Research Project

Mitigating BYOD Information Security Risks

ISYS 90044 Minor Research Project in IS

(25 Points)

Supervisors

Dr Atif Ahmad

Dr Sean B Maynard

Submitted By

Daniel Alejandro Arregui

Student ID: 659157

Department of Computing and Information Systems

School of Engineering

University of Melbourne

Date: 4 November, 2015

Abstract

BYOD is a trend in organizations to allow employees, contractors and suppliers to use their personal devices in the workplace. Users can access electronic organizational resources from their tablets, smartphones, laptops, etc. The benefits of allowing BYOD in organizations are convenient for both employees and organizations. Employees will feel more comfortable employing their personal devices and organizations will save resources that should be used to purchase of electronic equipment for their employees. However, the confidentiality, integrity and ability of the information are at risk because individuals will have access to it employing their personal devices. The challenge to organizations is to keep that information secure. While BYOD is a well-defined and accepted trend in several organizations, there is little documentation to address the information security risks posed by BYOD. The following research, in the form of an extensive literature review, has defined a comprehensive list of information security risks that are associated with allowing BYOD in the organizations. This list will be used to evaluate five BYOD policy documents from different organizations to determine how comprehensively BYOD information security risks are addressed. Based on this evaluation, it will be identified which BYOD information security risks have been acknowledged and addressed by these organizations.

Declaration:

I certify that:

- *This thesis does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any university; and that to the best of my knowledge and belief it does not contain any material previously published or written by another person where due reference is not made in the text.*
- *The thesis is 8100 words in length (excluding text in tables, references and appendices).*

Daniel Alejandro Arregui

(Student ID# 659157)

Acknowledgements

I am very grateful to Professors Sean Maynard and Atif Ahmand for the excellent guidance given by them, without their help this thesis would not have been possible. I want also to thank Kimberly Meates, Cristina Browning and Ron Borrowing for their help proofreading some parts of this document.

Table of Contents

1 INTRODUCTION 7

2 BACKGROUND 10

2.1 Benefits of Allowing BYOD into Organizations 10

2.2 Security Risks Associated with BYOD 10

2.3 BYOD Strategy 11

3 RESEARCH METHODOLOGY 13

4 LITERATURE REVIEW 15

4.1 BYOD Definition 15

4.2 Literature Review Synthesis of Risks Associated with Allowing BYOD into Organizations 15

4.3 Description of the Risks Associated with Allowing BYOD into Organizations 17

5 RESULTS 27

5.1 Description of BYOD Policies Analysis 27

5.2 Summary of BYOD Policies Assessment Associated With Allowing BYOD into Organizations 30

6 DISCUSSION 32

6.1 BYOD Risks That Arise From User Behaviour 32

6.2 BYOD Risks That Arise From Connectivity Procedures 35

6.3 BYOD Risks That Arise From Organizational Management Practices 36

7 CONCLUSION 37

7.1 Research contribution 38

7.2 Limitations 38

7.3 Future Research 39

REFERENCES 40

List of Tables

Table 1: Synthesis of risks associated with allowing BYOD into the organization in the literature 16

Table 2: Summary of BYOD policies analysis associated with allowing BYOD into organizations 31

1 Introduction

Mobile devices are in high demand because they can be employed in multiple daily users' activities. Particularly with the proliferation of smart devices, more and more tasks are performed on these devices (Kang et al., 2015). Users have been introducing personal devices into working environments in a trend know as "Bring Your Own Device" (BYOD). It refers to allowing employees, contractors, and suppliers to use their mobile devices in the workplace. Users can access information technology (IT) resources from their organizations, such as information and applications using their tablets, smartphones, laptops, etc. (Astani et al., 2013). Employing personal devices for work purposes is convenient not only for users, but also for organizations. Users can be more productive accessing electronic organizational resources from inside and outside the workplace and organizations can reduce the cost of providing electronic devices to their employees (Donaldson et al., 2015, Zulkefli et al., 2015, Kang et al., 2015). Nevertheless, the challenge for organizations is to establish security practices on devices that are privately owned to protect organizational information (Zahadat et al., 2015).

Donaldson et al.(2015) comment that despite the growth of information security concerns from BYOD, organizations cannot stop this trend. They propose that, in order for organizations to move forward, users will need to access organizational information from mobile and personal computing devices (Donaldson et al., 2015). BYOD, rather than being an emerging trend, is already a well-adopted practice among different kinds of organizations (Moreira et al., 2015). A study presented by Gartner Inc. predicts that more than the half of organizations will require employees to use their personal devices for work purposes by 2017 (Willis, 2013). In another study conducted by CISCO, it was found that 75% of organizations are investing in IT infrastructure to allow a large number of employees to connect safely to organizational resources (CISCO, 2012). All these facts show that organizations are allowing the use of personal devices in the workplace.

Currently, in order to maintain the confidentiality, integrity and availability of the company's electronic assets, international best practices often are often employed to manage the overall information security in organizations (Von Solms and Von Solms, 2009). Information Security Governance (ISG), a subset of Corporate Governance, provides guidelines for protecting electronic organizational information against possible security incidents. These best practices offer high-level recommendations to board direction and executive management to establish information security procedures (Von Solms and Von Solms, 2009). The purpose of these procedures is to protect the information security in the organization. Nevertheless, according to Zahadat et al.(2015), specific best practices and guidelines to establish a BYOD program into organizations are not yet well defined. Although security experts have identified several BYOD risks that may arise from allowing personal devices into organizations, BYOD risks have not been adequately addressed by the Information Systems (IS) community (Tu et al., 2015a).

Without a comprehensive BYOD risk list, it is often difficult to assess the organizations' procedures that have been implemented to mitigate the risks. Therefore, this thesis will evaluate five BYOD policies, which are employed to mitigate the security risks associated with allowing BYOD into these organizations. This evaluation aims to address the main research question:

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

In order to evaluate BYOD policies, it is necessary to identify the information security risks associated with allowing BYOD into organizations. Consequently, the sub-question in this thesis is the following:

What information security risks arise from BYOD in organizations?

Assessing BYOD policies with respect to a comprehensive list of BYOD risks will identify the extent to which these risks are addressed in BYOD policies. Thus, the second sub-question is the following:

To what extent are information security risks addressed in BYOD policies?

This thesis will develop a comprehensive list of BYOD risk proposed by multiple information security publications. Consequently, this list will be used to evaluate five different BYOD policies employed to mitigate the security risks associated with allowing BYOD into these organizations.

The structure of this thesis is as follows – section two describes the benefits, information security risks and challenges that arise from allowing BYOD into organizations. This section also highlights the importance of BYOD policy as part of information security strategy to prevent security incidents in organizations. Section three presents the research methodology: how the research was conducted, analysed and the literature synthesized. Section four presents the BYOD literature review, which includes a BYOD definition, synthesis and description of information security risks associated with allowing BYOD into organizations. Section five presents the evaluation of five organizational BYOD mitigation procedures reflected in their BYOD policies. It also details the criteria applied to realize this evaluation. Section six summarizes the findings of BYOD policy evaluation. It identifies the BYOD risks that are commonly acknowledged and addressed by organizations. Section seven concludes the discussion, and outlines the implications, contributions and further research propositions.

2 Background

2.1 Benefits of Allowing BYOD into Organizations

Adopting BYOD in organizations is not only beneficial for users, but also for organizations. First, it provides both flexible working hours and working environment for users (Zulkefli et al., 2015). Instead of being restricted to a physical location, users can access the same electronic resources from almost any location (Zulkefli et al., 2015). They can access organizational resources from their home or on the road by connecting their devices to the Internet (Donaldson et al., 2015). Second, adopting BYOD reduces organizational operation costs (Kang et al., 2015, Zulkefli et al., 2015). If organizations allow their employees to use their personal devices, they eliminate the cost of providing hardware, software, and in most of cases, technical maintenance of mobile devices (Kang et al., 2015). Additionally, organizations do not need to provide basic training operation to the users because they are already familiar with the functionalities of devices (Kang et al., 2015). Third, BYOD provides better productivity and efficiency among users (Kang et al., 2015). For example, according to Köffer et al. (2015), the technological enterprise tools provided by organizations to their employees are often considered *"slow and cumbersome."* Therefore, organizations allowing their employees to use their smartphones and tablets can increase their productivity (Köffer et al., 2015, Kang et al., 2015). BYOD creates a positive change in the working environment because employees don't feel restricted using organization' equipment. Indeed, Köffer et al. (2015) claim that BYOD in some cases not only increases productivity, but also stimulates innovation among employees.

2.2 Security Risks Associated with BYOD

Despite all the benefits of implementing BYOD in organizations, it has also created risks for organizations (Webb et al., 2014). Son (2011) states that employing personal devices in organizations has contributed to over half of information security breaches occurring in organizations, as employees often fail to comply with information security procedures. Allowing BYOD into the organization creates potential security breaches

because users' devices will have access to the internal network and sensitive organizational information (Moreira et al., 2015). The challenge for organizations is to influence the use of personal devices, which are not part of organizational fixed assets, to protect organizational information security. Organizations need effective ways to preserve confidentiality, integrity and availability of sensitive information accessed or manipulated with the rise of personal devices (Zulkefli et al., 2015, Ahmad et al., 2006). Wang et al. (2014) describe that the most common organizational information accessed with BYOD are e-mails and corporate documents. 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 organizational information using personal devices. The leaking of information may cause substantial damage to the organization, such as financial loss, operational disruption, damage to the organization reputation and damage to the client's image (Cappelli et al., 2012, Ahmad et al., 2014).

2.3 BYOD Strategy

Zahabat et al. (2015) explain that the challenge for organizations is maintaining a balance between managing securing the cost of information and the damage that can result from not protecting it. Von Solms (2009) indicates that organizations must ensure "cost-effectiveness," meaning that resources should not be misused unreasonably over-protecting organizational information, but also should not expose the leak of information. Particularly, disruptions to BYOD usage can result when strict information security restrictions are implemented (Von Solms and Von Solms, 2004). Michael and Viega (2010) believe that the more restrictions and security features on mobile devices, the less friendly and useful the device will be for the user. This phenomenon is evident as people are used to friendly and easy-to-use applications to accomplish their tasks (Von Solms and Von Solms, 2004). BYOD security practices should not be an organizational barrier and make it difficult to accomplish business objectives (Zahadat et al., 2015). Ideally, the information security procedures should not affect users' ability to work on their devices.

Corporate Governance, assisted by Risk Governance, is responsible for maintaining the aforementioned balance. BYOD security best practices should be employed according to specific business necessities and current organizational conditions to ensure that the confidentiality, integrity and availability of the company's electronic assets (data, information, software, hardware, people, etc.) are maintained. ISG best practices suggest that organizations need to implement policies, organizational structures, procedures, processes, technologies and compliance enforcement mechanisms, which work together to ensure information security in the organization(Von Solms and Von Solms, 2009).

BYOD policy is one of the components that ISG needs to establish in order to mitigate the security risks associated with allowing BYOD into the organization. Gaff (2015) considers BYOD policy as a formal agreement between the employer and the employee. It contains the terms and conditions under which the organization grants access to its sensitive information. Gaff (2015) states that BYOD policy will protect the interest of the organization and its employees because it will ensure the security of not only sensitive organizational information, but also private employee information.

3 Research methodology

In order to answer the research question, "*How comprehensively are BYOD information security risks addressed in BYOD policy?",* this thesis develops a comprehensive list of BYOD security risks drawn from literature. The following are the databases employed to identify relevant articles: "University of Melbourne Discovery", "Science Direct", "Springer", "IEEE", "ProQuest", "Taylor & Francis Group", and "Google Scholar". The keywords used to find articles were: BYOD, security policy, BYOD issues and challenges, BYOD strategies, BYOD policies, bring your own device, have your own device, choose your own device, here is your own device, bring your own device (BYOD), mobile security, policy management, mobile phone security, mobile device management, mobile device management system (MDM), mobile security, mobile device management technology, etc.

From this search were identified around 120 academic articles. To determine if they were relevant or not to the objective of this research, the title and the abstract were read and also the content were skimmed through. In the end, 50 references were relevant and they were used to build the comprehensive list of security risks associated with allowing BYOD into the organizations.

The second part of this research used the BYOD risks identified in the literature and assessed 5 organisational BYOD policies to determine if organisations were addressing these risks. To identify the policies to be assessed we used Google search to search for BYOD or Mobile Device policies. We identified more than 40 policies. To diversify the types of organizations analysed in this research, five types of organizations were selected - two BYOD policies from private organizations, two from public organizations and one from a non-profit organization.

Finally, these policies were evaluated against the comprehensive list of security risks associated with allowing BYOD into organizations. The analysis was made comparing each BYOD policy statement of the five organizations 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 organization acknowledges and therefore tries to mitigate that risk. In the other hand, if none of the policy statements is addressing a specific risk it was concluded that the organization does not acknowledge and therefore not tries to mitigate that risk. It is worth mentioning that this analysis does not include the extent or how effective the organizations are mitigating BYOD risks. However, the assessment will identify the extent of those risks addressed in the five BYOD policies.

4 Literature review

4.1 BYOD Definition

Some information security experts provide a broad BYOD definition. For example, according to Gartner (2012), BYOD can include a large variety of electronic devices:

- Workstations devices (desktops, laptops, notebooks or netbooks) to mobile communication devices (phones, smartphones, tablets, touch enable devices)
- Portable storage media (USB memory sticks, memory cards, portable hard drives, floppy disks)
- Media recorders (digital cameras, audio recorders)

From this broad BYOD definition, the BYOD scope has been narrowed in this research. The main feature to consider an electronic device like a BYOD is that "*the users can generate knowledge work with them.*" Therefore, BYOD scope has been limited to any personal device which the following characteristics:

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

4.2 Literature Review Synthesis of Risks Associated with Allowing BYOD into Organizations

Table 1 identifies thirteen BYOD risks associated with allowing BYOD into the organizations. The risks have been identified in the literature and they are described with a respective list of references. Additionally, to identify the most significant risks, they have been grouped into three common areas related to BYOD usage:

- User behaviour
- Connectivity risks

- Organizational management practices

BYOD Perspective	BYOD Risks Description – List of References
User Behaviour	End-users of BYOD may configure their personal devices in a manner that exposes the organization to information security incidents.(Wood, 2013, Ketel and Shumate, 2015) 1. End-users may choose certain BYOD platforms (combination of hardware and operating system) that may expose the organization to information security incidents. (Armando et al., 2014b, Mont, 2012). 2. End-users may customize BYOD platforms insecurely; thereby, exposing the organization to information security incidents. (Gest, 2013, Lawrence and Riley, 2014, Kang et al., 2015, Gajar et al., 2013, Ketel and Shumate, 2015) 3. End-users may install malicious applications on the BYOD; thereby, exposing the organization to information security incidents. (Armando et al., 2014a, Shumate and Ketel, 2014, Ketel and Shumate, 2015). 4. End-users may engage in insecure behaviour while using BYODs allowing viruses, spyware and other malware infections to proliferate; thereby, exposing the organization to information security incidents. (Dang-Pham and Pittayachawan, 2015, Ketel and Shumate, 2015, Miller et al., 2012, Shumate and Ketel, 2014, Wang et al., 2014, Gajar et al., 2013). 5. End-users insecure handling of BYODs may allow unauthorized access to organization information by third parties; thereby, exposing organization to information security incidents. (Wang et al., 2014) 6. End-users may access sensitive organizational information without authorization onto their BYODs exposing organizational information security incidents. (Potts, 2012) (Miller et al., 2012, Wang et al., 2014, Tu et al., 2015b). 7. End-users may lost/stolen BYODs with sensitive organizational information, thereby, exposing organization to information security incidents. (Miller et al., 2012, Tu et al., 2015a, Shumate and Ketel, 2014, Ketel and Shumate, 2015, Howie, 2012, Hakhinian, 2012, Wang et al., 2014). 8. End-users may modify or eliminate accidentally sensitive organizational information from BYODs (Dong et al., 2015, Castro et al., 2013, Wang et al., 2014, Shumate and Ketel, 2014, Miller et al., 2012).
Connectivity	9. The information security of the organization could be exposed when BYOD users connect their devices to a public network (Vishal et al., 2013, Ketel and Shumate, 2015, Shumate and Ketel, 2014). 10. The information security of the organization could be exposed when organizations allow users connect to organizational local area network with their BYODs. (Potts, 2012). 11. The information security of the organization could be exposed when BYOD users connect their devices to a personal area network (Nasim, 2012, Tan and Aguilar, 2012, Podhradsky et al., 2012, Haataja, 2008).
Organizational Management Practices	12. 12. Organizations may not have the security control of personal devices that are accessing sensitive organizational information. (Vishal et al., 2013, Wang et al., 2014) 13. Organizations may not provide periodic training sessions to BYOD users about securely manage organizational information into their personal devices; thereby, exposing the organization to information security incidents. (Tu et al., 2015a, Ketel and Shumate, 2015)

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

4.3 Description of the Risks Associated with Allowing BYOD into Organizations

4.3.1 BYOD Risks that Arise from User's Behaviour

Risk number 1: *BYOD Device Selection*

Mobile device platforms that can be considered for BYOD are BlackBerry, Symbian, Apple's iOS, Android, and Windows Mobile. Nevertheless, according to a survey conducted by *Good Technology* during the first quarter of 2015, Apple's iOS dominates the enterprise market by 81% (Good-Technology, 2015). The next-most-employed platforms in an enterprise environment are Android with 15% and Windows Mobile with 4%(Good-Technology, 2015). These mobile operating systems support a broad range of applications that are unique to each platform. In the same way, all of these platforms have unique security models with strengths and weaknesses to counter security incidents (Gajar et al., 2013). To illustrate this, the open structure of the Android operating system, which may be customized by the user, makes it more susceptible to attacks than other mobile systems (Wood, 2013). According to McAfee Labs, 80% of the mobile malware affects mobile devices especially with Android operating systems (Shumate and Ketel, 2014). On the other hand, Apple's iOS security cannot run an MDM agent because of security restrictions in the operating system. Therefore, organizations need to evaluate the security risks that may arise from these platforms before initiating a BYOD program. They have to define the benefits and disadvantages in opting for particular models and establish strategies to counter security incidents that may arise from them. Subsequently, they should convey to users which platforms must be included and supported by the BYOD program to access sensitive organizational information.

Risk number 2: *BYOD Customisation*

"Jailbreaking", "root", and "unlock" are three popular procedures that users may execute on personal devices to remove vendors' configuration restrictions. These procedures permit users to customize their devices according to their requirements. For example, this procedure will permit users to install third-party applications

unavailable on official vendor stores or unlock carrier-locked devices to be used with other carriers (Lawrence and Riley, 2014).

Nonetheless, these devices may affect the information security of the organization if they are used as a BYOD. According to Kang et al. (2015), "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 in those devices run with administrator (root) privileges and have considerable control over device sensors and applications (Kang et al., 2015). In this way, it is critical for organizations to define whether or not organizations will permit in the BYOD program the use of "jailbreaking" or "root" devices.

Risk number 3: *Installation of Malicious Applications*

Normally, users customize their devices according to their preferences and needs. They use application markets, like Apple Store and Google Play, to browse thousands of applications addressing different customer needs. According to Armando et al. (2014b), during the application installation process, users tend to grant some permissions like allowing push notifications or location-based services. They put aside security considerations because of the benefits that will be received from the application (Armando et al., 2014b).

The security risk arises when various 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 along with a highly trusted banking application. The free application can be a malicious one that can sniff, modify, or steal inter-application messages and, therefore, compromise organizational information security (Ketel and Shumate, 2015). Ketel and Shumate (2015) claim that users are often unable to recognize which applications have a malicious functionality such as collecting sensitive information from them. Those applications may affect the information security of the organization, generate problems for data privacy issues, and affect

organizations and customers' reputations (Ketel and Shumate, 2015). Ketel and Shumate (2014) maintain that it is critical for organizations to control which applications can be installed on BYOD in order to protect the information security of the organization.

Risk number 4: *Insecure Operational Behaviour*

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 impacts personal computers, malware is affecting mobile devices with the difference that since 2014, the number of mobile devices has exceeded the number of desktops in the world. Drew (2012) considers that with this 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).

Malware is capable of generating a cyber-attack in the organization, interrupting business process, capturing valuable information like passwords, and deleting significant and sensitive information (Ketel and Shumate, 2015). As a result, malware becomes a serious threat to organizations, especially when their employees are accessing business resources with their mobile devices. Organizations must encourage the installation of anti-virus software on BYODs in order to prevent the proliferation of malware infection on personal devices.

Risk number 5: *Unauthorized Access*

According to a survey conducted by the security firm 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 realize the security risks that may arise from unauthorized access to their devices by third parties.

According to Cappelli et al. (2012) the use of password-protected screen savers is essential to decrease information security incidents in electronic devices. They reduce the likelihood of unauthorized users' accessing sensitive information storage on devices and use of organization applications. Cappelli et al. (2012) maintain that BYOD information security procedures must enforce password robustness, changing passwords periodically, activating automatic screen savers after an inactivity period and not disclosing device passwords with third parties.

Risk number 6: *Exposure of Sensitive Organizational Data*

Potts (2012) maintains that employees sometimes bypass intentionally the organizational security system, when they need an electronic enterprise resource to complete a task. The use of personal devices in organizations increases the probability of circumventing security procedures. According to Potts (2012), this action is considered to be an employee's misuse and abuse, but not as a malicious act. The user would not deliberately want to affect the information security of the organization (Potts, 2012).

However, this action could expose confidential organizational information that should be restricted to only a few users into the organization (Wood, 2013). BYOD provides not only a wider range of endpoints where the employees can access the organizational resources, but also a powerful way to distribute sensitive information without authorization exposing data confidentiality (Miller et al., 2012). He states that organizations found it difficult to keep control over information once it has moved to a mobile device (Miller et al., 2012). To illustrate, sensitive information, such as customer data, should be restricted to a few users into the company. However, with personal devices, that information can be easily copied and propagated to other devices (Wang et al., 2014). For this reason, organizations must establish the services and electronic resources that are allowed to access mobile devices(Miller et al., 2012). The organization must consider the BYOD risks and determine the services and

application that will be accessible from personal devices such as e-mail, calendars, contacts, electronic documents, etc.

Risk number 7: *Lost BYOD Devices*

According to Wang et al., both theft and loss are the primary concerns for allowing BYOD into organizations (Wang et al., 2014). BYODs are much more susceptible to be lost or stolen than desktop or laptop computers (Tu et al., 2015a). For instance, a survey conducted by Kaspersky (2013) found that one of every six users around the world had suffered damage, loss, or theft of their mobile devices. Approximately 70 million smartphones were lost in 2013 and every 53 seconds one laptop is stolen (Tu et al., 2015a).

As was reported in the same survey Kaspersky (2013), theft and loss of mobile devices expose the confidentiality of organizational information (e.g. emails, business documents, financial information, and banking passwords), and personal information (e.g. photos, videos, personal emails, social network passwords and email accounts). According to Tu et al., (2015a), even though the serious consequences may lead to compromising that information, this risk has not been addressed adequately by the IS community. They consider that the organization might lose its reputation, but also that the users may compromise their privacy information (Tu et al., 2015a). Therefore, Ketel and Shumate (2015) suggest that organizations need to implement a technology tool to wipe remotely or lock the device to protect sensitive organizational information from a lost or stolen device.

Risk number 8: *Data Integrity Loss*

Because of the normal operation of personal devices, users may accidentally modify or eliminate sensitive organizational information. According to Castro et al. (2013), users often employ BYOD for both personal and business purposes. In this way, 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 organizational information are: to prohibit downloading of organizational information into personal devices; backing up and performing changes of control of documents; or using a virtualization technique to separate organizational space from personal space in personal devices (Vishal et al., 2013).

4.3.2 BYOD Risks That Arise from Connectivity Procedures

Risk number 9: *Exposure in Public Networks*

Employees, while outside of the organization, usually want to remain connected with organizational electronic resources with their mobile devices. They have to use a public network, such as Wi-Fi hotspots, to access email, electronic documents, etc. A study predicts that the number of hotspot around the world is increasing exponentially and by that by the end of 2018, this number will reach 34 million (Wakefield, 2014). As a result, Wi-Fi hotspots are extremely attractive for users because they tend to be free, and they are common in public places, such as restaurants, malls, hospitals and airports.

According to Goldsborough (2011), the confidentiality and integrity of the information are exposed when users employ Wi-Fi hotspots. Souppaya and Kent (2012) claim that public Wi-Fi hotspots are susceptible to a man-in-the-middle attack (sensitive information can be intercepted and modified) and eavesdropping (the information is secretly revealed). The integrity and the confidentiality of the communication are at risk because users are often unable to recognize which hotspot is reliable or not (Souppaya and Kent, 2012). Ketel and Shunate (2015) suggest that organizations can mitigate this risk by connecting through public networks employing encryption of the communication with a virtual private network (VPN). Accordingly, the confidentiality and integrity of the communication will be protected.

Risk number 10: *Local Network Exposure*

Potts (2012) maintains that inside threats emerge when an offender wants to bypass organizational security system employing the local area network. He states that most of the time the offender has been granted access to the internal network because that person was considered a trusted employee, supplier or partner (Potts, 2012). One study conducted by Verizon, one of the largest US wireless communication service provider, found that 85% of the cyber attacks used the corporate network in 2014 (Verizon, 2014). Potts (2012) argues that insider attacks are difficult to prevent since they occur in the local area network (LAN) of the organization and employing a valid user profile.

Ketel and Shumate (2015) consider that organizations, before granting access to the internal network, must establish security characteristics of the mobile device. Devices that do not meet the security conditions created by the organization should be denied internal access (Ketel and Shumate, 2015). Antivirus software, mobile operating systems, and security configuration settings are some of the mobile characteristics that organizations need to consider while granting access to their internal network (Ketel and Shumate, 2015). Moreover, Verison's study suggests that organizations not only need to control employee-owned device access, but also review their users privileges to access sensitive data with their devices (Verizon, 2014).

Risk number 11: *Exposure in Personal Networks*

The most popular personal area network (PAN) that users can establish is the 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). Tan and Aguilar (2012) consider that because BT provides a broad range of services and applications, such as files transmission, synchronization of data, hands-free headset, input and output connections to peripherals, it has become a default feature of personal devices.

As a Wi-Fi communication technology, Bluetooth has security threats that can be extensively exploited. 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 organization. According to Podradsky (2012), there are many types of Bluetooth attacks that can introduce security vulnerabilities into the business domains, such as eavesdropping, man-in-the-middle attacks, message modification, denial of service (DoS) attacks and resource misappropriation. Haataja and Podhradsky et al. (2008, 2012) suggest that the corporate information that is commonly compromised by Bluetooth attacks are: social security numbers, bank accounts information, documents related to business, access to sensitive files, contact information, and passwords. Additionally, Podhradsky et al. (2012) maintain that in order to perform those attacks, it is not required to have an in-depth knowledge of software, nor of highly specialized equipment. There are many tutorials and open-source software available for free on the Internet in order to initiate a Bluetooth attack. Therefore, 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.

4.3.3 BYOD Risks That Arise From Organizational Management Practices

Risk number 12: *BYOD Remote Management*

According to Vishal et al. (2013), organizations not only need to establish BYOD policies, but also ensure that employee-owned devices comply with these policies. They affirm that the challenge for organizations is to manage remotely both a large quantity and numerous models of personal devices (Vishal et al., 2013). Moreover, organizations need to consider the fact that mobile users are renewing their equipment continually, which complicates organizational security management even more.

Therefore, Leavitt (2013) insists that organizations need a technological tool to ensure employees' compliance with BYOD policies. Mobile Device Management (MDM) is a primary information security tool for organizations to manage employee-owned devices (Leavitt, 2013). MDM permits organizations to monitor, manage, secure, and apply security policies on employee-owned mobile devices (Ketel and Shumate, 2015). According to a survey directed by Deloitte (2013), MDM is the most common tool to manage mobile devices in organizations with a 43% of acceptance between the surveyed organizations. 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). Then, employing MDM and NAC will perform functionalities such as, 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) etc.

Risk number 13: *BYOD Training*

As Leavitt (2013) has argued, end-users may engage in insecure behaviour while using BYODs. Some examples of insecure device operation are connecting to insecure public networks, employing weak or no passwords and customizing device software. Users, without appropriate information security knowledge, may perform those activities and social learning may contribute to this insecure behaviour (Leavitt, 2013). Tu et al. (2015a) 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 because it is not the most appropriate way to acquire information security best practices (Tu et al., 2015a).

According to Tu et al. (2015a), if BYOD users do not receive appropriate security information and training about an adequate way to operate their devices, social learning may affect information security negatively in the organization. For this reason,

Shumate and Ketel (2014) insist that the organizations 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 organization 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 organizational 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 organization).

5 Results

In this section, the five BYOD policies were analysed with the comprehensive list of security risks associated with allowing BYOD into organizations, which is detailed in the previous section (Table 1). These BYOD policies regulate user's procedures and practices so individuals can access securely electronic organizational resources. As consequence, BYOD policy statements attend to mitigate the security risks associated with allowing BYOD into organizations. The analysis in this section was made comparing each BYOD policy statement of the five organizations 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 organization 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 organization is not acknowledging and therefore not applying a mitigation strategy to mitigate that risk. The analysis of these five organizations is detailed in appendix 1.

5.1 Description of BYOD Policies Analysis

In order to determine if the organization's BYOD policy addresses the risks, each of the policy statements were compared one by one with the Table 1. The following section explains how this was accomplished:

5.1.1 BYOD Risks That Arise From User's Behaviour

Risk number 1: *BYOD Device Selection*

To ascertain whether or not organizations have considered the risks associated with BYOD insecure platforms, policy documents were analysed with statements around the guidance of BYOD platform selection.

Risk number 2: *BYOD Customisation*

To determine if organizations are addressing the risks related with insecure customizations of device platforms, BYOD policy statements were assessed looking for

terms such as “jailbreaking”, “rooting” and “unlock” devices. According to the results obtained, only one organization have not determined wether these devices will be appropriate for use within the organization.

Risk number 3: *Installation of Malicious Applications*

BYOD policies were inspected for statements that encourage the installation of applications from reputable sources on personal devices to avoid information security incidents with malicious applications. The analysis in this research reveals that only one organization has not addressed this risk in the BYOD policy.

Risk number 4: *Insecure Operational Behaviour*

To claim that an organization has recognized the risks related with the proliferations of viruses, spyware, and other malware infections, BYOD policies were examined looking for statements that encourage the installation of software against this malware and its proper licensing and continuous updating. According to the results achieved in this research, all the organizations have supported the installation of antivirus in personal devices.

Risk number 5: *Unauthorized Access*

To ascertain whether or not organizations have contemplated the risks associated with allowing unauthorized access to organizational information employing personal devices, BYOD policies were scanned looking for statements that encourage the use of authentication mechanisms. Those mechanisms can include the use of screen saver passwords or a biometric authentication mechanism. The findings of this research show that all the organizations have encouraged using authentication mechanisms on personal devices.

Risk number 6: *Exposure of Sensitive Organizational Data*

Policy documents were evaluated to determine whether organizations have considered the risks associated with unauthorized access of sensitive organizational information onto personal devices. The policy statements considered were the ones

with services and applications that can be accessible from personal devices, such as e-mail, calendars, contacts, electronic documents, etc.

Risk number 7: *Lost BYODs*

In order to consider that an organization has contemplated the risk related with end-users may lose BYODs with sensitive organizational information, BYOD policies statements were scanned looking for procedures to block or wipe the organizations information from a BYOD remotely.

Risk number 8: *Data Integrity Loss*

In order to address the risk associated with modifying or eliminating sensitive organizational information from BYODs, the statements that regulate organizational information in personal devices or perform change control of documents were looked in the BYOD policies.

5.1.2 BYOD Risks That Arise From Connectivity Procedures

Risk number 9: *Exposure in Public Networks*

To claim if organizations have anticipated the risks associated when BYOD users connect their devices to a public network, policy statements advising to encrypt the communication or to avoid using public hotspots were inspected.

Risk number 10: *Internal Network Exposure*

BYOD policies were inspected for statements that encourage the installation of MDM agents to monitor configuration settings or adopt a “secure device secure configuration” in order to avoid information security incidents in the organizational local area network.

Risk number 11: *Exposure in Personal Networks*

To argue that an organization has anticipated the risks when BYOD users connect their devices to a personal area network, policy statements were assessed with

recommendations to disable Bluetooth functionalities when it is not used, changing BT default devices names.

5.1.3 BYOD Risks That Arise From Organizational Management Practices

Risk number 12: *BYOD Remote Management*

To ascertain whether or not organizations have contemplated the risks related with the lack of control of personal devices that are accessing sensitive organizational information, BYOD policies were assessed for a description of tools such as mobile device management or network access controller.

Risk number 13: *BYOD Training*

In order to affirm that an organization has considered the risks associated with the lack of secure operation while accessing sensitive information from personal devices, policies were assessed to determine if training sessions were delivered by the organization to ensure that employees understood BYOD risks.

5.2 Summary of BYOD Policies Assessment Associated With Allowing BYOD into Organizations

It was assessed the five BYOD policies with respect to the list of security risks associated with allowing BYOD identified in section 4. Table 2 represent the summary of the findings obtained in this research. The table identifies the risks that have been acknowledged and addressed by these organizations.

SUMMARY BYOD POLICY EVALUATION						
BYOD perspective	**BYOD risks**	**Non-profit Organization**	**Health Organization**	**Educational Organization**	**Government Organization**	**Private Organization**
User behaviour	1. End-users may choose certain BYOD platforms (combination of hardware and operating system) that may expose the organization to information security incidents.	YES	YES	YES	YES	YES
	2. End-users may customize BYOD platforms insecurely; thereby, exposing the organization to information security incidents.	NO	YES	YES	YES	YES
	3. End-users may install malicious applications on the BYOD; thereby, exposing the organization to information security incidents.	YES	YES	YES	YES	NO
	4. End-users may engage in insecure behaviour while using BYODs allowing viruses, spyware and other malware infections to proliferate; thereby, exposing the organization to information security incidents.	YES	YES	YES	YES	YES
	5. End-users insecure handling of BYODs may allow unauthorized access to organization information by third parties; thereby, exposing organization to information security incidents.	YES	YES	YES	YES	YES
	6. End-users may access sensitive organizational information without authorization onto their BYODs exposing organizational information security incidents.	YES	YES	NO	YES	YES
	7. End-users may lost/stolen BYODs with sensitive organizational information, thereby, exposing organization to information security incidents.	YES	YES	YES	YES	YES
	8. End-users may modify or eliminate accidentally sensitive organizational information from BYODs.	NO	NO	YES	YES	YES
Connectivity procedures	9. The information security of the organization can be exposed when BYOD users connect their devices to a public network.	NO	YES	YES	YES	NO
	10. The information security of the organization can be exposed when organizations allow users connect to organizational local area network with their BYODs.	YES	YES	NO	NO	YES
	11. The information security of organizational can be exposed when BYOD users connect their devices to a personal area network.	NO	NO	YES	NO	NO
Management practices	12. Organizations may not have the security control of personal devices that are accessing sensitive organizational information.	YES	YES	NO	YES	YES
	13. Organizations may not provide periodic training sessions to BYOD users about securely manage organizational information into their personal devices; thereby, exposing the organization to information security incidents.	NO	YES	NO	NO	NO

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

Yes: it is addressed in BYOD policy
No: it is not addressed in BYOD policy

6 Discussion

The following section describes an analysis of the five BYOD policy documents and the information security risks discussed in the literature review. In addition, a critical evaluation of this analysis is included.

6.1 BYOD Risks That Arise From User Behaviour

Risk number 1: *BYOD Device Selection*

The findings in this research support those of Wood (2013), who underlines the importance of specifying BYOD platforms in policies. Different BYOD platforms have unique security weaknesses that may trigger information security incidents while accessing sensitive organizational information. Thus, it is not surprising that all the organizations evaluated in this research have established platforms that permit access to organizational information. Indeed, some of them have defined the platform, the model and the version of the operating systems that are included in the BYOD program. The more specific the models are in the policies, the better the control organizations can exert on those devices.

Risk number 2: *BYOD Customisation*

The BYOD statements to prohibit the use of “jailbreaking” and “root” devices to access organizational information are consistent with the information security recommendations suggested by Kang et al. (2015). Organizations evaluated in this research have recognized that those types of devices tend to be more vulnerable to viruses and insecure applications, which may expose the organization to information security incidents. However, none of the five organizations have considered “unlock” devices. In the same way that “jailbreaking” and “root” devices are a threat to the information security of the organization, “unlock” devices do not have the security controls that prevent access to information by insecure applications. Therefore, organizations should also exclude “unlock” devices to access organizational information.

Risk number 3: *Installation of Malicious Applications*

Shumate and Ketel (2014) acknowledge that malicious applications installed on BYODs can compromise organizational information. Similarly, most of the organizations in this research have recognized this risk by attempting to persuade users about the applications that can be installed on their personal devices. Most of them address this risk with policy statements that recommend only downloading applications from reputable sources. Nevertheless, it is not clear how the organizations will control the implementation of this policy statement. 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.

Risk number 4: *Insecure Operational Behaviour*

Ketel and Shumate (2015) have drawn attention to the fact that malware can generate a cyber-attack in organizations. Similarly, all the organizations in this study are aware of the information security threats that may trigger the proliferation of malware in BYODs. Policy statements in this research outline the use of anti-virus software on personal devices. In order to strengthen this policy, organizations should not only encourage the installation of anti-virus software on personal devices, but also provide licenses to users for free. This would motivate users to install anti-virus software on their devices, as this will protect both organizational and personal information.

Risk number 5: *Unauthorized Access*

In alignment with Cappelli et al. (2012) who recommends password-protected screen savers on personal devices, the five BYOD policy statements support using an authentication mechanism to secure access to the device. Additionally, organizations can strengthen the authentication mechanism with MDM functionality. To illustrate, the BYOD policy analysed in this research belonging to a Government organization (see appendix 1) performed an e-mail wipe after several password-failed attempts to access the device. Organizations that implement this technique will strengthen the confidentiality protection of the information that is stored on personal devices.

Risk number 6: *Exposure of Sensitive Organizational Data*

The tendency to protect sensitive information storage on personal devices of four of the organizations presented in this research is in line with Miller et al. (2012), who state the importance of defining the services and applications that will be accessible from personal devices. Some of the organizations have defined e-mail, office calendar and contact lists as services appropriate to be accessed from personal devices. However, these organizations have not mentioned in their policies how they are going to protect the access to non-authorized services and applications from BYODs.

Risk number 7: *Lost BYODs*

Wang et al. (2014) mention in their investigation that the loss of personal devices is one of the primary concerns when addressing information security risks related to BYOD into organizations. In alignment with this observation, this research revealed that almost all of the organizations evaluated have implemented a mobile device management solution to wipe organizational information from a BYOD remotely. However, organizations must additionally clarify in their BYOD policies whether this tool will wipe not only organizational information but also the entirety of information on personal devices.

Risk number 8: *Data integrity Loss*

Wang et al. (2014) also recognize in their article that a user may accidentally eliminate sensitive organizational information from personal devices. Similarly, three of the five organizations evaluated have recognized this risk and consequently prohibit the storage of organizational information in personal devices. However, none of the five organizations have considered employing a virtualization technique to separate organizational space from personal space in personal devices. This method would provide an alternative solution to manage both personal and business information in the same device without affecting each other.

6.2 BYOD Risks That Arise From Connectivity Procedures

Risk number 9: *Internal Network Exposure*

Only two BYOD policies in this research encourage VPN utilization while connecting to a public network from personal devices. These policy statements are coherent with Ketel and Shumate (2015) recommendations to protect organizational integrity and confidentiality of the information. However, one of these organizations has adopted a risky strategy to "make a risk-conscious decision" before connecting to a public network. It should be stressed that such procedures may compromise the security of the information because end-users may not have adequate knowledge to define whether a network is secure or not.

Risk number 10: *Internal Network Exposure*

Ketel and Shumate (2015) make further recommendations to protect the security of the information from insider attacks from personal devices. Two organizations in this research followed these recommendations by encouraging the installation of MDM agents in personal devices in their BYOD statements. MDM agent along with management software will control security configuration settings in personal devices such as configuration settings, software customization, and malware. However, in order to reduce the probability of an insider attack is required to integrate the MDM with a network access controller. In this way, organizations can grant BYOD users access to the local area network.

Risk number 11: *Exposure in Personal Networks*

Only one of the five organizations has mitigated the risks that are associated with personal area network attacks. In alignment with proposals by Podhradsky et al. (2012), this policy statement recommends disabling the Bluetooth service while it is not in use. The literature review recognizes the high impact of this risk to the information security of the organization. However, while developing this research, statistics were not found regarding personal area network attacks. The lack of

awareness in BYOD policies of this risk may be the result of its low occurrence probability.

6.3 BYOD Risks That Arise From Organizational Management Practices

Risk number 12: *BYOD Remote Management*

Leavitt (2013) states that in order to preserve the information security in organizations, it is necessary to manage and control remotely users' compliance with BYOD policies. Similarly, four of the organizations in this research have considered addressing this risk, and they have implemented an MDM solution before granting access to sensitive information of the organization. It was expected that most of the organizations have considered implementing a technological solution to efficiently manage and control a large quantity and numerous models of personal devices employed in the workplace.

Risk number 13: *BYOD Training*

Only one of the five organizations mentioned in their policy statements addressing the risk related to insecure behaviour while allowing BYOD into organizations as recommended by Tu et al. (2015a). The scope of BYOD policies is often limited to describe users' guidelines to mitigate information security risks. Therefore, it cannot be concluded that organizations have not considered this risk because it may be included in another document such as a IS strategic plan report of the organization.

7 Conclusion

This study began by answering the first sub-question, which was *"What information security risks arise from BYOD in organizations?"* From the existing literature, thirteen different BYOD risks were identified and were categorised into three different categories: user behaviour, connectivity procedures and management practices.

Subsequently, the second sub-question "*To what extent are information security risks addressed in BYOD policies?*" was proposed. In order to answer this question, separate analyses were conducted for each of the three different risks categories. First, it was found that organizations are aware of the risks related to "User Behaviour" and procedures to mitigate these risks. They recognize that current 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 indicates that there is some weakness in mitigating the risks associated with "Connectivity Procedures". In particular, some organizations have not recognized the information security incidents that may originate from an insecure connection to both a public and personal area network. Third, the research, regarding "Management Practices", suggests that organizations are relying on MDM as the main technological tool to monitor users' devices that are accessing organizational information. Due to the limitations of this research; however, it cannot be concluded whether organizations are considering the importance of providing training sessions to BYOD users.

The aforementioned analyses were conducted in order to answer the main research question, *"How comprehensively are BYOD information security risks addressed in BYOD policy?"*

7.1 Research contribution

The research presented in this paper proposes a list of risks associated with allowing BYOD into organizations, which was developed from existing literature. This list may be used as a checklist by organizations while setting up or improving a BYOD program. Moreover, researchers and practitioners can take these criteria into consideration when developing best practices or establishing BYOD frameworks.

The findings of this research imply that organizations are addressing the risks associated with user operation using appropriate information security tools. However, the information security best practices related to connectivity procedures need to be improved. Organizations need to be aware of information security incidents that may arise while connecting to different networks.

With the comprehensive list of BYOD risks and the findings of this research, organizations can build better information security procedures to manage information security risks associated with allowing BYOD into the workplace. They can use this information along with their organizational structures, procedures, processes and technologies to not only create better BYOD policies, but also more efficient information security procedures. These procedures must be adjusted to the information security necessities and business goals of the organization in order to be practical.

7.2 Limitations

The analyses and the BYOD risks described in this thesis are solely based on the existing literature. As BYOD is a fairly new research area in the IS community, it was necessary to build a BYOD risks list to evaluate information security procedures of organizations. BYOD policies were used to evaluate information security procedures to mitigate BYOD risks. However, more value benefit would have been gained by assessing BYOD policies in conjunction with IS strategic plans and interviews with IS

leaders. Due to time and resource constraints, these techniques could not be used to gather more information.

7.3 Future Research

In this research BYOD policies were evaluated against a comprehensive list of security risks associated with allowing BYOD into organizations. The evaluation was designed to identify statements in BYOD policies that are mitigating information security risks into organizations. As can be observed in appendix 1, in some cases, organizations applied different procedures to mitigate a similar information security risk. A further comparative study could be undertaken to identify the most effective procedures when addressing similar risks. This study should take into consideration that different organizations have unique information security priorities, depending heavily on their business goals. To achieve this, security procedures to mitigate information security risks should be evaluated within a specific industry sector.

References

AHMAD, A., BOSUA, R. & SCHEEPERS, R. 2014. Protecting organizational competitive advantage: A knowledge leakage perspective. *Computers & Security,* 42**,** 27-39.

AHMAD, A., RUIGHAVER, A. B. & TEO, W. T. An Information-Centric Approach to Data Security in Organizations. 2006. Piscataway, IEEE, 2255-2259.

ARMANDO, A., COSTA, G., MERLO, A. & VERDERAME, L. 2014a. Formal modeling and automatic enforcement of Bring Your Own Device policies. *International Journal of Information Security,* 14**,** 123-140.

ARMANDO, A., COSTA, G., VERDERAME, L. & MERLO, A. 2014b. Securing the "Bring Your Own Device" Paradigm. *Computer,* 47**,** 48-56.

ASTANI, M., READY, K. & TESSEMA, M. 2013. BYOD Issues and Strategies in Organizations *Issues in Information Systems,* 14**,** 195.

CAPPELLI, D., MOORE, A. & 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.

CASTRO, P. C., LIGMAN, J. W., PISTOIA, M., PONZO, J., THOMAS, G. S., WOOD, S. P. & BALUDA, M. 2013. Enabling Bring-Your-Own-Device using mobile application instrumentation. *IBM Journal of Research & Development,* 57**,** 1-11.

CHIN, E., FELT, A. P., GREENWOOD, K. & WAGNER, D. 2011. Analyzing inter-application communication in Android. *Proceedings of the 9th International Conference: Mobile Systems, Applications & Services***,** 239.

CISCO. 2012. Cisco Study: IT Saying Yes To BYOD. Available: http://newsroom.cisco.com/press-release-content?type=webcontent&articleId=854754.

DANG-PHAM, D. & PITTAYACHAWAN, S. 2015. Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. *Computers & Security,* 48**,** 281-297.

DELOITTE 2013. Understanding the bring your own device landscape.

DONALDSON, S. E., SIEGEL, S. G., WILLIAMS, C. K. & ASLAM, A. 2015. Enterprise Cybersecurity Capabilities. *Enterprise Cybersecurity*, 311.

DONG, Y., MAO, J., GUAN, H., LI, J. & CHEN, Y. 2015. A Virtualization Solution for BYOD With Dynamic Platform Context Switching. *IEEE Micro,* 35, 34-43.

DONOVAN, F. 2014. Employees fail to take basic steps to secure BYOD devices, data. *Fierce Mobile IT*, 1.

DREW, J. 2012. Managing Cybersecurity Risks. *Journal of Accountancy,* 214, 44-48.

GAFF, B. M. 2015. BYOD? OMG! *Computer,* 48, 10-11.

GAJAR, GHOSH, A. & RAI 2013. Bring Your Own Device (BYOD)- Security Risks and Mitigating Strategies. *JGRCS*.

GARTNER. 2012. *BYOD - Bring Your Own Device - Free Gartner Research* [Online]. http://www.gartner.com/it-glossary/. Available: http://www.gartner.com/it-glossary/bring-your-own-device-byod [Accessed 6 September 2015.

GEST, J. 2013. Managing BYOD. Smart Business Network, Inc.

GOLDSBOROUGH, R. 2011. Wi-Fi convenience comes with risks.

GOOD-TECHNOLOGY 2015. Good Technology Report: Apple's iOS still dominates the Enterprise Market by a Wide Margin with iPad Activations at 81%.

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)*, 232.

HAKHINIAN, M. 2012. Install mobile app safeguards. Haymarket Media Group.

HOWIE, J. 2012. *Bring Your Own Device (BYOD) Security _ Security content from Windows IT Pro* [Online]. Windowsitpro. Available: http://windowsitpro.com/security/bring-your-own-device-byod-security 2 Aug. 2015].

KANG, D., OH, J. & 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*, 165.

KASPERSKY 2013. One in Every Six users suffer loss or theft of mobile devices. Kaspersky Lab.

KETEL, M. & SHUMATE, T. 2015. Bring Your Own Device: Security technologies. *SoutheastCon 2015*, 1-7.

KÖFFER, S., ORTBACH, K., JUNGLAS, I., NIEHAVES, B. & HARRIS, J. 2015. Innovation Through BYOD? *Business & Information Systems Engineering*, 1.

KRAMER, S. & BRADFIELD, J. C. 2010. A general definition of malware. *Journal in Computer Virology*, 105.

LAWRENCE, D. & RILEY, M. 2014. A fresh reason not to jailbreak your iphone. Bloomberg L.P.

LEAVITT, N. 2013. Today's mobile security requires a new approach. *Computer*, 16.

MILLER, K. W., VOAS, J. & HURLBURT, G. F. 2012. BYOD: Security and Privacy Considerations. *IT Professional,* 14, 53-55.

MONT, J. 2012. The risks and benefits of employee-owned devices. Wilmington Compliance Week, Inc.

MOREIRA, F., COTA, M. P. & GONCÌ¨ALVES, R. 2015. The Influence of the Use of Mobile Devices and the Cloud Computing in Organizations. *New Contributions in Information Systems & Technologies*, 275.

NASIM, R. 2012. Security Threats Analysis in Bluetooth-Enabled Mobile Devices.

PODHRADSKY, A. L., CASEY, C. & CERETTI, P. 2012. Managing Bluetooth risks in the workplace. *Wireless Telecommunications Symposium 2012*, 1.

POTTS, M. 2012. The state of information security. *Network Security*, 9.

SCHULZE, H. 2014. BYOD & Mobile Security Report. Available: http://www.slideshare.net/informationsecurity/byod-mobile-security-report.

SHUMATE, T. & KETEL, M. 2014. Bring Your Own Device: Benefits, risks and control techniques. *SOUTHEASTCON 2014, IEEE*, 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, 296-302.

SPENCER, L. 2015. 16 million mobile devices hit by malware in 2014: Alcatel-Lucent. *ZDNet*.

TAN, M. & AGUILAR, K. S. 2012. An investigation of students' perception of Bluetooth security. *Information Management & Computer Security,* 20, 364-381.

TU, Z., TUREL, O., YUAN, Y. & ARCHER, N. 2015a. Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. *Information & Management,* 52, 506-517.

TU, Z., TUREL, O., YUAN, Y. & ARCHER, N. 2015b. Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. Elsevier B.V.

VERIZON. 2014. 2014 DATA BREACH INVESTIGATIONS REPORT. Available: http://www.verizonenterprise.com/DBIR/2014/reports/rp_dbir-2014-executive-summary_en_xg.pdf [Accessed 22 August 2015].

VIEGA, J. & MICHAEL, B. 2010. Mobile Device Security. *IEEE Security & Privacy Magazine,* 8**,** 11.

VISHAL, G., DEEPAK, S. & LOVEKESH, D. 2013. An Approach to Implement Bring Your Own Device (BYOD) Securely. *International Journal of Engineering Innovations and Research***,** 154.

VON SOLMS, B. & VON SOLMS, R. 2004. The 10 deadly sins of information security management. *Computers & Security,* 23**,** 371-376.

VON SOLMS, S. H. & VON SOLMS, R. 2009. *Information security governance. [electronic resource]*, New York, NY : Springer, 2009.

WAKEFIELD, J. 2014. *One wi-fi hotspot for every 150 people, says study* [Online]. http://www.bbc.com/news. Available: http://www.bbc.com/news/technology-29726632 [Accessed 22 Ausg 2015 2015].

WANG, Y., WEI, J. & VANGURY, K. Bring your own device security issues and challenges. Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th, 2014. IEEE, 80-85.

WEBB, J., AHMAD, A., MAYNARD, S. B. & SHANKS, G. 2014. A situation awareness model for information security risk management. *Computers & Security,* 44**,** 1-15.

WILLIS, D. A. 2013. Bring Your Own Device: The Facts and the Future. Available: https://l1.osdimg.com/remote-support/dam/pdf/en/bring-your-own-device-the-facts-and-the-future.pdf.

WOOD, A. 2013. BYOD in the Financial Sector: the Pros and Cons for End Users and the Business. *Credit Control,* 34**,** 72.

ZAHADAT, N., BLESSNER, P., BLACKBURN, T. & OLSON, B. A. 2015. BYOD security engineering: A framework and its analysis. *Computers & Security*.

ZULKEFLI, Z., SINGH, M. M. & MALIM, N. H. A. H. 2015. Advanced Persistent Threat Mitigation Using Multi Level Security – Access Control Framework.

Computational Science & Its Applications -- ICCSA 2015: 15th International Conference, Banff, AB, Canada, June 22-25, 2015, Proceedings, Part IV, 90.

Appendix 1

Non-profit Public Organization BRING YOUR OWN DEVICE POLICY			
Perspective	**BYOD Risks**	**Compliance**	**Comments**
BYOD user's behaviour	1. End-users may choose certain BYOD platforms (combination of hardware and operating system) that may expose the organization to information security incidents.	YES	The BYOD policy addresses the risk by **"4.3 Devices and Support.** Approved mobile devices include all versions of the iPhone running iOS 6 or above, iPad iOS 7.0.6 or and Windows phones (Nokia Lumia)."
	2. End-users may customize BYOD platforms insecurely; thereby, exposing the organization to information security incidents.	NO	The BYOD policy does not address the risk.
	3. End-users may install malicious applications on the BYOD; thereby, exposing the organization to information security incidents.	YES	The BYOD policy addresses the risk by ***"4.3 Devices and Support.*** *Does not have third-party software or applications that pose a threat to the organization's systems and networks or that could introduce application incompatibilities."*
	4. End-users may engage in insecure behaviour while using BYODs allowing viruses, spyware and other malware infections to proliferate; thereby, exposing the organization to information security incidents.	YES	The BYOD policy addresses the risk by ***"4. 1*** *Is properly protected against viruses, spyware, and other malware infections and that the system has properly licensed anti-malware software, when appropriate."*
	5. End-users insecure handling of BYODs may allow unauthorized access to organization information by third parties; thereby, exposing organization to information security incidents.	YES	The BYOD policy addresses the risk by ***"4.4 Security.*** *(BYOD device passwords must be a minimum of 8 characters/numbers.)"*
	6. End-users may access sensitive organizational information without authorization onto their BYOD exposing organizational information security incidents.	YES	The BYOD policy addresses the risk by ***"4.2 Acceptable Use*** *(-- Store or transmit illicit materials, including private, proprietary or confidential customer data unless this data is encrypted using ACSO approved methods and guidelines.-- Store or transmit proprietary information belonging to another company)"*
	7. End-users may lost/stolen BYOD with sensitive organizational information, thereby, exposing organization to information security incidents.	YES	The BYOD policy addresses the risk by ***"4.4 Security.*** *(The employee's device may be remotely wiped if the device is lost)"*
	8. End-users may modify or eliminate accidentally sensitive organizational information from BYODs	NO	The BYOD policy does not address the risk.
Connectivity procedures	9. The information security of organizational could be exposed when mobile users connect their devices to a public network	NO	The BYOD policy does not address the risk.
	10. The information security of organizational could be exposed when organizations allow users connect to organizational local area network with their BYODs.	YES	The BYOD policy addresses the risk by *"Devices must be presented to the ICT Department for provisioning and configuration of Wi-Fi and standard apps, such as ACSO software, Outlook and security tools, before they can be permitted access the ACSO Wi-Fi network. The installation of Mobile Device Management software (AirWatch) will monitor the compliancy of BYOD devices but will not be accessing or collecting personal data on the device."*
	11. The information security of organizational could be exposed when mobile users connect their devices to a personal area network	NO	The BYOD policy does not address the risk.

Organizational managing practices	12. Organizations may not have the security control of personal devices that are accessing sensitive organizational information.	YES	The BYOD policy addresses the risk by ***"2.1 AirWatch MDM****, 4.5 Device Reset and Data Deletion"*
	13. Organizations may not provide periodic training sessions to BYOD users about securely manage organizational information into their personal devices; thereby, exposing the organization to information security incidents.	NO	The BYOD policy does not address the risk.

Health Organization BRING YOUR OWN DEVICE POLICY			
Perspective	**BYOD risks**	**Compliance**	**Comments**
BYOD user behaviour	1. End-users may choose certain BYOD platforms (combination of hardware and operating system) that may expose the organization to information security incidents. (List of operating systems)	YES	The BYOD policy addresses the risk by *"3.2 The basic requirements are as follows, (as at September 2014) - Apple devices running iOS6 or later, and specifically;- iPhone 4 onward, iPad2 onwards, including the iPad Air and all versions of the iPad Min, Blackberry Phones"*
	2. End-users may customize insecurely BYOD platforms; thereby, exposing the organization to information security incidents.	YES	The BYOD policy addresses the risk by *"6.5 'Jailbroken' Apple devices are strictly forbidden from accessing the CCG infrastructure."*
	3. End-users may install malicious applications on the BYOD; thereby, exposing the organization to information security incidents.	YES	The BYOD policy addresses the risk by *"The MDM software monitors and manages access to approved applications, but the in-app activities of individual users are not monitored as the organisation deems this to be an invasion of personal privacy."*
	4. End-users may engage in insecure behaviour while using BYODs allowing viruses, spyware and other malware infections to proliferate; thereby, exposing the organization to information security incidents.	YES	The BYOD policy addresses the risk by *"IT detects a data or policy breach, a virus or similar threat to the security of the company's identifiable data and technology infrastructure."*
	5. End-users insecure handling of BYODs may allow unauthorized access to organization information by third parties; thereby, exposing organization to information security incidents.	YES	The BYOD policy addresses the risk by *"In order to prevent unauthorized access, devices must be passcode protected using the features of the device. The device must also lock itself with a password or PIN if idle for five minutes."*
	6. End-users may access sensitive organizational information without authorization onto their BYOD exposing organizational information security incidents.	YES	The BYOD policy addresses the risk by *"4.7 Employee use of CCG IT infrastructure and access via personally owned devices is as follows;* *- Calendars - Access permitted* *- Email - Access permitted* *- Contacts - Access permitted* *- Documents - Access currently not permitted"*
	7. End-users may lost/stolen BYOD with sensitive organizational information, thereby, exposing organization to information security incidents.	YES	The BYOD policy addresses the risk by *"Enable the 'Find my iPhone' app to their device to locate their device should it be lost or stolen."*
	8. End-users may modify or eliminate accidentally sensitive organizational information from BYODs	NO	The BYOD policy does not address the risk.
Connectivity procedure	9. The information security of organizational could be exposed when mobile users connect their devices to a public network	YES	The BYOD policy addresses the risk by *"The MDM software forces data traffic through an encrypted channel using a Virtual Private Network (VPN). The Information Commissioner's Office considers this step to be one of the most important in evidencing that an organisation has taken appropriate and reasonable measures of data security."*
	10. The information security of organizational could be exposed when organizations allow users connect to organizational local area network with their BYODs.	YES	The BYOD policy addresses the risk by *"4.5 Corporate identifiable data can only be created, processed, stored and communicated on personal devices running the CCGs chosen Mobile Device Management (MDM) client software. Devices not running MDM can connect to the CCG guest network providing an internet connection, but will not be granted access to the corporate infrastructure."*
	11. The information security of organizational could be exposed when mobile users connect their devices to a personal area network	NO	The BYOD policy does not address the risk.

Organizational managing practices	12. Organizations may not have the security control of personal devices that are accessing sensitive organizational information.	YES	The BYOD policy addresses the risk by *"Employees wishing to use their personal devices as per this policy will be required to download to their device an approved Third Party App (currently MobileIron). http://www.mobileiron.com/en/solutions/mobile-device-management This application enables the organisations IT provider to manage the CCG infrastructure and enable certain security features on the device."*
	13. Organizations may not provide periodic training sessions to BYOD users about securely manage organizational information into their personal devices; thereby, exposing the organization to information security incidents.	YES	The BYOD policy addresses the risk by *"Users are also supported via staff training and a quick reference usage guide."*

Educational Organization BRING YOUR OWN DEVICE POLICY			
Perspective	**BYOD risks**	**Compliance**	**Comments**
BYOD user behaviour	1. End-users may choose certain BYOD platforms (combination of hardware and operating system) that may expose the organization to information security incidents. (List of operating systems)	YES	The BYOD policy addresses the risk by *"1 If your device is an Apple iPhone or iPad, it is encrypted and protection is effective as soon as you set a PIN locking code."* and *"2 If your device is Android, there is an option to turn on whole-device encryption in its configuration settings. Other devices may or may not be encryptable. We recommend that you include your ability to encrypt as a factor when you are choosing your own devices."*
	2. End-users may customize insecurely BYOD platforms; thereby, exposing the organization to information security incidents. (Jail-break/Root)	YES	The BYOD policy addresses the risk by *"Configure your device to maximise its security. For example each new technology brings new enhanced security features. Take time to study and discover how to use these and decide which of them are relevant to you. Seek help from your IT support team if necessary."*
	3. End-users may install malicious applications on the BYOD; thereby, exposing the organization to information security incidents.	YES	The BYOD policy addresses the risk by *"Only download applications ('apps') or other software from reputable sources."*
	4. End-users may engage in insecure behaviour while using BYODs allowing viruses, spyware and other malware infections to proliferate; thereby, exposing the organization to information security incidents.	YES	The BYOD policy addresses the risk by *"Use anti-virus software and keep it up to date"*
	5. End-users insecure handling of BYODs may allow unauthorized access to organization information by third parties; thereby, exposing organization to information security incidents (C,I,A).	YES	The BYOD policy addresses the risk by *"Set and use a passcode (e.g. pin number or password) to access your device. Whenever possible, use a strong passcode. Do not share the passcode with anyone. Set your device to lock automatically when the device is inactive for more than a few minutes. Take appropriate physical security measures. Do not leave your device unattended. • If other members of your household use your device, ensure they cannot access University information, for example, with an additional account passcode. (Our preference is for you not to share the device with others.)The BYOD policy addresses the risk by "Use anti-virus software and keep it up to date"*
	6. End-users may access sensitive organizational information without authorization onto their BYOD exposing organizational information security incidents.	NO	The BYOD policy does not address the risk.
	7. End-users may lost/stolen BYOD with sensitive organizational information, thereby, exposing organization to information security incidents (C,I,A).	YES	The BYOD policy addresses the risk by " *Consider what the potential consequences could be for you, your friends or your family should your device become lost or stolen, and what protection configuration you want to put in place to prevent your data from being misused. Configure your device to enable you to remote-wipe it should it become lost."*
	8. End-users may modify or eliminate accidentally sensitive organizational information from BYODs.	YES	The BYOD policy addresses the risk by *"Make arrangements to back up your documents. Keep master copies of work documents on a University managed storage service."*
Connectivity procedure	9. The information security of organizational could be exposed when mobile users connect their devices to a public network	YES	The BYOD policy addresses the risk by *"Control your device's connections by disabling automatic connection to open, insecured Wi-Fi networks and make risk-conscious decisions before connecting."*
	10. The information security of organizational could be exposed when organizations allow users connect to organizational local area network with their	NO	The BYOD policy does not address the risk.

	BYODs.		
	11. The information security of organizational could be exposed when mobile users connect their devices to a personal area network	YES	The BYOD policy addresses the risk by *"Disable services such as Bluetooth and wireless if you are not using them."*
Organizational managing practices	12. Organizations may not have the security control of personal devices that are accessing sensitive organizational information.	NO	The BYOD policy does not address the risk.
	13. Organizations may not provide periodic training sessions to BYOD users about securely manage organizational information into their personal devices; thereby, exposing the organization to information security incidents.	NO	The BYOD policy does not address the risk.

Government Organization BRING YOUR OWN DEVICE POLICY			
Perspective	**BYOD risks**	**Compliance**	**Comments**
BYOD user behaviour	1. End-users may choose certain BYOD platforms (combination of hardware and operating system) that may expose the organization to information security incidents. (List of operating systems)	YES	The BYOD policy addresses the risk by *"The policy considers Apple/Android and Blackberry Devices."*
	2. End-users may customize insecurely BYOD platforms; thereby, exposing the organization to information security incidents. (Jail-break/Root)	YES	The BYOD policy addresses the risk by *"User agrees to maintain the original device operating system and keep the device current with security patches and updates, as released by the manufacturer. The user will not "Jail Break" the device (installing software that allows the user to bypass standard built-in security features and controls);"*
	3. End-users may install malicious applications on the BYOD device; thereby, exposing the organization to information security incidents.	YES	The BYOD policy addresses the risk by *"User will allow [AGENCY NAME] to enforce standard [AGENCY NAME] BES policies on the personal device, with the exception that the user will be allowed to download third-party apps to personal device;"*
	4. End-users may engage in insecure behaviour while using BYOD devices allowing viruses, spyware and other malware infections to proliferate; thereby, exposing the organization to information security incidents.	YES	The BYOD policy addresses the risk by *"Users must allow [AGENCY NAME] administrators to install Trend Micro security suite (firewall, antivirus, and web site protector applications) on their personal device; User will maintain anti-virus (AV) protection on the device ([AGENCY NAME] - provided or other). The AV software in use will be identified at the end of this document for review/approval by OIT; "*
	5. End-users insecure handling of BYOD devices may allow unauthorized access to organization information by third parties; thereby, exposing organization to information security incidents (C,I,A).	YES	The BYOD policy addresses the risk by *"User agrees that the device will not be shared with other individuals or family members, due to the business use of the device (potential access to government e-mail, etc); As a default, Notify-Link will be enabled to perform an e-mail wipe on the phone after 25 password failed attempts (please be advised that only e-mail on the device will be deleted); Users must comply with all [AGENCY NAME] password policies, including use of strong passwords, password expiration (6 months), and password history (3)."*
	6. End-users may access sensitive organizational information without authorization onto their BYOD exposing organizational information security incidents.	YES	The BYOD policy addresses the risk by *"Accessing [PRODUCT NAME] (e-Mail/Calendar) Services on BYOD"* and *"User will not download or transfer sensitive business data to their personal devices. Sensitive business data is defined as documents or data whose loss, misuse, or unauthorized access can adversely affect the privacy or welfare of an individual (personally identifiable information), the outcome of a charge/complaint/case, proprietary information, or agency financial operations. This excludes government e-mail that is protected through the various security controls listed below;"*
	7. End-users may lost/stolen BYOD with sensitive organizational information, thereby, exposing organization to information security incidents.		The policy addresses the risk by *"If the device is lost or stolen, the user will notify the [AGENCY NAME] Help Desk ([AGENCY HELPDESK PHONE] or [AGENCY HELPDESK EMAIL]) within one hour, or as soon as practical after you notice the device is missing. [AGENCY NAME] OIT will lock the device, e-mail on the device will be deleted, and notify-link services will be deactivated;"*
	8. End-users may modify or eliminate accidentally sensitive organizational information from BYODs.	YES	The BYOD policy addresses the risk by *"User will not download/transfer sensitive [AGENCY NAME] business data/documents to any non-[AGENCY*

			NAME] device."
Connectivity procedure	9. The information security of organizational could be exposed when mobile users connect their devices to a public network	YES	The BYOD policy addresses the risk by *"Users may only use [AGENCY NAME] approved and configured VPN client software to access [AGENCY NAME]'s VPN;"*
	10. The information security of organizational could be exposed when organizations allow users connect to organizational local area network with their BYODs.	NO	The BYOD policy does not address the risk.
	11. The information security of organizational could be exposed when mobile users connect their devices to a personal area network	NO	The BYOD policy does not address the risk.
Organizational managing practices	12. Organizations may not have the security control of personal devices that are accessing sensitive organizational information.	YES	The BYOD policy addresses the risk by *"The Notify-Link is a cloud based mobility solution that provides secure, real-time synchronization of email, calendar, and contacts to and from the Apple/Android devices. With Notify-Link, users have the ability to compose, reply, forward, or delete their email while mobile, as well as open a variety of email attachment formats. With the use of Notify Link Apps, business e-mails and appointments are downloaded and stored on the device, so additional security requirements are necessary."*
	13. Organizations may not provide periodic training sessions to BYOD users about securely manage organizational information into their personal devices; thereby, exposing the organization to information security incidents.	NO	The BYOD policy does not address the risk.

Private Organization BRING YOUR OWN DEVICE POLICY			
Perspective	**BYOD risks**	**Compliance**	**Comments**
BYOD user behaviour	1. End-users may choose certain BYOD platforms (combination of hardware and operating system) that may expose the organization to information security incidents. (List of operating systems)	YES	The BYOD policy addresses the risk by *"Current devices approved for Bring Your Own Device use are listed below along with the minimum system requirements:* *• Android 4 or higher Smart Phones and Tablets** *• iOS 5 or higher iPhones and iPads* *• Windows Mobile 8 or higher* *Devices below these specifications will not comply with our policies and therefore will not be supported."*
	2. End-users may customize insecurely BYOD platforms; thereby, exposing the organization to information security incidents.	YES	The BYOD policy addresses the risk by *"In addition to the above security settings, all users are expected to use their device in an ethical manner. Using your device in ways not designed or intended by the manufacturer is not allowed. This includes, but is not limited to, "jailbreaking" your iPhone or "rooting" your android device."*
	3. End-users may install malicious applications on the BYOD device; thereby, exposing the organization to information security incidents.	NO	The BYOD policy does not address the risk.
	4. End-users may engage in insecure behaviour while using BYOD devices allowing viruses, spyware and other malware infections to proliferate; thereby, exposing the organization to information security incidents.	YES	The BYOD policy addresses the risk by *"Upon receipt of the signed policy statement, the IS Service Desk will make an appointment with you to enable the mobile device management software on your device and in the case of Android devices to install anti-virus software on your device."*
	5. End-users insecure handling of BYOD devices may allow unauthorized access to organization information by third parties; thereby, exposing organization to information security incidents.	YES	The BYOD policy addresses the risk by *"You will not lend anyone your device to access Wiltshire Council information or use Wiltshire Council infrastructure. In order to access your Outlook e-mail, calendar and Lync, you will need to enter your network account password. This rotates every 90 days, as per domain policy. The policy will require a four digit pin to access your device. Your device or application will lock every 5 minutes requiring re-entry of your pin."*
	6. End-users may access sensitive organizational information without authorization onto their BYOD exposing organizational information security incidents.	YES	The BYOD policy addresses the risk by *"Device, Application or Data Access Limitations* *The IT Services covered by policy are:* *• E-mail – business e-mails are accessed and three days' worth are downloaded to the device, after which they are overwritten* *• Calendar* *• Contacts* *• Tasks* *• Lync"*
	7. End-users may lost/stolen BYOD with sensitive organizational information, thereby, exposing organization to information security incidents.	YES	The BYOD policy addresses the risk by *"If a security incident should occur, e.g. your device is lost or stolen or is infected with malware, you are required to inform the IS Service Desk immediately with details. Information Services reserves the right to wipe either Wiltshire Council data and applications or the whole device, if it is deemed necessary. This may impact other applications and data, such as the native Address Book data and any personal files on your device. Generally, the following guidelines apply: In the case of an Android device, the whole device will be wiped. In the case of an iOS device, corporate data and applications will be wiped."*
	8. End-users may modify or eliminate accidentally sensitive organizational information from BYODs	YES	The BYOD policy addresses the risk by *"You must not use your device to store corporate e-mails, files and data."* And *"User will not download/transfer sensitive business data/documents to any non-*

			device"
Connectivity procedure	9. The information security of organizational could be exposed when mobile users connect their devices to a public network	NO	The BYOD policy does not address the risk.
	10. The information security of organizational could be exposed when organizations allow users connect to organizational local area network with their BYODs.	YES	The policy addresses the risk by "Approval Process The device owner and user will raise a Service Request through the IS Service Desk by phoning 01225 718XX."
	11. The information security of organizational could be exposed when mobile users connect their devices to a personal area network	NO	The BYOD policy does not address the risk.
Organizational managing practices	12. Organizations may not have the security control of personal devices that are accessing sensitive organizational information.	YES	The BYOD policy addresses the risk by *"Upon approval of the application and installation of the mobile device management software, the device owner can connect to the Wiltshire Council infrastructure to access their Wiltshire Council e-mail, calendar and Lync at his own risk."*
	13. Organizations may not provide periodic training sessions to BYOD users about securely manage organizational information into their personal devices; thereby, exposing the organization to information security incidents.	NO	The BYOD policy does not address the risk.