[12] Young, J. R., Top Smartphone Apps to Improve Teaching, Research, and Your Life, Education Digest: Essential Readings Condensed for Quick Review 76(9) (2011), 12-15.

[13] Zhao, Z., & Colon Osono, F. C, "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), 2012.

Thank you

Q & A