2016

Mitigating BYOD Information Security Risks

Daniel Alejandro Arregui
The University of Melbourne, darregui@student.unimelb.edu.au

Sean B. Maynard
The University of Melbourne, seanbm@unimelb.edu.au

Atif Ahmad
The University of Melbourne, atif@unimelb.edu.au

Mitigating BYOD Information Security Risks

Daniel Alejandro Arregui

Sean B. Maynard

Atif Ahmad
Department of Computing and Information Systems
University of Melbourne
Australia
Email: darregui@student.unimelb.edu.au
Sean.Maynard@unimelb.edu.au
Atif@unimelb.edu.au

Abstract

Organisations that allow employees to Bring Your Own Device (BYOD) in the workplace trade off the convenience of allowing employees to use their own device against higher risks to the confidentiality, integrity, and availability of organisational information assets. While BYOD is a well-defined and accepted trend in some organisations, there is little research on how policies can address the information security risks posed by BYOD. This paper reviews the extant literature and develops a comprehensive list of information security risks that are associated with allowing BYOD in organisations. This list is then used to evaluate five BYOD policy documents to determine how comprehensively BYOD information security risks are addressed. The outcome of this research shows that of the 13 identified BYOD risks, only 8 were adequately addressed by most of the organisations.

Keywords: BYOD, Information Security Management, Security Risk

1 Introduction

As technology has become more ubiquitous, the use of mobile devices for conducting organisational work has increased. In particular, the demand of employees to be able to use their own devices in the workplace for carrying out organisational tasks is a driving force behind organisations adopting a Bring Your Own Device (BYOD) approach to doing business. In allowing BYOD in the workplace, employees can access organisational information assets on employee owned devices (Astani et al. 2013). This is convenient for users and the organisation. Users can be more productive, accessing electronic organisational resources from inside and outside the workplace and organisations can reduce the cost of providing electronic devices to their employees (Donaldson et al. 2015; Kang et al. 2015). However, this convenience introduces challenges for organisations in terms of how to implement security practices on devices that are privately owned (Zahadat et al. 2015).

Donaldson et al. (2015) comment that despite the growth of information security concerns from BYOD, organisations cannot stop this trend. Currently, in order to maintain the confidentiality, integrity and availability of the organisations information assets, international best practices often are usually employed (Von Solms and Von Solms 2009). However, specific best practice for establishing a BYOD program in organisations is not yet well defined (Zahadat et al. 2015). Subsequently, although security experts have identified several BYOD risks that may arise, BYOD risks have not been adequately addressed by the Information Systems (IS) community (Tu et al. 2015).

The purpose of this paper is twofold. First, it analyses the literature around BYOD and security to identify a comprehensive list of security risks particular to BYOD. Second, it carries out an evaluation of five BYOD policies to identify those risks that are not being mitigated by those policies. This evaluation aims to address the main research question:

How comprehensively are BYOD information security risks addressed in BYOD policy?

This paper is structured as follows. Background to the area of BYOD and information security is presented and the challenges that arise from organisations allowing BYOD are identified. The research approach is then described. This is followed by a comprehensive review of literature around BYOD and its related security risks which identifies 13 BYOD specific security risks. Finally, an analysis of 5 BYOD policies is made, the results of this analysis and discusses, and the implications, contributions and further research propositions are outlined.

2 Background

In this section the definition, organisational benefits and security issues of BYOD are introduced.

2.1 BYOD Definition

There are a number of definitions of the concept of BYOD in the literature. In this paper we adapt the definition provided by Gartner (2012) which states that BYOD can potentially include a large variety of electronic devices including: workstations, mobile communication devices portable storage media (USB memory sticks, memory cards, portable hard drives, floppy disks) and media recorders. From this broad BYOD definition, the BYOD scope has been narrowed in this research. The main feature to consider in an electronic device like a BYOD is that *users are often conducting knowledge work*. In this study the BYOD scope has been limited to personal devices with the following characteristics:

- The user can do knowledge work with the device.
- It must be owned by the individual and not by the organisation.
- The device is portable.
- It is capable of installing third party software applications.
- It can be connected to at least one wireless network interface, a mobile phone network (2G, 3G, 4G), a local area wireless computer network (Wi-Fi) or a personal area network (Bluetooth).

2.2 Benefits of Allowing BYOD into Organisations

Organisations allowing BYOD in the workplace gain a number of benefits. First, employees are more likely to do organisational work whilst off site as they can access the same electronic resources from almost any location as they can in their workplace (Donaldson et al. 2015). Second, adopting BYOD reduces organisational operation costs (Kang et al. 2015). If organisations allow their employees to use their personal devices, they eliminate the cost of providing hardware, software and technical maintenance (Kang et al. 2015). Additionally, organisations do not need to provide training to users on

using the device as they are already familiar with its functionality (Kang et al. 2015). Third, BYOD provides better productivity and efficiency among users (Kang et al. 2015). According to Köffer et al. (2015), enterprise tools provided by organisations are often considered *"slow and cumbersome."* Therefore, organisations allowing their employees to use their smartphones and tablets can increase their productivity (Kang et al. 2015; Köffer et al. 2015). Additionally, allowing BYOD creates a positive change in the working environment because employees don't feel restricted using organisation' equipment. Indeed, Köffer et al. (2015) claim that BYOD in some cases not only increases productivity, but also stimulates innovation among employees, giving more flexibility and can result in an increase in employee contentment.

2.3 BYOD and Information Security

Despite the benefits of implementing BYOD in organisations, it has also created novel security risks for organisations (Webb et al. 2014). Allowing BYOD into the organisation creates potential security breaches because users' devices will have access to the internal network and sensitive organisational information (Moreira et al. 2015). Son (2011) suggests that employing personal devices in organisations has contributed to over half of information security breaches occurring in organisations, as employees often fail to comply with information security procedures. The challenge for organisations is to influence the use of personal devices, which are not part of organisational fixed assets, to protect organisational information security. Organisations need effective ways to preserve confidentiality, integrity and availability of sensitive information accessed or manipulated with the rise of personal devices (Ahmad et al. 2006). Cappelli et al. (2012) remark that information security incidents can be triggered by former employees, contractors, suppliers and business partners, who may have access to sensitive organisational information using personal devices. Information leakage may cause substantial damage to the organisation, including financial loss, operational disruption, damage to the organisation reputation and damage to the client's image (Ahmad et al. 2014).

3 Research methodology

This paper undertakes a comprehensive literature review to identify BYOD specific security risks. The review searched for literature on BYOD and Mobile Devices related to security, policy, issues, challenges and utilised the following search engines: "Science Direct", "Springer", "IEEE", "ProQuest", "Taylor & Francis Group", and "Google Scholar". 120 academic articles were selected based on their titles and abstracts from this search. Each article was then read to determine their relevance and those articles that were not relevant to this research were discarded. This resulted in 50 papers being identified that were relevant, which were then analysed using thematic coding as described by Neuman (2006). This analysis resulted in the identification of 13 subthemes (or security risks related to BYOD).

The second part of this research uses the BYOD risks identified to assess 5 organisational BYOD policies to determine whether organisations address the risks. Initially we searched for (using Google) and identified 27 policies related to mobile devices and BYOD in organisations. From this we read each policy and discarded 19 of these as they did not deal with the use of personal devices (rather just mobile devices provided by the organisation). This left 8 policies. As this was preliminary research, a selection of different organisations types was selected (related to the 8 policies we were able to collect), 5 in total: Org1 – Non Profit Organisation, Org2 – Health Organisation, Org3 Educational Organisation, Org4 Government Organisation, Org5 – Private Organisation. The remaining 3 policies were all in the education sector and were not used in the study (there were similar in form and content to the other policies in the education sector). The policies were evaluated against the comprehensive list of security risks associated with allowing BYOD into organisations. The analysis was made comparing each BYOD policy statement with the risks identified in the literature. If one statement in the BYOD policy addresses one of the identified risks, it was concluded that the organisation acknowledges and therefore tries to mitigate that risk. Conversely, if none of the policy statements addressed a specific risk it was concluded that the organisation does not acknowledge and therefore doesn't mitigate that risk. The analysis did not include how effective the organisation was in mitigating BYOD risks. However, it did identify the extent of those risks addressed in the five BYOD policies.

4 Literature Review Synthesis of Risks Associated with Allowing BYOD into Organisations

Table 1 summarises thirteen BYOD risks from the literature that are associated with allowing BYOD into organisations. Additionally, to identify the most significant risks, they have been grouped into

three common areas related to BYOD usage: User behaviour, Connectivity risks, Organisational management practices. This section will discuss each risk in turn.

User Behaviour	
Risk 1: BYOD Device Selection Risk 2: BYOD Customisation Risk 3: Installation of Malicious Applications Risk 4: Insecure Operational Behaviour	Risk 5: Unauthorised Access Risk 6: Exposure of Sensitive Organisational Data Risk 7: Lost BYOD Devices Risk 8: Data Integrity Loss
Connectivity	
Risk 9: Exposure in Public Networks Risk 10: Local Network Exposure	Risk 11: Exposure in Personal Networks
Organisational Management Practices	
Risk 12: BYOD Remote Management	Risk 13: BYOD Training

Table 1: Synthesis of risks associated with allowing BYOD into the organisation

4.1 BYOD Risks that Arise from User's Behaviour

This section identifies and discusses 8 risks that arise from user's behaviour.

4.1.1 Risk 1: BYOD Device Selection

Users can choose from many BYOD platforms (eg. Apple's iOS, Android, and Windows Mobile). Each platform has a unique security model, with strengths and weaknesses to counter security incidents (Gajar et al. 2013). To illustrate this, Android's open structure is customisable by the user which makes it more susceptible to attacks than other mobile systems (Wood 2013). Whereas, Apple's iOS security prevents the use of mobile device management (MDM) because of security restrictions in the operating system. The specific selection of a BYOD platform by users can expose the organisation to information security incidents, that are not present in other platforms (Armando et al. 2014; Mont 2012). Organisations need to evaluate the security risks for each BYOD platform before initiating a BYOD program. They should define the benefits and disadvantages of particular platforms and establish strategies to counter security incidents that may arise. This information should be conveyed to users.

4.1.2 Risk 2: BYOD Customisation

Users can customise some BYOD platforms to alter their "security" features; thereby, exposing the organisation to information security incidents (Gest 2013; Kang et al. 2015; Lawrence and Riley 2014). "Jailbreaking", "root", and "unlock" are three popular procedures that users may execute on personal devices to remove vendors' configuration restrictions, thereby customising their devices according to their requirements. These procedures allow users to install third-party applications unavailable on official vendor stores or unlock carrier-locked devices (Lawrence and Riley 2014). Users bringing these devices into organisations may affect information security when utilised as BYOD's. Kang et al. (2015) suggests that "jailbreaking" or "root" devices are made more vulnerable to insecure applications because they can access device sensors (microphone, camera, etc.) or sensitive information storage in the device (contacts, calendars, etc.) without restrictions. Insecure applications on jailbroken devices run with administrator privileges with considerable control over device sensors and applications (Kang et al. 2015). Subsequently, it is critical for organisations to define whether or not the use of "jailbreaking" or "root" devices is permitted as a BYOD.

4.1.3 Risk 3: Installation of Malicious Applications

Normally, users customise their devices according to their preferences and needs, using application markets, like Apple Store and Google Play, to browse and install applications. Armando et al. (2014) suggests that during the application installation process, users grant permissions, like allowing push notifications or location-based services, putting aside security considerations because of the benefits that will be received (Armando et al. 2014). The security risk arises when applications with different levels of trust are installed on the same device (Chin et al. 2011). For example, a free game application will be installed on the same device as a highly trusted banking application. The free application may be a malicious one that can sniff, modify, or steal inter-application messages and, therefore, compromise organisational information security (Ketel and Shumate 2015). Ketel and Shumate (2015) claim that users are unable to recognise which applications have malicious functionality. Those applications affect the information security of the organisation, generate problems for data privacy, and affect organisations and customers' reputations (Ketel and Shumate 2015). Ketel and Shumate

(2014) maintain that it is critical for organisations to control which applications can be installed on BYOD in order to protect the information security of the organisation.

4.1.4 Risk 4: Insecure Operational Behaviour

Users engage in insecure behaviour while using BYODs allowing viruses and other malware infections to proliferate; exposing the organisation to information security incidents. (Gajar et al. 2013; Miller et al. 2012; Shumate and Ketel 2014; Wang et al. 2014). Malware is software created to disrupt the normal operation of other software, gather personal information, or access personal computer devices (Kramer and Bradfield 2010). In the same way that it impacts personal computers, malware is affecting mobile devices. Drew (2012) states that with the exponential growth of mobile devices in the last five years, malicious software targeting mobile devices has also been increasing. Indeed, according to Alcatel-Lucent's report, 16 million mobile devices were infected with malware in 2014, representing a value 25% higher than in 2013 (Spencer 2015). Organisations must encourage the installation of anti-virus software on BYODs in order to prevent the proliferation of malware infection from BYODs.

4.1.5 Risk 5: Unauthorised Access

How users handle BYODs may allow unauthorised access to organisation information by third parties; exposing organisations to information security incidents (Wang et al. 2014). According to a survey conducted by Botdefender, 30% of BYOD users share their personal devices with relatives and friends, 40% do not have a save screen mechanism, and only 9% employ a biometric authentication mechanism to secure access to the device (Donovan 2014). This research clearly shows that BYOD users do not realise the security risks that may arise from unauthorised access to their devices by third parties. Cappelli et al. (2012) suggest that the use of password-protected screen savers, along with good password practices (enforcing password robustness, changing passwords periodically etc.) is essential to decrease information security incidents. This reduces the likelihood of unauthorised users' accessing sensitive information storage on devices and use of organisation applications.

4.1.6 Risk 6: Exposure of Sensitive Organisational Data

BYOD provides not only a wider range of endpoints where the employees can access organisational resources, but also allows distribution of sensitive information without authorisation, exposing data confidentiality (Miller et al. 2012). Once data is on a mobile device, control is difficult (Miller et al. 2012). Sensitive information, such as customer data, is generally restricted to a few users in the organisation, however, with personal devices, that information can be easily copied (Wang et al. 2014). Potts (2012) maintains that employees sometimes intentionally bypass organisational security, when they need an electronic enterprise resource to complete a task. This action is considered to be non-malicious misuse of organisational resources. Whilst normally the employee would not deliberately want to affect the information security of the organisation (Potts 2012), their actions could expose confidential organisational information (Wood 2013). For these reasons, organisations should establish the services and electronic resources that are allowed to access mobile devices (Miller et al. 2012). The organisation must consider the BYOD risks and determine the services and application that will be accessible from personal devices such as e-mail, calendars, contacts and electronic documents.

4.1.7 Risk 7: Lost BYOD Devices

Wang et al. (2014) suggest that one of the primary concerns for organisations about BYOD devices is the likelihood that the device could be lost or stolen. Kaspersky (2013) found that one of every six users has suffered damage, loss, or theft of their mobile devices. Theft and loss of mobile devices exposes the confidentiality of organisational information (e.g. emails, business documents and financial information), in addition to personal information. According to Tu et al., (2015), even though the serious consequences may lead to compromising that information, this risk has not been addressed adequately. A single lost device can affect an organisations reputation and could compromise customer privacy (Tu et al. 2015). Ketel and Shumate (2015) suggest that organisations need to implement technology tools able to remotely wipe or lock devices to protect sensitive organisational information.

4.1.8 Risk 8: Data Integrity Loss

In the normal operation of personal devices, users may accidentally modify or eliminate sensitive organisational information (Dong et al. 2015; Miller et al. 2012). As users employ BYOD for both personal and business purposes, both environments need to coexist harmoniously in the same device without adversely affecting each other (Wang et al. 2014). Therefore, the security procedures to prevent the accidental modification or elimination of sensitive organisational information are required. For instance: to prohibit downloading of organisational information into personal devices;

backing up and performing changes of control of documents; or using a virtualisation technique to separate organisational space from personal space in personal devices (Vishal et al. 2013).

4.2 BYOD Risks That Arise from Connectivity Procedures

This section identifies and discusses 3 risks that arise from connectivity procedures.

4.2.1 Risk 9: Exposure in Public Networks

Employees want to remain connected with organisational electronic resources with their BYOD devices even outside the organisation. Usually such connections are made via public networks, such as Wi-Fi hotspots, which are usually free and are common in public places such as restaurants and airports making them extremely attractive for users. Goldsborough (2011) explains that the confidentiality and integrity of BYOD information is exposed when users employ Wi-Fi hotspots. Souppaya and Kent (2012) state that public Wi-Fi hotspots are susceptible to a man-in-the-middle attacks and eavesdropping, causing compromises in the integrity and confidentiality of information. organisations can mitigate this risk by connecting through public networks employing encryption of the communication with a virtual private network (VPN) (Ketel and Shumate 2015).

4.2.2 Risk 10: Local Network Exposure

Potts (2012) argues that insider threats emerge when an employee bypasses BYOD security controls through connecting to a local area network inside an organisation. Potts (2012) argues that insider attacks are difficult to prevent since they occur in the local area network (LAN) of the organisation using a valid user profile. Ketel and Shumate (2015) consider that organisations must establish security characteristics of mobile devices and devices that do not meet the security conditions should be denied access. Antivirus software, mobile operating systems, and security configuration settings are some of the mobile characteristics that organisations need to consider while granting access to their internal network (Ketel and Shumate 2015). Moreover, Verizon's study suggests that organisations not only need to control employee-owned device access, but also review their users privileges to access sensitive data with their devices (Verizon 2014).

4.2.3 Risk 11: Exposure in Personal Networks

The information security of the organisation could be exposed when BYOD users connect their devices to a personal area network (Haataja 2008; Nasim 2012; Tan and Aguilar 2012). The most popular personal area network is one employing Bluetooth Technology (BT). BT is a wireless communication technology used within short ranges and is made of up to 7 devices acting as slaves (Nasim 2012). Podhradsky et al. (2012) claim that when a BT device is introduced as a business tool, it may be a threat not only to the user, but to the organisation as Bluetooth attacks can introduce security vulnerabilities into the business. These include eavesdropping, message modification and resource misappropriation (Podhradsky et al. 2012). Haataja (2008) and Podhradsky et al. (2012) suggest that the corporate information that is commonly compromised by Bluetooth attacks are: social security numbers, bank account information, business documents, contact information, and passwords. Podhradsky et al. (2012) suggest that the following security procedures may be adopted to reduce the likelihood of a Bluetooth incident: disable BT functionality if it is not used, change default device names, do not use the owner's name as part of the device name, and change default pairing passkeys.

4.3 BYOD Risks That Arise From Organisational Management Practices

This section identifies and discusses 2 risks that arise from organisational management practices.

4.3.1 Risk 12: BYOD Remote Management

Vishal et al. (2013) suggest that organisations need to establish BYOD policies, and also need to ensure that employee-owned devices comply with these policies. They affirm that the challenge for organisations is to manage remotely both a large quantity and numerous models of personal devices (Vishal et al. 2013). Leavitt (2013) insists that organisations need a technological tool to ensure employees' compliance with BYOD policies. Mobile Device Management (MDM) is a primary information security tool for organisations to manage employee-owned devices (Leavitt 2013). MDM permits organisations to monitor, manage, secure, and apply security policies on employee-owned mobile devices (Ketel and Shumate 2015). However, according to Schulze (2014), MDM alone does not provide sufficient security protection in a BYOD environment. MDM needs to be complemented with users' authentication control like Network Access Control (NAC). NAC controls the users that are allowed to access what sort of data (Ketel and Shumate 2015). Employing MDM and NAC allows the following functionality: device enrolment into the network (e.g. connection, device registration, user

authentication), device security compliance (e.g. passcode, encryption), device operation (e.g. profile configuration, certificates, accounts) and monitoring (e.g. policies, alerts, rules).

4.3.2 Risk 13: BYOD Training

Users, without appropriate information security knowledge, may perform insecure behaviour and social learning may contribute to this insecure behaviour (Leavitt 2013). Tu et al. (2015) maintain that social learning, which includes family, friends, colleagues, or social media, plays a significant role in the mobile security environment. They criticise that social learning may generate information security incidents as often information security best practice is not learnt via a social means (Tu et al. 2015). There is also work around the concept of consequential ethics that may relate to BYOD training (Ruighaver et al. 2010). Shumate and Ketel (2014) insist that the organisations require not only a well-defined set of BYOD guidelines, but they should also provide information security training sessions to their employees. Employees must know exactly what the organisation expects from them while they are working with their devices. The guidelines must include: safe device operation (e.g. establish lock codes or passcodes, avoid lending the device to third parties); networks allowed to access (e.g. hotspots are prohibited, a VPN connection needs to be established); measures to store organisational information (e.g. information must be encrypted, do not upload information to the cloud); and protocols to follow in case the device is lost or stolen (e.g. report immediately to the organisation).

5 Results & Discussion

In this section, the results of the analysis of the five BYOD policies are presented showing whether organisations have considered the risks identified (see table 1) in their BYOD policy. This section also discusses the findings obtained from the analysis of the five BYOD policy documents. In addition, a critical evaluation is included as a product of this assessment.

The analysis compared each BYOD policy statement of the five organisations with the 13 risks detailed in Table 1. If one of the policy statements addresses one or more risks in Table 1, it was inferred that the organisation is acknowledging and is applying a mitigation strategy to mitigate that risk. In contrast, if none of the policy statements is addressing a specific risk in Table 1, it was inferred that the organisation is not acknowledging and therefore not applying a mitigation strategy to mitigate that risk. Table 2 presents a summary of the findings obtained in this research. The table identifies the risks that have been acknowledged and addressed by the organisations.

Org1 – Non Profit Organisation, Org2 – Health Organisation, Org3 Educational Organisation, Org4 Government Organisation, Org5 – Private Organisation. (Y – risk is addressed, N – risk is not addressed)						
BYOD perspective	BYOD risks	Org1	Org2	Org3	Org4	Org5
User behaviour	Risk 1: BYOD Device Selection	Y	Y	Y	Y	Y
	Risk 2: BYOD Customisation	N	Y	Y	Y	Y
	Risk 3: Installation of Malicious Applications	Y	Y	Y	Y	N
	Risk 4: Insecure Operational Behaviour	Y	Y	Y	Y	Y
	Risk 5: Unauthorised Access	Y	Y	Y	Y	Y
	Risk 6: Exposure of Sensitive Organisational Data	Y	Y	N	Y	Y
	Risk 7: Lost BYOD Devices	Y	Y	Y	Y	Y
	Risk 8: Data Integrity Loss	N	N	Y	Y	Y
Connectivity procedures	Risk 9: Exposure in Public Networks	N	Y	Y	Y	N
	Risk 10: Local Network Exposure	Y	Y	N	N	Y
	Risk 11: Exposure in Personal Networks	N	N	Y	N	N
Management practices	Risk 12: BYOD Remote Management	Y	Y	N	Y	Y
	Risk 13: BYOD Training	N	Y	N	N	N

Table 2: Summary of BYOD policies analysis associated with allowing BYOD into organisations

5.1 Risk 1: BYOD Device Selection

Different BYOD platforms have unique security weaknesses that may trigger information security incidents while accessing sensitive organisational information. Thus, it is not surprising that all the organisations evaluated in this research have identified and limited the platforms that will be permitted to access organisational information. Indeed, some of them have defined the platform, the model and the version of the operating systems that will be included in the BYOD program. The more specific the models are in the policies; the better the control organisations can exert on those devices.

5.2 Risk 2: BYOD Customisation

The BYOD statements to prohibit the use of use of "jailbreaking" and "root" devices to access organisational information are consistent with that suggested by Kang et al. (2015). Organisations in this research have recognised that those types of devices tend to be more vulnerable to viruses and insecure applications, which may expose the organisation to information security incidents. However, none of the five organisations have considered "unlocked" devices. In the same way that "jailbreaking" and "root" devices are a threat to the information security of the organisation, "unlocked" devices do not have the security controls that prevent access to information by insecure applications. Therefore, organisations should also exclude "unlocked" devices to access organisational information.

5.3 Risk 3: Installation of Malicious Applications

Shumate and Ketel (2014) acknowledge that malicious applications installed on BYODs can compromise organisational information. In the same way, most of the organisations in this research have recognised this risk. They attempt to guide users to the applications that should be installed on their personal device. Most organisations address this risk with policy statements that recommend downloading applications from reputable sources only. Nevertheless, it is unclear how organisations will enforce this policy. An alternative solution to monitor applications on personal devices is to install MDM agent on personal devices. MDM agent, along with MDM software, is an automatic and efficient way to monitor the installation of approved applications into personal devices.

5.4 Risk 4: Insecure Operational Behaviour

Ketel and Shumate (2015) have drawn attention to the fact that malware can generate a cyber-attack in organisations. Similarly, all the organisations in this study are aware of the information security threats that may trigger the proliferation of malware in BYODs. Identified policy statements claim to use anti-virus software on personal devices. Furthermore, in order to strengthen this policy, organisations should be encouraged to install anti-virus software on personal devices, but also provide licenses to users for free. They can motivate users willing to install anti-virus software on their devices because this statement will protect both organisational and personal information.

5.5 Risk 5: Unauthorised Access

In alignment with Cappelli et al. (2012)'s recommendations to install password-protected screen savers on personal devices, the five organisational BYOD policies support using an authentication mechanism to secure access to the device. Additionally, organisations can strengthen the authentication mechanism with MDM functionality. To illustrate, one BYOD policy analysed (from a government organisation) mandates an e-mail wipe on the device after several failed password attempts. Organisations that implement this technique will strength the confidentiality protection of the information that is storage into personal devices.

5.6 Risk 6: Exposure of Sensitive Organisational Data

The predisposition to protect sensitive information storage on personal devices of four organisations in this research agrees with Miller et al. (2012)'s suggestion to define the services and applications that will be accessible from personal devices. Some of the organisations have defined e-mail, office calendar and contact list as services appropriate to be accessed from personal devices. However, these organisations have not mentioned in the policies how they are going to protect the access to non-authorised services and applications from BYODs.

5.7 Risk 7: Lost BYODs

As specified by Wang et al. (2014), most of the organisations attempted to protect themselves from the loss of personal devices. Consequently, almost all the organisations evaluated in this research have implemented a mobile device management solution to wipe organisational information from a BYOD remotely. Organisations should make it clear however in policy whether this functionality will wipe only organisational information or the whole information storage including personal information.

5.8 Risk 8: Data integrity Loss

Wang et al. (2014) suggest that users may accidentally eliminate sensitive organisational information in personal devices. Three of the five organisations evaluated have recognised this risk prohibiting the storage of organisational information only in BYOD devices. However, none of the five organisations have considered employing virtualisation techniques to separate organisational space from personal

space in BYOD devices. This method can provide an alternative solution to manage both personal and business information in the same device without it affecting each other.

5.9 Risk 9: Internal Network Exposure

Only two BYOD policies mandated VPN use while connecting to public networks from BYOD devices. These policy statements align with the recommendations of Ketel and Shumate (2015) to protect organisational integrity and confidentiality of the information. However, one of these two organisations have adopted a risky strategy to allow employees to "make a risk-conscious decision" before connecting to a public network without VPN usage. Such procedures may compromise the security of the information because end-users may not have adequate knowledge to define whether a network is secure.

5.10 Risk 10: Internal Network Exposure

Ketel and Shumate (2015) recommendations to protect the security the information from insider attacks from personal devices. These recommendations support the BYOD statements that encourage the installation of MDM agents in personal devices was taken by two organisations in this research. A MDM agent along with management software will control security configuration settings in personal devices such as configuration settings, software customisation, and malware. However, in order to reduce the probability of an insider attack is required to integrate the MDM with NAC solution to grant user access to personal devices to the local area network.

5.11 Risk 11: Exposure in Personal Networks

Only one of the five organisations has mitigated the risks that are associated with personal area network attacks. In alignment with Podhradsky et al. (2012)'s proposal, this policy statement recommends disabling the Bluetooth service while is not in use. Literature review recognises the high impact of this risk to the information security of the organisation. However, while developing this research, it was not found statistics regarding personal area network attacks. The lack of awareness in BYOD policies of this risk may be the result of its low occurrence probability.

5.12 Risk 12: BYOD Remote Management

Leavitt (2013) states that in order to preserve information security in organisations, it is necessary to remotely manage and control users' compliance with BYOD policies. Four of the organisations studied addressed this risk, and have implemented an MDM solution before granting access to sensitive information. It was expected that organisations would implement a technical solution to help to efficiently manage and control the large number and type of BYOD devices employed in the workplace.

5.13 Risk 13: BYOD Training

Only one of the five organisations in their policy statements has addressed the risk related to insecure behaviour while allowing BYOD into organisations as was recommended by Tu et al. (2015). The scope of BYOD policies is often limited to describing guidelines to mitigate information security risks. Therefore, it cannot be concluded that organisations have not considered this risk because it may be included in another document like IS strategic plan report of the organisation.

6 Conclusion

This study set out to answer the research question *"How comprehensively are BYOD information security risks addressed in BYOD policy"*? 13 BYOD specific risks were identified from the literature that were subsequently used to assess 5 organisation's BYOD policies. This study identifies that first, organisations are aware of the risks related to "User Behaviour" and its procedures to mitigate these risks. Also, organisations recognise that information security tools are necessary to mitigate BYOD risks (e.g. anti-virus software, authentication mechanisms, MDM software monitor, and document encryption). Second, the study results indicate that there is a weakness in mitigating the risks associated with "Connectivity Procedures". Some organisation's policies do not recognise the information security incidents that may originate from an insecure connection to both a public and personal area network. Third, regarding "Management Practices", the research suggests that organisations are relying on MDM as the main technological tool to monitor users' devices that are accessing organisational information.

Additionally, because of the limitations of this research it cannot be concluded whether organisations are considering the importance to provide training sessions to BYOD users. The content and the BYOD

risks described in this paper are solely based on the existing literature. BYOD is a fairly new research topic in the IS community (although there is some work on privacy – see (Carron et al. 2016)), so it was necessary to build a BYOD risks list to evaluate information security strategies of organisations with regard to BYOD. BYOD policies were used to evaluate organisational strategies, but it would have been more valuable to assess BYOD policies along with IS strategic plans and interviews with IS leaders. This presents a unique opportunity for future research.

The findings of this research imply that organisations are addressing the risks associated with users BYOD use with appropriate information security tools. However, they need to improve the information security best practices related to connectivity procedures. Organisations need to be aware of the information security incidents that may generate while connecting to different networks.

With the comprehensive list of BYOD and the findings of this research, organisations can build better information security procedures to manage information security risks associated with allowing BYOD in the workplace. They can use this information along with their organisational structures, procedures, processes and technology to build not only better BYOD policies, but also more efficient information security procedures. These procedures must adjust to the organisational reality and business goals in order to be practical for the organisation.

In this research, BYOD policies were evaluated against a comprehensive list of security risks associated with allowing BYOD into organisations. The evaluation was designed to identify statements in BYOD policies that mitigate information security risks in organisations. A further comparative study can be undertaken to identify the most effective strategy to address the same risk. This study must also consider the fact that the different organisations have unique information security priorities, as it depends heavily on the business goals of the organisation. Therefore, this future study must be focused to evaluate security strategies to mitigate information security risks from a specific industry sector.

References

Ahmad, A., Bosua, R., and Scheepers, R. 2014. "Protecting Organizational Competitive Advantage: A Knowledge Leakage Perspective," *Computers & Security* (42), 5/1/May 2014, pp 27-39.

Ahmad, A., Ruighaver, A.B., and Teo, W.T. 2006. "An Information-Centric Approach to Data Security in Organizations," Piscataway, IEEE, pp. 2255-2259.

Armando, A., Costa, G., Verderame, L., and Merlo, A. 2014. "Securing the "Bring Your Own Device" Paradigm," *Computer* (47:6), pp 48-56.

Astani, M., Ready, K., and Tessema, M. 2013. "Byod Issues and Strategies in Organizations " *Issues in Information Systems* (14:2), 12//, p 195.

Cappelli, D., Moore, A., and Trzeciak, R. 2012. *The Cert Guide to Insider Threats : How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud) / Dawn Cappelli, Andrew Moore, Randall Trzeciak*. Upper Saddle River, NJ : Addison-Wesley, c2012.

Carron, X., Bosua, R., Maynard, S.B., and Ahmad, A. 2016. "The Internet of Things and Its Impact on Individual Privacy: An Australian Privacy Principle Perspective," *Computer Law & Security Review* (21:1), pp 4-15.

Chin, E., Felt, A.P., Greenwood, K., and Wagner, D. 2011. "Analyzing Inter-Application Communication in Android," *Proceedings of the 9th International Conference: Mobile Systems, Applications & Services*), 06/28/, p 239.

Donaldson, S.E., Siegel, S.G., Williams, C.K., and Aslam, A. 2015. "Enterprise Cybersecurity Capabilities," *Enterprise Cybersecurity*), 01//, p 311.

Dong, Y., Mao, J., Guan, H., Li, J., and Chen, Y. 2015. "A Virtualization Solution for Byod with Dynamic Platform Context Switching," *IEEE Micro* (35:1), pp 34-43.

Donovan, F. 2014. "Employees Fail to Take Basic Steps to Secure Byod Devices, Data," *Fierce Mobile IT*), 09/30/, p 1.

Drew, J. 2012. "Managing Cybersecurity Risks," *Journal of Accountancy* (214:2), 08//, pp 44-48.

Gajar, Ghosh, A., and Rai. 2013. "Bring Your Own Device (Byod)- Security Risks and Mitigating Strategies," *JGRCS*).

Gartner. 2012. "Byod - Bring Your Own Device - Free Gartner Research." Retrieved 6 September 2015, from http://www.gartner.com/it-glossary/bring-your-own-device-byod

Gest, J. 2013. "Managing Byod." Smart Business Network, Inc., pp. 20-20.

Goldsborough, R. 2011. "Wi-Fi Convenience Comes with Risks." Autumn Publishing, p. 18.

Haataja, K.M.J. 2008. "Further Classification of Bluetooth-Enabled Ad-Hoc Networks Depending on a Risk Analysis within Each Classified Group," *Seventh International Conference on Networking (ICn 2008)*), 01//, p 232.

Kang, D., Oh, J., and Im, C. 2015. "Context Based Smart Access Control on Byod Environments," *Information Security Applications 15th International Workshop, WISA 2014, Jeju Island, Korea, August 25-27, 2014. Revised Selected Papers*), 01//, p 165.
Kaspersky. 2013. "One in Every Six Users Suffer Loss or Theft of Mobile Devices." Kaspersky Lab.
Ketel, M., and Shumate, T. 2015. "Bring Your Own Device: Security Technologies," *SoutheastCon 2015*), pp 1-7.
Köffer, S., Ortbach, K., Junglas, I., Niehaves, B., and Harris, J. 2015. "Innovation through Byod?," *Business & Information Systems Engineering*:Preprints), 01/01/, p 1.
Kramer, S., and Bradfield, J.C. 2010. "A General Definition of Malware," *Journal in Computer Virology*:2), p 105.
Lawrence, D., and Riley, M. 2014. "A Fresh Reason Not to Jailbreak Your Iphone." Bloomberg L.P., p. 37.
Leavitt, N. 2013. "Today's Mobile Security Requires a New Approach," *Computer*:11), p 16.
Miller, K.W., Voas, J., and Hurlburt, G.F. 2012. "Byod: Security and Privacy Considerations," *IT Professional* (14:5), pp 53-55.
Mont, J. 2012. "The Risks and Benefits of Employee-Owned Devices." Wilmington Compliance Week, Inc, p. 48.
Moreira, F., Cota, M.P., and GoncÌ¨alves, R. 2015. "The Influence of the Use of Mobile Devices and the Cloud Computing in Organizations," *New Contributions in Information Systems & Technologies*), 01//, p 275.
Nasim, R. 2012. "Security Threats Analysis in Bluetooth-Enabled Mobile Devices,"), 06/07/.
Neuman, W.L. 2006. *Social Research Methods: Qualitative and Quantitative Approaches*, (Sixth ed.).
Podhradsky, A.L., Casey, C., and Ceretti, P. 2012. "Managing Bluetooth Risks in the Workplace," *Wireless Telecommunications Symposium 2012*), 01//1/ 1/2012, p 1.
Potts, M. 2012. "The State of Information Security," *Network Security*:7), p 9.
Ruighaver, A.B., Maynard, S.B., and Warren, M. 2010. "Ethical Decision Making: Improving the Quality of Acceptable Use Policies," *Computers and Security* (29:7), pp 731-736.
Schulze, H. 2014. "Byod & Mobile Security Report."
Shumate, T., and Ketel, M. 2014. "Bring Your Own Device: Benefits, Risks and Control Techniques," *SOUTHEASTCON 2014, IEEE*), pp 1-6.
Son, J.-Y. 2011. "Out of Fear or Desire? Toward a Better Understanding of Employees' Motivation to Follow Is Security Policies," *Information & Management* (48), 1/1/2011, pp 296-302.
Souppaya, M., and Kent, K.A. 2012. "Guidelines for Managing and Securing Mobile Devices in the Enterprise: Recommendations of the National Institute of Standards and Technology," US Department of Commerce, National Institute of Standards and Technology.
Spencer, L. 2015. "16 Million Mobile Devices Hit by Malware in 2014: Alcatel-Lucent," in: *ZDNet*. www.zdnet.com.
Tan, M., and Aguilar, K.S. 2012. "An Investigation of Students' Perception of Bluetooth Security," *Information Management & Computer Security* (20:5), pp 364-381.
Tu, Z., Turel, O., Yuan, Y., and Archer, N. 2015. "Learning to Cope with Information Security Risks Regarding Mobile Device Loss or Theft: An Empirical Examination," *Information & Management* (52:4), pp 506-517.
Verizon. 2014. "2014 Data Breach Investigations Report."
Vishal, G., Deepak, S., and Lovekesh, D. 2013. "An Approach to Implement Bring Your Own Device (Byod) Securely," *International Journal of Engineering Innovations and Research*:2), p 154.
Von Solms, S.H., and Von Solms, R. 2009. *Information Security Governance. [Electronic Resource]*. New York, NY : Springer, 2009.
Wang, Y., Wei, J., and Vangury, K. 2014. "Bring Your Own Device Security Issues and Challenges," *11th Consumer Communications and Networking Conf (CCNC), 2014 IEEE* pp. 80-85.
Webb, J., Ahmad, A., Maynard, S.B., and Shanks, G. 2014. "A Situation Awareness Model for Information Security Risk Management," *Computers & Security* (44), 7/1/July 2014, pp 1-15.
Wood, A. 2013. "Byod in the Financial Sector: The Pros and Cons for End Users and the Business," *Credit Control* (34:2), 03//, p 72.
Zahadat, N., Blessner, P., Blackburn, T., and Olson, B.A. 2015. "Byod Security Engineering: A Framework and Its Analysis," *Computers & Security*), 6/26.