SUCCESS MODEL FOR BYOD IMPLEMENTATION CONSIDERING HUMAN AND SECURITY PERSPECTIVES IN MALAYSIA GOVERNMENT ENVIRONMENT

HASLINDA BINTI MAT AKHIR

UNIVERSITI TEKNOLOGI MALAYSIA

SUCCESS MODEL FOR BYOD IMPLEMENTATION CONSIDERING HUMAN AND SECURITY PERSPECTIVES IN MALAYSIA GOVERNMENT ENVIRONMENT

HASLINDA BINTI MAT AKHIR

A project report submitted in partial fulfilment of the
requirements for the award of the degree of
Master of Science (Information Assurance)

Advanced Informatics School
Universiti Teknologi Malaysia

JUNE 2017

To my beloved late Mak (mother) and Abah (father).

ACKNOWLEDGEMENT

In successfully producing this thesis, I was provided with the assistance from various individuals, and organisations including academicians, and practitioners. They have contributed concerning my understanding and point of view. In specific, I wish to express my sincere appreciation to my supervisor, Dr. Nurazean Maarop, for supervision, guidance, advice, critics, motivation, and inspiration throughout the whole process of this research. Without her continuous attention and support, this thesis would not have been the same as presented here.

I would like to extend my gratitude to Public Service Department of Malaysia (JPA) for sponsoring my Master's study. Expert Reviewers from UTM, Dr. Jastini Mohd Jamil from Universiti Utara Malaysia (UUM), Dr. Muslihah Wook from Universiti Pertahanan Nasional Malaysia (UPNM), Surya Sumarni Hussein, Faizura Haneem Mohamed Ali, and Wan Azlin Zurita Wan Ahmad from Malaysian Public Sector ICT Experts, and selected Malaysian Government agencies also deserve special thanks for their assistance in giving suggestions and supplying the relevant review of this research in Pilot Study Phase.

My companion postgraduate students should also be acknowledged for their help as well. My sincere appreciation also extends to all my colleagues and others who have provided assistance on several occasions. Their views and tips are useful indeed. Unfortunately, it is not possible to list all of them in this limited space.

I am grateful to all my family members, my husband (Hillmay Md Saad) for always supporting and encouraging me with their best wishes and advice when needed. To end with, I wish to thank everybody for helping me directly or indirectly throughout this project and it is highly appreciated.

ABSTRACT

Currently, the most benefits of BYOD implementation is to provide mobility and flexibility in workplaces with the use of compact mobile devices makes it stress-free to bring it everywhere. Although the concept is easy for the user, it introduces a new threat to the security of information technology. The network will be vulnerable to threats such as data leakage, complex security governance, lack of personal mobile devices control management, and incompetent employees in such technology. In this study, the most significant factors of BYOD implementation success model in Malaysian government environment are investigated by considering security perspective. This proposed model is to assist the government to develop a secure success model for implementing BYOD based on baseline theory models such as DeLone & McLean and other information system effectiveness theories. This study used a mixed-method convergent design by combining qualitative and quantitative approaches. The data collected is through interview sessions with the selected government's employees including the expert team and using questionnaires for verification. The quantitative data gathered has been analysed by computer software named Statistical Package for the Social Sciences. The findings of this study are to pay attention to the security perspective of the BYOD implementation. The proposed success model will valuable to IT leaders and decision makers in implementing the BYOD technology securely and appropriate security controls can be incorporated by government agencies in Malaysia as well as embrace the consumerization of IT trend in the workplace to provide employees with a modest, ubiquitous access capability whether at the office, home or abroad, regardless of their computing devices.

ABSTRAK

Pada masa kini, faedah pelaksanaan BYOD yang ketara adalah menyediakan mobiliti dan fleksibiliti di tempat kerja melalui penggunaan peranti mudah alih padat yang menjadikan peranti tersebut bebas dibawa ke mana-mana sahaja. Walaupun konsep ini mudah untuk pengguna, tetapi ianya memperkenalkan satu ancaman baharu kepada keselamatan teknologi maklumat. Sistem rangkaian terdedah kepada ancaman seperti kebocoran data, tadbir urus keselamatan yang kompleks, kekurangan pengurusan kawalan peranti mudah alih peribadi, dan pekerja yang tidak mahir dalam teknologi seperti ini. Dalam kajian ini, faktor-faktor yang paling penting bagi model kejayaan pelaksanaan BYOD dalam persekitaran kerajaan Malaysia dikenal pasti dengan mengambil kira perspektif keselamatan. Model yang dicadangkan ini adalah untuk membantu kerajaan dalam membangunkan model kejayaan selamat bagi pelaksanaan BYOD berdasarkan model teori asas seperti DeLone & McLean dan lain-lain teori keberkesanan sistem maklumat. Kajian ini menggunakan kaedah reka bentuk penyelidikan campuran serentak dengan menggabungkan pendekatan kualitatif dan pendekatan kuantitatif. Data yang dikumpul adalah melalui sesi temubual dengan pekerja kerajaan terpilih termasuk pasukan pakar dan menggunakan soalselidik untuk pengesahan. Data kuantitatif yang dikumpul dianalisis oleh perisian komputer Pakej Statistik untuk Sains Sosial. Dapatan kajian ini memberi perhatian kepada perspektif keselamatan bagi pelaksanaan BYOD. Model kejayaan yang dicadangkan akan bermanfaat kepada peneraju IT dan pembuat keputusan dalam melaksanakan teknologi BYOD dengan selamat dan kawalan keselamatan yang bersesuaian boleh diaplikasikan oleh agensi-agensi kerajaan di Malaysia serta trend kepenggunaan IT dapat diterima di tempat kerja bagi keupayaan capaian yang menyeluruh kepada pekerja sama ada di pejabat, rumah atau di luar negara, tanpa mengira peranti pengkomputeran mereka.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

API	-	Application Programming Interface
BYOD		Bring Your Own Device
CC	-	Cloud Computing
CGSO	-	Office of the Chief Government Security Officer
CIA	-	Confidentiality, Integrity, Availability
DLP	-	Data Leakage Protection
CSM	-	Cybersecurity Malaysia
GA/PSA	-	Government Agency/Public Sector Agency
InfoSec	-	Information Security
IT/ICT	-	Information and Communications Technology
IS	-	Information System
ISMS	-	Information Security Management System
MAMPU	-	Malaysian Administrative Modernization & Management Planning Unit
MAM	-	Mobile Application Management
MCMC	-	Malaysia Communication and Multimedia Commission
MCMM	-	Ministry of Communications and Multimedia
MDM	-	Mobile Device Management
MIM	-	Mobile Information Management
MyMIS	-	Malaysian Public Sector Management of Information and Communications Technology Security Handbook
SPSS	-	Statistical Package for the Social Sciences
SSL/TLS	-	Secure Socket Layer/Transport Layer Security
VPN	-	Virtual Private Network
Wi-Fi	-	Wireless Fidelity

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

Within a decade ago revealed the increasing of Information and Communication Technology (ICT) usage to change the way services are provided and creates a positive change in the working culture, reduce operating costs as well as increase productivity and quality of service among government employees (Perez-Gonzalez & Daiz-Daiz, 2015; Siang *et al.*, 2012). This situation powered by the introduction of concepts such as Bring Your Own Device (BYOD). BYOD is a concept or a policy where organisations allow employees to bring their personally-owned mobile devices such as smartphones, tablets and/or laptops at work to access corporate data, information and applications (Dhingra, 2016).

The evolving of mobile technology is a major challenge where the phenomenon of BYOD has become a trend in most organisations in many countries including Malaysia (Akin-Adetoro & Kabanda, 2015; Downer & Bhattacharya, 2016; Engan, 2015). According to Gartner (2014) Mobile Device Survey, the evolution of BYOD programs is the single most radical shift in the economics of client computing for business since PCs invaded the workplace and by 2018 more than 50% of users will use a tablet or smartphone first for all online activities (Rivera & Van Der Meulen, 2014). It has been reported by the Malaysian Communications and Multimedia Commission (MCMC), that mobile phone penetration rate per 100 inhabitants was 144.8% for the second quarter of 2015 (MCMC, 2015).

In the Public Sector, BYOD also becomes a major issue of concern that involves of data security elements, especially official information and official secrets information contained in all the mobile devices. BYOD has been commonly implemented by the Malaysian government agencies to provide mobility (work from any location without physical limitations through the use of variety mobile devices to perform official duties), flexibility, increase productivity as well as cost savings to the agencies in line with the new Public Sector Information Security Policy updated by MAMPU in 2015 (Engan, 2015). This is supported by the BYOD Concept Effectiveness Study done to Ministry of Defence in 2013 (MINDEF, 2013), that indicates working was more effective and productive by carrying and using a device such as a smartphone, tablet or laptop at work. These statistics show that mobile devices tend to access information faster through BYOD implementation and give advantages by increasing employee's satisfaction and business productivity enhances collaboration and mobility, expands mobile access to resources and reduce spending on the sourcing support of devices by organisations (Selviandro *et al.*, 2015).

BYOD has been generally adopted and implemented in Malaysian government environment around 2010 since the evolving of mobile technology, whereby all the enforcement of security measures including guidelines establishment is managed centrally by Malaysian Administrative Modernization and Management Planning Unit (MAMPU) together with the government agencies that cover for ICT security respectively such as Office of the Chief Government Security Officer (CGSO), National Security Council (NSC/MKN), and Cybersecurity Malaysia (CSM). Much Electronic Government (EG) applications in Malaysia today can be accessed through mobile devices such as Government Public Key Infrastructure (GPKI), Human Resources Management Information System (HRMIS), myJAKIM, myHealth, myKPDNKK, myTour, and much more, and it is harmonized with the government initiative towards mobile devices services utilized via mobile applications store called Government Applications Store (1GovAppStore) which was introduced later as a Gallery of Malaysian Government Mobile Applications (GAMMA) to encourage mobile devices applications usage for work purposes (MAMPU, 2015b; Sulaiman, 2013).

There are many elements and factors that may influence the effectiveness of the BYOD implementation in the government securely. Downer and Bhattacharya (Downer & Bhattacharya, 2016) have concluded that BYOD has not addressed as security issue requires by the organisation. The characteristics of current BYOD architectures and implementations make them unnecessarily difficult to deploy, or those characteristics render them incapable of delivering values in which alternate approaches can be achieved (Boon, 2016). The deployment of BYOD technology intrinsically implies and enforces a higher assurance environment rather than operational cost consideration.

The basic principles of Information Security (InfoSec) that have to be preserved are the Confidentiality, Integrity, and Availability (CIA) Triad (Matthew, 2014; "The CIA Principle," 2001). InfoSec Management must be in place and ICT systems must be kept in an available, secure and reliable form towards a good security compliance (Reinfelder & Weishaupl, 2016). Due to various issues and threats, we have to bear with the security implications such as information theft and leakage, damage to the system software or hardware, the loss in terms of time and finance, lost confidence in the organization's delivery system and affect the image of the organization (Bann *et al.*, 2015).

1.2 Problem Background

The implementation of BYOD in many organisations including Malaysian government agencies currently still has several issues relates to security threats which have impacted the agency' security towards confidential data for using employees' personal devices (Boon, 2016; Dzazali, 2012; Engan, 2015). It does not have a sufficient level of security which the devices are not originally designed for business and the devices are prone to security holes such as a virus, malware contained in mobile devices and data loss (Selviandro *et al.*, 2015). Through web browser exploitation, phishing, drive-by download, downloaded application, Wi-Fi network interception, BYOD implementation will face a big challenge which contributes to device loss and damage (Boon, 2016; Eslahi *et al.*, 2014).

Based on the Electronic Information Leakage Protection Study in Public Sector done by NSC/MKN in collaboration with MAMPU in the year 2012 (Dzazali, 2012), top medium high potential causes leakages of Malaysian Public Sector information was through mobile devices by BYOD usage implementation concept. There was 8,427 high and medium incidents level were detected involving agencies under Putrajaya Campus Network (PCN) that exposed of classified information such as Official Secrets, tender procurement, the Cabinet paper as well as confidential and restricted materials (Dzazali, 2012). Performing official tasks remotely using private-owned mobile devices to make office work and store official documents have the loopholes that government agencies need to pay attention at. The previous study found that information leakage occurred in BYOD implementation which vulnerability of corporate data and several risks associated with information leakage and exposure to unauthorized parties, threat posed by hackers to data/strategic official information and official secrets contained in the device and lack of awareness about security safeguards of data/information in a mobile device identified (Boon, 2016; Dzazali, 2012; Engan, 2015). The chances of a security breach of sensitive information are high when employees left the organisation, there is an official and strategic information as well as official secrets on the mobile devices that are still accessible (Boon, 2016; Dzazali, 2012; Engan, 2015). User accountability and integrity risks also are the concerns such as exposure and release information to unauthorized parties among users, monitoring user activity in accountability identify users from time to time, users keep the device's confidentiality of the password and attention to a particular official secret information during the creation, processing, storage, transmission, delivery, transfer and destruction of the device (Boon, 2016; French *et al.*, 2014).

By allowing employees to BYOD, Malaysian government agencies are opening a new chapter for security managers and administrators towards complex security management. The security governance framework and corporate security policies will need to be redefined and a great deal of effort will be required to make each policy efficiently operational and streamlined. The infrastructure issues indicate that users have variety of device's speed and OS compatibility, also devices using the organization's network Wi-Fi will create the IT department having difficulty in enforcement and controlling the device as well as device technical

problems contained official information (Eslahi *et al.*, 2014; French *et al.*, 2014). Many of the mobile devices used by employees in the workplace such as Android, iOS, and Windows devices were not designed with full data security features in place (MAMPU, 2015b; Vargas *et al.*, 2012). For example, there is a deficiency in resilient security controls of the Android 2.3 (Gingerbread) Operating System (OS) version, that leaves vulnerable to the organisation and corporate information stored in such devices (Vargas *et al.*, 2012). This can be fragile in the business security which could lead to exploitation in the aspect of data leaks, lost devices, loss of control, malware, employee's privacy, and legal concerns.

As mobile devices are personally owned by employees, they download a range of personal applications into devices involving entertainment, games and much more (Armando *et al.*, 2012). Issues of mobile devices management relate to ownership arise which employee-owned mobile devices while the official data/information is owned by the organisation (Chang *et al.*, 2014; MAMPU, 2013). Currently, some organisations implement device-based control technology policy such as Mobile Device Management (MDM) for strict control types of downloaded applications placed on users' mobile devices (Rhee & Yi, 2015) but challenges continue when allocating such an MDM agent to personal devices to enforce security (MAMPU, 2013).

There is also issues of data privacy concerns and regulatory compliance (Vignesh & Asha, 2015) due to non-existence of a proper policy or unclear/disorganized BYOD Security Policies/Procedures that explains the boundary and restriction when government agencies' employees using personal mobile devices for accessing corporate confidential information and securing areas/places from external and internal intrusions (Boon, 2016; MAMPU, 2013; Morrow, 2012; Wong, 2012). Limited research has been done to encounter security issues that consist of the most major challenge confronting BYOD policy such as corporate data are being delivered to devices that are not managed by the IT department which have security implications for data leakage and information theft (Olalere *et al.*, 2015).

These findings shows that the implementation of BYOD in Malaysian government agencies still has several issues relates to security threats, information leakage, complex security management, mobile devices management (data ownership), and data privacy concerns and regulatory compliance (Boon, 2016; Dzazali, 2012; Engan, 2015; Eslahi *et al.*, 2014; Olalere *et al.*, 2015; Selviandro *et al.*, 2015) which must be taken seriously to find the solution to protect government information.

Up to now, there are several related Malaysian Cyber Laws/Acts/Circulars/ Instructions/Guidelines to put security controls towards InfoSec or Public Sector ICT Security Assurance including BYOD implementation. According to the new Black Book Security Instruction published by the CGSO, the user of mobile computing facilities who is processing official secrets out of the office shall ensure that it is protected against loss and damage as well as the information contained therein is not compromised (Engan, 2015). The user of mobile devices should ensure the implementation of security measures for the physical protection, access control, backup data and protection from attacks by malicious software. Besides, it is stated in the new Public Sector Information Security Policy updated by MAMPU, the features of mobility in organization communication refers to a way of working in which involve of an internal communication infrastructure facilities and external telecommunications; a variety of mobile devices usage; access to information and application system of the organization; and communication enabled across multiple physical locations to perform official duties (Engan, 2015). In the General Circular No. 3, 2000: Government Information and Communications Technology Security Policy Framework (MAMPU, 2000), Malaysian Public Sector ICT Management Security Handbook (MyMIS) 2002 (MAMPU, 2002), and Information Instruction 2007 (MAMPU, 2007), the agencies must provide a security measures against unauthorized access, modification, and repudiation to safeguard the BYOD implementation issues arise. This must also comply to the General Circular No. 2 1987 – Management Official Secrets in Accordance with the Official Secrets Act (Amendment) 1986 ("Official Secrets Act of Malaysia 1972," 2015, "The Malaysian Official Secrets Act 1972," 2004) which described the rules to be observed by government departments and agencies in managing the Official Secrets accordance with the provisions of the Official Secrets Act (Amendment) 1986.

As with all other evolutionary approaches, BYOD comes with its own set of concerns and objections. Even though there have general initiatives done such as Instructions/Guidelines establishment (Dzazali, 2012; Engan, 2015) and implementation of Data Leakage Protection (DLP) (Dzazali, 2012; MAMPU, 2013) to put security controls towards InfoSec, it is still not enough to specifically ensure the secure success for BYOD implementation in Malaysia government environment as the security implications such as information leakage still occurs. This is proven by the incidents of data and leakage involving agencies under PCN that impacted the government which classified information such as Official Secrets, tender procurement, the Cabinet paper as well as confidential and restricted materials have been exposed (Dzazali, 2012).

1.3 Problem Statement

Currently, BYOD implementation in Malaysian government agencies is a major issue of concern because of the data and information security elements, in precise official information and official secrets contained in the mobile devices of employees. The BYOD implementation is vulnerable to security threats, information leakage and any other security concerns related to the mobile technology. In the past decade, much research has focused on various BYOD security models or framework. It remains unclear why the models have limitations and require enhancements as well as improvements before widely implemented securely. BYOD benefit the user and the organisation, but it needs to be managed in a systematic way so that information is not compromised. The existing BYOD security solutions are not able to overcome the official information and official secrets in the mobile devices from being compromised and the Confidentiality, Integrity, Availability Triad of information being violated by security threats. Control measures to implement BYOD in the organisation must balance the needs of security, functionality and easy to use. Based on the foundations of BYOD security and controls outlined by Malaysian government authorities such as MAMPU and CGSO considering the information must be protected under any circumstances (on usage, location, device, and access), the BYOD implementation succession is dependably on security that contribute to

the mobile technology as well as user's behaviour concerning security relations that implementing the technology. Therefore, there is a need and indispensable to develop a holistic, unique and secure success model for BYOD implementation to ensure the information security that preserves the confidentiality, integrity, availability triad of strategic data organisation.

1.4 Research Question

Considering the issues and problem statement mentioned, several Research Questions (RQs) of this study can be extracted and is formulated as follows:

1.4.1 RQ1: What are the factors of BYOD implementation success model from both human and security perspectives?

1.4.2 RQ2: How to develop a secure success model for BYOD implementation in Malaysia government environment?

1.4.3 RQ3: Which factors are most significant in determining success implementation of BYOD in Malaysian government environment?

1.5 Research Objective

The purpose of this study is to develop a secure success model for BYOD implementation in Malaysia government environment that overcomes the security concerns when implementing secure BYOD. The targeted goal will be accomplished by completing the following Research Objectives (ROs):

1.5.1 RO1: To identify the factors of BYOD implementation success model from both human and security perspectives.

1.5.2 RO2: To develop a secure success model for BYOD implementation in Malaysia government environment.

1.5.3 RO3: To evaluate the proposed model in determining success implementation of BYOD in Malaysian government environment.

1.6 Scope of Study

The respondents of this study will cover all employees of ICT Security Division and ICT Policy Development in Malaysian Federal Government agencies especially working in Putrajaya and Cyberjaya Selangor which confined to the current BYOD implementation. This study will only review and analyse the relevant security's factors in implementing BYOD securely from both human and security perspectives such as policy management and technology. In addition, a sample of selected government agencies with employees who have various background knowledge of information technology is identified to evaluate the secure success model for BYOD implementation. Data collection methodology will be mixed-methods with a combination of interview and questionnaire. Data collected will be analysed using Statistical Package for the Social Sciences (SPSS), Microsoft Excel and/or other related statistical software.

1.7 Significance of Study

This study will be a substantial effort in stimulating the practice of secure BYOD technology implementation in Malaysian government agencies. Focusing on the development of the BYOD secure success model, where the model can be used as a guide for implementing BYOD technology in a secure success way.

1.7.1 Theoretical Contribution

In this study, a relevant factor that reflected in current BYOD implementation and existing security models from various researchers are identified and investigated in the motivating deployment of a secure success model for BYOD implementation in Malaysia government environment. Together, the factors that mark significantly in implementing the BYOD technology securely also highlighted. This study is likewise about discovering probable security factors resulting from the literature that entails comprehensive investigation. The impact to the theoretical not restricted to what has been specified, even adding facts in more understanding on technical characteristics.

1.7.2 Practical Contribution

The impact of this study would be attention to researchers in BYOD technology as well as the organisation and developer mostly in security practice. The results and recommended secure success model will valuable to IT leaders and decision makers of the agencies in implementing the BYOD technology successfully and suitable security controls can be embraced by government agencies in Malaysia.

1.8 Summary

This section covers the overview of BYOD implementation issues and the problem statement is acknowledged when BYOD users connect their mobile devices to a government network for official services usage. The weakness is wide-open a major issue of concern because of the information security elements, in precise official information and official secrets that contained in the mobile devices of employees. Therefore, in this research, a success model for BYOD implementation will be proposed to determine success implementation of BYOD in Malaysia government environment.

This research comprises six chapters. Chapter One (1) deals with research background about bringing personal mobile devices to the organisation to carry out daily tasks which consist of the Overview, Problem Background, Problem Statement, Research Question, Research Objective, Scope of Study, and Significance of Study.

In Chapter Two (2), a Literature Review (LR) of the BYOD definition, BYOD Baseline Theory Model from both human and security perspectives are discussed. BYOD Previous Researchers' Findings on existing BYOD Model/Framework and Technologies will be indicated and benchmark in order to discover the gaps or limitations between the current implementation.

Chapter Three (3) consists of the Research Methodology which supports in working the study. Instruments Design, Data Collection Method, Data Analysis Procedure, and Pilot Study activities are detailed as techniques and methods selected to achieve the aim and objective of the study.

Chapter Four (4) describes the proposed Conceptual Model for BYOD success implementation based on the initial findings gathered from the LR and initial Expert Review. Existing BYOD Security Model/Framework has been analysed and factors of those models have been identified. A secure success conceptual model for BYOD implementation in Malaysia government environment has been proposed.

Chapter Five (5) consists of the Results and Data Analysis which presented statistical analysis figures about data analysis on significant factors affecting the success of BYOD implementation through techniques and methods identified in Chapter 4.

Chapter Six (6) consists of the Discussion and Conclusion for Findings Summary which the results in Chapter 5 are supporting or not the proposed BYOD model in achieving the objectives specified earlier. Contribution, Limitations, and Future Works are also discussed in this chapter.

REFERENCES

Abdullah, N. (2015). Mobile Future Trends in Public Sector.

Ackerman, A., & Krupp, M. (2012). Five Components to Consider for BYOT/BYOD. *International Association for Development*, (Celda), 35–41.

Ahmad, R., & Usop, H. (2011). *Conducting Research in Social Sciences, Humanities, Economics and Management Studies: A Practical Guide*. RS Group Publishing House.

Akin-Adetoro, A., & Kabanda, S. (2015). Contextualising BYOD in SMEs in developing countries. *Proceedings of the 2015 Annual Research Conference on South African Institute of Computer Scientists and Information Technologists - SAICSIT '15*, 1–8.

Alzair, F. (2016). *A Critical Review of the Governance of Personal IT Devices in Work Environments*.

Armando, A., Costa, G., & Merlo, A. (2013). Bring Your Own Device, Securely. *Proceedings of the 28th Annual ACM Symposium on Applied Computing - SAC '13*, 1852.

Armando, A., Costa, G., Verderame, L., Merlo, A., Bennett, L., Tucker, H., … Price, M. (2012). Changing User Attitudes to Security in Bring Your Own Device (BYOD) and the Cloud. *Network Security*, *2012*(3), 5–8.

Bann, L. L., Singh, M. M., & Samsudin, A. (2015). Trusted Security Policies for Tackling Advanced Persistent Threat via Spear Phishing in BYOD Environment. *Procedia Computer Science*, *72*, 129–136.

Beatson, M. (2014). BYOD? I'm Not So Sur. Retrieved December 19, 2016, from http://www.futureofworkhub.info/comment/2014/12/17/byod-im-not-so-sur.

Bhattacherjee, A. (2012). Social Science Research: Principles, Methods, and Practices. Retrieved from http://scholarcommons.usf.edu/oa_textbooks.

Boon, G. L. (2016). A Review on Understanding of BYOD Issues, Frameworks and Policies. *The 3rd National Graduate Conference (NatGrad2015), Universiti Tenaga Nasional*, (April 2015), 8–9.

Bradley, J., Loucks, J., Macaulay, J., Medcalf, R., & Buckalew, L. (2012). Horizons BYOD: A Global Perspective Harnessing Employee-Led Innovation. *CISCO IBSG Horizons*, 1–21.

Bradley, T. (2011). Pros and Cons of Bringing Your Own Device to Work.

Breslav, S., Goldstein, R., Khan, A., & Hornbæk, K. (2015). Exploratory Sequential Data Analysis for Multi-Agent Occupancy Simulation Results. In *simaud* (p. 8).

Cavoukian, A. (2013). BYOD: Is your Organization Ready?

Chang, J. M., Ho, P. C., & Chang, T. C. (2014). Securing BYOD. *IT Professional*, *16*(5), 9–11. http://doi.org/10.1109/MITP.2014.76.

Che Kamal. S. (2015). *Persepsi Pengguna Terhadap Faktor Keselamatan Konsep Membawa Peranti Anda Sendiri*.

Coakes, S. J., Steed, L., & Ong, C. (2009). SPSS Analysis without Anguish Version 16.0 for Windows.

Coakes, S. J., Steed, L., & Price, J. (2008). SPSS: Analysis Without Anguish; version 15.0 for Windows. *SPSS for Windows*.

Cochran, W. G. (1977). *Sampling Techniques*. *New York: John Wiley and Sons* (3rd Editio). John Wiley & Sons.

Cook, I. (2012). BYOD Research - Ovum Research Published. Retrieved December 19, 2016, from http://cxounplugged.com/2012/11/ovum_byod_research-findings-released.

Creswell, J. W. (2014a). Research Design: Qualitative, Quantitative and Mixed Methods Approaches. In *Research design Qualitative Quantitative and Mixed Methods Approaches* (pp. 3–26).

Creswell, J. W. (2014b). *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*. *Sage Publications*.

Creswell, J. W., & Plano Clark, V. L. (2011). *Designing and Conducting Mixed Methods Research*. SAGE Publications.

DeLone, W. H., & McLean, E. R. (1992). Information Systems Success: The Quest for the Dependent Variable. *Information Systems Research*, *3*(1), 60–95.

DeLone, W. H., & McLean, E. R. (2003a). The DeLone and McLean Model of Information Systems Success: A Ten-Year Update. *Journal of Management Information Systems*, *19*(4), 9–30.

DeLone, W. H., & McLean, E. R. (2003b). The DeLone and McLean Model of Information Systems Success: A Ten-Year Update. *Journal of Management Information Systems*, *19*(4), 9–30.

Dhingra, M. (2016). Legal Issues in Secure Implementation of Bring Your Own Device (BYOD). *Procedia Computer Science*, *78*(December 2015), 179–184.

Disterer, G., & Kleiner, C. (2013a). BYOD Bring Your Own Device. *Procedia Technology*, *9*, 43–53.

Disterer, G., & Kleiner, C. (2013b). BYOD Bring Your Own Device. *Procedia Technology*, *9*, 43–53.

Dong, Y., Mao, J., Guan, H., Li, J., & Chen, Y. (2015). A Virtualization Solution for BYOD with Dynamic Platform Context Switch. *IEEE Micro*, *35*(1), 34–43.

Downer, K., & Bhattacharya, M. (2016). BYOD security: A new business challenge. In *Proceedings - 2015 IEEE International Conference on Smart City, SmartCity 2015, Held Jointly with 8th IEEE International Conference on Social Computing and Networking, SocialCom 2015, 5th IEEE International Conference on Sustainable Computing and Communic* (pp. 1128–1133).

Dzazali, D. S. (2012). *Perlindungan Ketirisan Maklumat Elektronik*.

El Ajou, N. (2012). Bring Your Own Device Trend is ICT Industry's Hottest Talking Point at GITEX Technology Week.

Engan, J. (2015). *Cabaran BYOD dalam Persekitaran Kerja*.

Eslahi, M., Naseri, M. V., Hashim, H., Tahir, N. M., & Saad, E. H. M. (2014). BYOD: Current State and Security Challenges. In *ISCAIE 2014 - 2014 IEEE Symposium on Computer Applications and Industrial Electronics* (pp. 189–192).

Finneran, M., & Brashear, J. (2014). A Legal Perspective of BYOD.

French, A. M., Guo, C., & Shim, J. P. (2014). Current Status, Issues, and Future of Bring Your Own Device (BYOD). *Communications of the Association for Information Systems*, *35*(10), 191–197.

Fuli, L. I. (2009). *A Stress and Coping Perspective on Creativity: A Reward for Creativity Policy as a Stressor in Organizations*. *Creativity*.

Gens, F., Levitas, D., & Segal, R. (2011). IDC 2011 Consumerization of IT Study.

George, D., & Mallery, P. (2013). SPSS for Windows Step by Step A Simple Guide and Reference.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). Multivariate Data Analysis (p. 785). Prentice Hall.

Harding, G., Schein, J. R., Nelson, W. W., Vallow, S., Olson, W. H., Hewitt, D. J., & Polomano, R. C. (2010). Development and Validation of a New Instrument to Evaluate the Ease of Use of Patient-Controlled Analgesic Modalities for Postoperative Patients. *Journal of Medical Economics*, *13*(1), 42–54.

Harkins, M. (2016). Mobile: Learn from Intel's CISO on Securing Employee-Owned Devices.

Harris, J., Ives, B., & Junglas, I. (2012). IT Consumerization: When Gadgets Turn Into Enterprise IT Tools. *MIS Quarterly Executive*, *11*(3), 99–112.

Hertzog, M. A. (2008). Considerations in Determining Sample Size for Pilot Studies. *Research in Nursing & Health*, *31*(2), 180–91.

Ho, C. P. (2013). *Research Methodology Manual*. (E-Sentral Ebook Portal, Ed.). Kuala Lumpur: INTAN.

Kranton, R. E. (1996). Reciprocal Exchange: A Self-Sustaining System. *American Economic Review*, *86*(4), 830–851.

Krejcie, R. V, & Morgan, D. W. (1970). Determining Sample Size for Research Activities. *Educational and Psychological Measurement*, *38*(1), 607–610.

Kumar, A. (2014). More than 50% Malaysian Enterprises Use BYOD but Lack Mobile Solutions.

Laumer, S., & Eckhardt, A. (2012). The Updated DeLone and McLean Model of Information Systems Success. *Information Systems Theory*, *1*(November 2015), 63–86.

Maarop, N. (2013). *Understanding the Acceptance of Teleconsultation Technology in Malaysian Government Hospitals*. University of Wollongong.

Maarop, N., Win, K. T., & Singh, H. S. (2014). Understanding Demographics Influence on Teleconsultation Acceptance in Hospital: A Mixed- Method Study. *Journal of Advanced Management Science*, *2*(2), 117–122.

MAMPU. (2000). General Circular.

MAMPU. (2002). Circulars Guidelines.

MAMPU. (2007). IT Instructions.

MAMPU. (2013). Data Leakage Protection (DLP).

MAMPU. (2015a). GAMMA-Gallery of Malaysian Government Mobile Applications.

MAMPU. (2015b). Ke Arah Perkhidmatan Mudah Alih.

MAMPU. (2016a). Galeri Aplikasi Mudah Alih Kerajaan Malaysia (GAMMA).

MAMPU. (2016b). Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA).

Mansfield-Devine, S. (2012). Interview: BYOD and the Enterprise Network. *Computer Fraud and Security*, (4), 14–17.

Matthew, H. (2014). What is CIA Triad?

MCMC. (2015). Communications and Multimedia Pocket Book of Statistics. *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative Data Analysis: An Expanded Sourcebook*. Sage Publications.

Miles, M. B., Huberman, A. M., & Saldaña, J. (2013). *Qualitative Data Analysis: A Methods Sourcebook*.

Millman, R. (2013). Surge in BYOD Sees 7/10 Employees Using their Own Devices.

MINDEF. (2013). Connected MinDef: BYOD 1 Fenomena.

Mohd Zahri, D. D. N. A. (2013). *Getting to the Next Level of Smart Government*.

Morrow, B. (2012). BYOD Security Challenges: Control and Protect your Most Sensitive Data. *Network Security*, *2012*(12), 5–8.

Nunnally, J. C. (1978). *Psychometric Theory*. McGraw-Hill.

Official Secrets Act of Malaysia 1972. (2015).

Olalere, M., Abdullah, M. T., Mahmod, R., & Abdullah, A. (2015). A Review of Bring Your Own Device on Security Issues, *5*(2).

Olson, D. H. (2010). FACES IV & the Circumplex Model: Validation Study. *In Press Journal of Marital & Family Therapy*.

Pallant, J. (2011). *SPSS Survival Manual: A Step by Step Guide to Data Analysis using SPSS*.

Palys, T. (2008). Purposive Sampling. *Qualitative Research Methods*, *2*, 697–8.

Perez-Gonzalez, D., & Daiz-Daiz, R. (2015). Public Services Provided with ICT in the Smart City Environment: The Case of Spanish Cities. *Journal of Universal Computer Science*, *21*(2), 248–267.

Reinfelder, L., & Weishaupl, E. (2016). A Literature Review on Smartphone Security in Organizations Using a New Theoretical Model – the Dynamic Security Success Model.

Rhee, K. H., & Yi, J. H. (2015). Context-Based Smart Access Control on BYOD Environments. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *8909*, 165–176.

Richards, S. (2013). NSW Government Mobile Device & Application Framework, 1–17.

Rivera, J., & Van Der Meulen, R. (2014). Gartner Says By 2018, More Than 50 Percent of Users Will Use a Tablet or Smartphone First for All Online Activities. *Gartner Inc. Press Release*.

Rozali, M. R. (2015). *Security Implementation Approach for the Use of Bring Your Own Device in Government Agencies*.

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research Methods for Business Students*.

Schindler, E. (2016). Protecting Corporate Data When an Employee Leaves.

Sedgwick, P. (2013). Convenience Sampling, *347*(oct25 2), f6304–f6304.

Sekaran, U. (2005). *Research Methods for Business: A Skill-Building Approach* (4th Ed). John Wiley & Sons.

Selviandro, N., Wisudiawan, G., Puspitasari, S., & Adrian, M. (2015). Preliminary Study for Determining BYOD Implementation Framework Based on Organizational Culture Analysis Enhanced by Cloud Management Control. In *2015 3rd International Conference on Information and Communication Technology, ICoICT 2015* (pp. 113–118).

Siang, L. C., Noor, Z. M., & Ann, T. B. (2012). Kesan ICT terhadap Produktiviti Pekerja Dalam Sektor Perkhidmatan terpilih di Malaysia. *Jurnal Ekonomi Malaysia*, *46*(2), 115–126.

Snyder, B. (2012). Staying Connected from Anywhere just Got a Lot Easier.

Suen, L.-J. W., Huang, H.-M., & Lee, H.-H. (2014). A Comparison of Convenience Sampling and Purposive Sampling. *The Journal of Nursing*, *61*(3), 105–111.

Sulaiman, D. M. (2013). *Smart Government Initiatives Government Appstore*.

The CIA Principle. (2001).

The Malaysian Official Secrets Act 1972. (2004), 1–15.

Thomson, G. (2012). BYOD: Enabling the Chaos. *Network Security*, *2012*(2), 5–8.

Tokuyoshi, B. (2013). The Security Implications of BYOD. *Network Security*, *2013*(4), 12–13.

Treasury. (2016). Portal 1PP: Peraturan Alat Komunikasi Mudah Alih.

Ugochukwu Franklin, O., & Ismail, M. Z. (2015). The Future of BYOD in Organizations and Higher Institution of Learning. *International Journals*, *3*(1), 13.

Van Leeuwen, D. (2014). Bring Your Own Software. *Network Security*, *2014*(3), 12–13.

Vargas, R. J. G., Anaya, E. A., Huerta, R. G., & Hernandez, A. F. M. (2012a). Security controls for Android. In *Proceedings of the 2012 4th International Conference on Computational Aspects of Social Networks, CASoN 2012* (pp. 212–216).

Vargas, R. J. G., Anaya, E. A., Huerta, R. G., & Hernandez, A. F. M. (2012b). Security Controls for Android. In *Proceedings of the 2012 4th International Conference on Computational Aspects of Social Networks, CASoN 2012* (pp. 212–216).

Vejayon, J. (2014). *Developing a Guideline for Adopting BYOD in a Higher Learning Institution*.

Vignesh, U., & Asha, S. (2015). Modifying security policies towards BYOD. In *Procedia Computer Science* (Vol. 50, pp. 511–516).

Weber, R. H., & Studer, E. (2016). Cybersecurity in the Internet of Things: Legal Aspects. *Computer Law & Security Review*, *32*(5), 715–728.

Wong, W. (2012). BYOD: The Risks of Bring Your Own Device. *Risk Management (00355593)*, *59*(5), 9–9.

Yapp, E. (2013). Malaysians are All for BYOD, but their IT Depts aren't: Survey | Digital News Asia.

Yin, C., Liu, L., & Liu, L. (2014). BYOD Implementation: Understanding Organizational Performance through a Gift Perspective. *PACIS 2014 Proceedings*, 9.

Yong, W., Jinpeng, W., & Vangury, K. (2014). Bring Your Own Device Security Issues and Challenges. In *2014 IEEE 11th Consumer Communications and Networking Conference (CCNC)* (pp. 80–85). IEEE.