VOL. 10, NO. 3, FEBRUARY 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences


www.arpnjournals.com

BRING YOUR OWN DEVICE ORGANISATIONAL INFORMATION SECURITY AND PRIVACY

Abubakar Bello Garba, Jocelyn Armarego, David Murray
School of Engineering and Information Technology, Murdoch University, South St, Murdoch, Australia
Email: A.Bello@murdoch.edu.au

ABSTRACT

BYOD is a growing trend in corporate environments, where employees bring their own devices to work. Factors that have led to the growing popularity of BYOD include the benefits of work flexibility, increased productivity, and efficiency of employees. Despite these benefits, there are concerns over information security and privacy. Since BYOD allows employees to access organisational data anytime anywhere, it is necessary to ensure the confidentiality and integrity of organisational information resources and assets. This paper will review BYOD, and information security and privacy in BYOD environments. Three different cases study organisational practices for BYOD security and privacy. Finally, advice on how to handle security and privacy in BYOD environments, using explicit policies, is presented. The paper will assist organisations, information technology and information security/privacy professionals to understand risks associated with BYOD, and policy development to mitigate them.

Keywords: Bring Your Own Device (BYOD), organisational perceptions, employees' behavioural intention, BYOD policies.

INTRODUCTION

The rapid advancement in information technology systems brought about the emergence of mobile computing, and later "Bring Your Own Device (BYOD)". The latter simply denotes private or personally owned information technology resources (such as computer hardware devices or software) that are used for business purposes (Niehaves, Koffer, & Ortbach, 2012). BYOD refers to the use of smart phones, tablets, and personal laptops which are not supplied or owned by the business organisation/employer, but are owned by the employees. Although the devices can either be mobile or non-mobile, some organisations allow employees to bring their own desktop devices to work, as long as the organisation can gain full control of that device. However, most organisations that have chosen to embrace BYOD prefer to allow mobile devices, because the organisation benefits from lower corporate cost, less technical training for employees, and increased productivity (Gens, Levitas, & Segal, 2011).

The drive behind BYOD can be traced back to the 1980s when many organisations identified the ideal employee as one with creativity, initiative and determination, who could get things done by any means across geographical borders (Dawson, 2012). This recognition by organisations caused employees to harness new and quicker ways of working, in order to prove competence to their employers. The launch of the iPhone in 2007, coupled with the increasing availability of wireless networks, re-initiated the idea of BYOD. The BYOD trend was first fully embraced in a corporate scenario in 2009 by Cisco, when they acknowledged the benefits of allowing employees to use their own devices to access network and business resources (Harkins, 2013). It was not until 2011 that the term BYOD came to the forefront, due to reported benefits by IT service providers.

Today, BYOD is common in corporate environments, and is re-organising ownership and control of organisational information systems and resources. Gens et al. (2011) noted that BYOD is changing the way businesses primarily operate, due to an increase in the number of organisations opening their networks and data to consumer handheld mobile devices, such as iOS or Android-based devices. According to a survey recently conducted by Cisco, approximately 95% of the participants said their organisation allows employees to use their personally owned devices for work in one way or the other (Cisco Networks, 2012). The survey also found that companies report an increase in employee productivity and efficiency. On this basis, many other companies began modifying their IT systems to integrate BYOD. Nevertheless, despite the benefits of BYOD, information security and privacy are realised as key concerns (Miller, Voas, & Hurlburt, 2012).

Information security in BYOD organisations

At corporate levels, information security concerns the protection of valuable assets of organisations. These assets are information that is either processed, recorded or stored, and owned by the organisation (Parker & Sarup, 1995). Information security concerns in BYOD are mainly centered on the confidentiality of data, since it is the organisational asset at risk. Other security concerns revolve around the risk introduced by mixing of personal and work data, and applications. Unlike organisation-owned devices that only have IT approved software on them, BYOD devices may have different applications downloaded and installed. There is also a chance for data exfiltration from one app to another on BYOD devices. Another matter of concern is the lack of adequate safeguards implemented on devices, retainment of confidential organisational data on devices by employees, and stolen, lost or hacked devices. These all could easily introduce malware and viruses that can infect devices and potentially lead to compromise and exposure of confidential data. Seven types of BYOD security threats are examined in the section to follow. Although many of

these threats exist, they are exacerbated by the mobility of devices.

1) Malware and BYOD: Mobile malware is a well-known threat to mobile devices and is rapidly growing as a result of BYOD adoption (Felt, Finifter, Chin, Hanna, & Wagner, 2011). The aim of malware is to break-in to a mobile device to spy or steal users' information, and damage the device. Mobile users are often deceived by attackers to install malicious software applications on their device. In some cases the hackers wait for opportunities when the mobile device is vulnerable to remotely access the device. Malware threats can consist of viruses, worms, Trojans, and botnets. It is noted in a report by Alcatel-Lucent (2013) that 11.6 million mobile devices are infected at any given time with malware. Malware deployed on mobile devices, has the ability to communicate non-stop with remote "command and control" sites, avoiding many corporate security measures.

2) Phishing, social engineering and BYOD: These attacks are well thought-out methods of deception that a hacker uses to collect or force mobile device users to send confidential information about themselves (Dodge, 2007). This can be used to trick BYOD users to download malware onto their mobile device. Other planned methods of deception can be email messages sent from persons recognised by the recipients asking them to reply with confidential information. Invitation to register personal details on a website, or persuading individuals to install software (malware) or to download an attachment which runs a hidden key-logger program to their BYOD device, is also another method used by hackers.

3) Direct attacks and BYOD: Hackers can use their intellectual skills to identify and analyse a particular mobile device system, and then launch attacks against it. The aim of the attack is typically to access, destroy, rewrite/modify, and extract confidential information, or to publicise the hackers for their exceptional talents. Direct attack with the intent of stealing, destroying or modifying confidential data can have huge effects on organisations, particularly those providing services to customers through the Internet. The well-known "Anonymous" have launched direct attacks on many organisations all over the world (Imperva, 2013). Some of their attacks compromised mobile devices to access or expose confidential financial information.

4) Data communication interception/spoofing and BYOD: These can be major threats to wireless networks used by BYOD devices. If a mobile user sends information over the Internet and it is intercepted, this becomes a serious concern, because of the risk that the data can be accessed, modified, or even destroyed. At the same time if a mobile device can be spoofed through a wireless network and deceived into sending information to a wrong recipient or receiving any kind of malicious data, this can result into an even greater security concern. Even if the network is encrypted, there is still the risk of someone (i.e access point owners or malicious insiders) having something physically attached to the network that could attempt to exploit a VPN tunnel. The continuous interception and spoofing of wireless data streams, and the use of deceptive ways to attract mobile device users to fraudulent wireless access points, have become a major threat to mobile technology itself, and a big security challenge to BYOD organisations (Ashford, 2012). As an example, a vulnerability called "Hole 196" has been discovered by security researchers in the Wi-Fi security protocol (WPA2) the majority of organisations use to secure their Wi-Fi networks (AirTight Networks, 2010). If organisations are connected via Hole 196, attackers could exploit this vulnerability to access personal data of others, as well as inject malicious threats into the wireless network.

5) Loss/theft of devices and BYOD: Mobile devices loss and theft is an increasing concern, as they are more likely to occur with mobile devices than traditional computers. While mobile devices have brought increased flexibility, they can be easily lost or stolen. Over 2 million mobile devices were stolen in the United Kingdom during 2005 (Braue, 2007). Similarly, it has been reported by the Australian Mobile Telecommunications Association that, almost every year, there is over 100,000 mobile devices reported stolen or lost (AMTA, 2013). When mobile devices are lost or stolen, valuable information can easily fall into the wrong hands, and may be used for fraudulent and other illegal purposes. In the majority of cases, the cost of the device to the owners or the organisations is nowhere as important as the value of the information stored on the device.

6) Malicious insider actions and BYOD: Government and other large business organisations have long been reporting how malicious insiders have exposed confidential data. Malicious insiders are one of the most challenging and problematic security issues to handle. Insiders have direct access to organisational information resources and networks; hence it is easier for them to steal, modify or destroy data. With BYOD, malicious insider threats are easier to realise, since mobile device users have access to organisational systems and resources anytime anywhere. BYOD employees who are malicious insiders have the possibility of executing malware attacks, phishing, data interception and spoofing, and easy theft of mobile devices can occur without notice in the organisations.

7) User policy violations and BYOD: A user policy violation is one of the easiest ways to expose a BYOD device to vulnerabilities. BYOD users do not require any malicious intent. Ignorance and carelessness, such as accessing and downloading untrusted web content that might contain malware, and disabling antivirus and firewall applications to increase speed and performance, can expose BYOD devices to vulnerabilities and threats.

The Citigroup financial company experienced a breach that exposed the data of over 5000 of their customers, due to one of their employee's using a peer-to-peer (P2P) file-sharing application from a BYOD laptop device on their network (Masin, 2013). Vance and Siponen (2012) noted that organisations are constantly faced with challenges of ensuring their employees comply with user policies. No matter how well developed and structured organisational policies are, they are rendered useless if not used adequately by employees.

Trend Micro (2012) reported that 93% of BYOD tablet computers and 84% of BYOD smartphones accessing corporate data do not have any form of security installed on them. BYOD does not only reduce organisational control of systems that employees conduct business on, but the mobile nature of devices makes it difficult for organisations to enforce policies and restrictions on employees working with BYOD devices. Moreover, contemporary studies by mobile security researchers indicate that attackers will continue to exploit vulnerabilities and issue threats to mobile devices to modify or destroy organisational data, particularly using malicious software (Goode, 2010). Traditional security methods and processes, such as host-based firewalls and content filtering, are becoming outdated against the emerging threats in mobile devices (BeyondTrust, 2013), mostly because they take up system resources. Hence, organisations need to make security and privacy of BYOD devices a top priority.

Information privacy in BYOD organisations

Information technology systems have long threatened information privacy. Technological advancements, like mobile computing devices and the boosted increase in computing power, have made it easier and cheaper for personal information to be compromised (Joinson & Paine, 2007). At an organisational level, information privacy is a critical problem for businesses, and is exacerbated by the introduction of BYOD. Organisational information privacy is the behaviour or attitude of firms towards protecting their information resources and their customers' personally identifiable information (Greenaway & Chan, 2005). There is a growing concern of how individuals' personal information is exposed by organisations either intentionally or as a result of their information systems being hacked due to usage of mobile devices by employees (Ashford, 2012).

In BYOD, information breaches are a key issue that the majority of organisations are facing worldwide (Ashford, 2012). As a result, organisations are implementing control measures that allow them to remotely wipe personal data on BYOD devices, force-install apps, and monitor device usages. Such measures can lead to private data retention, and privacy exposure. Also, from BYOD organisation employees' standpoint, the fact that they own their devices does not exempt the devices from forensic reviews in cases of litigation. This will require all personal information such as browsing history, pictures, movies/songs played and downloaded, personal contacts, calls, emails, text messages, and other social networking activities stored on the devices to be accessible. Employers who use mobile device management tools also have the ability to deliberately track and monitor employees' online activities and the real time location of their devices. According to a study by Fiberlink (2012), 82% of the employees surveyed considered tracking their devices as an invasion of their privacy. Another 76% of the employees disagree with their employers having access to applications installed on their devices. Over 80% showed concern about the possibility of their employers tracking websites and browsing history on their devices during off-work periods. More than 86% were worried about unauthorised remote wipes/deletions of their personal data. The legal implications are also worrying (Kaneshige, 2012).

As many organisations around the world continue to shift towards BYOD based environments, a considerable attention should be given to information privacy and security. A research survey conducted as part of a project undertaken through Murdoch University reveals the status quo of BYOD usage/perception in several organisations, and its potential impact on organisational confidential information resources and assets.

METHODOLOGY

The study employed a qualitative research methodology, applying a case study approach. Because of their ability to help study cases effectively, interview and web-based questionnaire instruments were developed and used to collect data. The surveys were administered at three organisations that consented to take part in the study, with a total of 62 participants taking part. Face- to-face in-depth interviews were held with 10 executive staff, and web-based questionnaires were administered to 52 general employees of the organisations. Detailed notes and the recorded interview sessions were transcribed. Descriptive statistics and thematic content analysis using NVivo and SPSS analytical software were two major techniques that have been extensively used to analyse the data collected from the study.

Case studies: Technology giant, educational institution, and financial organisation

This study underwent review by the Murdoch University Human Ethics Research Committee and was granted approval (No: 2013199). The study was conducted across three organisations from different industries related to technology, education, and finance, to determine BYOD proliferation, potential impact, and how the organisations are currently addressing BYOD issues.

The Technology Giant organisation has been among the first to embrace BYOD, and takes information security and privacy very seriously. Over 100,000 of their employees access the organisation's network through mobile devices, with 80% of them supplying their own devices. When loosening restrictions on personal devices,

the organisation realised new problems: employees' devices were full with applications they couldn't control.

The Educational institution is a leading research and higher educational organisation. Based on the nature of the organisation's operations and type of services delivered, it is heavily reliant on IT systems and allows BYOD, whilst considering information security and privacy to be critical elements.

The Financial organisation is highly dependent on IT systems and resources for conducting its day-to-day business. As a result, it allows BYOD in the belief that it enhances work flexibility and productivity. A key part of the organisation's goal is to maintain confidentiality in its affairs and its customers, citing information security and privacy its top priority.

Throughout the case studies, information was obtained on each organisation's operational activities, principally with the aim of understanding BYOD usage and perception, as well as BYOD information security and privacy in the organisations.

BYOD perception and usage patterns

The findings obtained across the three cases revealed that BYOD is both prevalent and highly utilised in the case organisations. Slight variations were observed in the degree of adoption and integration of BYOD due to the nature of their industry and operations, but, nevertheless, they all hold the same assumption that BYOD information security and privacy is an integral aspect to their businesses.

The Technology Giant and Financial organisation have specific device requirements for BYOD, but the Educational institution allows any device to access their network and resources. Table-1 illustrates additional findings which revealed that smartphones were the most highly used as BYOD across the three organisations, followed by laptops, then tablet PCs.

Table-1. BYOD devices usage frequencies in the organisations.

	Smartphone	Tablet PC	Laptop	Percent of cases
Technology giant	35.7%	28.6%	35.7%	100%
Educational institution	34.8%	34.8%	30.4%	100%
Financial organisation	42.9%	25.7%	31.4%	100%
Total average	37.8%	29.7%	32.5%	

Generation X, defined as workers between the age of 37-52 were more dependent on BYOD, followed by generation Y (18-36 years), and the baby boomer (over 52 years) generation. BYOD usage was seen to be a key element that impacted positively on the performance of the organisations and their employees' productivity. More flexibility to carry out work, increased information sharing and collaboration, and high level of convenience due to ability to work remotely was noted from users of smartphones, tablet PCs, and laptops. The users pointed out that: "BYOD gives us the choice to use devices and technologies which we are more familiar and comfortable with, making us very happy, and much more productive and efficient."

BYOD support

The Technology Giant organisation allocated the most resources to support BYOD. The organisation has developed and implemented BYOD policies, procedures, network and application management infrastructure that integrates into their overall ICT infrastructure. However, it is lacking a distinction between support for BYOD and the organisation owned devices, resulting in negative effects on users' experience. The respondents indicated that: "there is no differentiation between private and organisation owned devices, and any information on BYOD devices belongs to the organisation."

The respondents of the Educational and Financial organisations indicated that their organisation did not allocate adequate resources for BYOD, and have no specific policies, procedures, nor sufficient infrastructure for BYOD. These organisations do not provide any support to BYOD users and their devices.

BYOD information security

Threat of confidential information loss has emerged as the greatest BYOD information security concern for the three organisations, all citing that, securing corporate information is their primary goal. The Financial organisation officially allows BYOD only at mobile phone capability, but employees used laptops and tablet devices to access resources without the organisation's consent.

In the Technology Giant organisation, the objectives of its information security policy were defined with respect to BYOD. The organisation has adopted information security standards and tailored them to accommodate BYOD in order to ensure maximum security for its information resources and assets. Technical controls like mobile device management tools to manage and audit devices, and enforce security policies to ensure BYOD users are in full compliance, were also implemented. However, the organisation lacks a unified approach to auditing all BYOD devices. Some executives reported that their devices have never been audited, while others mentioned that their devices are constantly audited.

In contrast, both the Educational and Financial organisations have not defined their information security policy objectives with respect to BYOD, with the Educational institution specifically lacking confidence that its employees would comply with BYOD information security policies and procedures if they were in place. Although there is an indication that both organisations are in compliance with information security standards, it seemed that the standards have not been personalised to include BYOD. The organisations also appear to lack adequate technical controls to manage and audit BYOD

devices. However, the Financial organisation was noted to have a secured application management system for accessing corporate emails from BYOD devices. Table-2 provides the summary of the participants responses concerning the BYOD security controls and measures used in the organisations.

Table-2. BYOD security controls and measures used by the organisations.

	Technology giant	Educational institution	Financial organisation
Ensure employee personal devices are up-to-date (OS, and apps updates)	70.0%	0.0%	0.0%
Install security software (i.e antivirus, anti-malware)	80.0%	4.0%	0.0%
Encourage employees to immediately report lost or stolen devices	90.0%	8.0%	7.1%
Discourage employees from downloading unverified and untrusted applications	80.0%	12.0%	7.1%
Limit or block mobile device access to networks	40.0%	4.0%	42.8%
MAM (Mobile application management)	80.0%	0.0%	7.1%
Ensure employees activate lock screens	10.0%	0.0%	0.0%
No control measures used		72.0%	35.9%

The Technology Giant mandates the use of passwords, screen locks, and ensuring unverified and untrusted applications are not downloaded or installed by BYOD users. The Educational and Financial organisations do not facilitate the use of sufficient control measures by BYOD users, but the Financial organisation, in particular, tends to limit or block BYOD devices access from their networks. Additionally, both the Educational and Financial organisations lacked dedicated information security personnel for BYOD.

In all three organisations, participants were asked to identify BYOD security incidents that have occurred in their organisation. The Technology Giant and Educational institution admitted that BYOD devices were at least once or more often lost or stolen, infected with malware and viruses, subjected to network attacks, personal data loss, and data exposure through hacking. The Financial organisation reported no awareness of any BYOD security incidents that have occurred within their organisation.

BYOD information privacy

Although all three organisations have acknowledged that information privacy is important for BYOD, they all seem to lack sufficient knowledge of how to achieve privacy in BYOD environments. Management of all the organisations has at least indicated that they are in compliance with privacy principles and regulations. However, the organisations have not used these principles and regulations to implement any privacy frameworks that address issues relating to BYOD. Likewise, the majority of the employees across the organisations show no familiarity with what information privacy principles exist. Table-3 presents the employees' level of awareness of information privacy principles.

Table-3. BYOD employees knowledge of information privacy principles.

	Technology giant	Educational institution	Financial organisation
I don't know what privacy principles are	40.0%	52.9%	54.0%
I don't know what privacy principles exist in my organisation	60.0%	41.8%	23.0%
I am only aware of Australian privacy principles	0%	5.8%	23.0%

The results in Table-3 imply that the organisations have not educated employees on the level of BYOD privacy they are entitled to, as well as other associated privacy risks in BYOD. This is more evident in the Technology Giant organisation, because an executive indicated that the company treats all BYOD devices as organisation-owned, making employees' personal data their data. Additionally, due to full BYOD devices management and auditing in the Technology Giant organisation, there is clear visibility to their employees' personal data, leaving the employees with little or no entitlement to BYOD privacy. In contrast, the Educational

and Financial organisations' private corporate data can easily be exposed due to lack of support and control of BYOD devices.

The Technology Giant and Educational institution have admitted being victims of data interception, cyber-stalking, identity theft, and the exposure of confidential files and information. The Financial organisation showed no awareness of any privacy issues that have resulted from BYOD practices in their organisation.

BYOD information security and privacy knowledge

All the case study organisations have a common belief that information security and privacy for BYOD is the responsibility of everyone dealing with critical confidential information resources in their organisation. The BYOD information security knowledge in the Technology Giant organisation appears to be almost comprehensive. There was a positive perspective of sharing information security knowledge across the entire organisation. Most of the employees exhibited knowledge of who to contact when BYOD security and privacy incidents occur, as well as how to protect sensitive data in BYOD devices. Additionally, some level of security awareness programs and training for BYOD was present, although, the organisation seems to be lacking any formalities for BYOD privacy: there were no formal mechanisms for education and sharing knowledgeable information related to privacy.

On the other hand, the Educational and Financial organisations exhibited no signs of having security and privacy awareness programs and training concerning BYOD. Even though the employees of both organisations showed understanding of how to secure data on BYOD devices, several of them shared their BYOD devices passwords with work colleagues, friends and family, which is a major security issue of concern for the organisations.

In order to build in-depth knowledge about how to reduce potential BYOD security and privacy incidents across all the organisations, further data analysis was conducted in regards to Liability, Device Management, Monitoring and Tracking Devices, and Self-Incident Handling, to identify behavioural intention patterns of employees in each of the organisations. Figure-1 provides a summary of the results.

Likert-scale measurement levels using a minimum of 1 = strongly disagree, to a maximum of 5 = strongly agree, was used to understand the employees intention. The results showed that while there were similarities across all the organisations in terms of their employees' behaviour to accept the BYOD information security and privacy processes, there were also variations. In all the organisations, the employees have a tendency to accept liability for security and privacy incidents that occur through their BYOD devices, as well as having little or no desire to manage these incidents themselves. The Technology Giant organisation employees were neutral concerning full device management, but the Educational and Financial organisations employees to some extent disagree with BYOD devices being managed by their employers. The survey of the users revealed that 63% and 60% of the employees in the Educational and Financial organisation respectively, believed that the organisation should not be able to control their BYOD device. It is possible that there are differences in organisational culture in comparison to the Technology Giant. All respondents from all organisations disagree with monitoring and tracking of their BYOD devices.

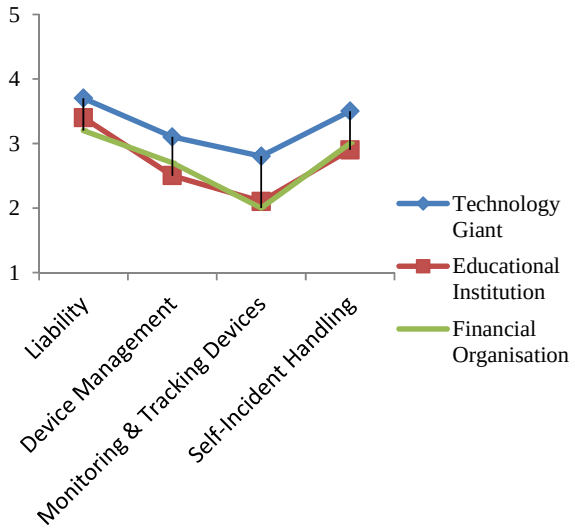

Figure-1. Employees behavioural intent for BYOD across the organisations.

Summary of case studies

In general, the Technology Giant organisation maintained a proactive approach to information security, and has implemented policies, technical controls, awareness programs and training for BYOD. However, the organisation is quite dormant when it comes to BYOD privacy, particularly for their employees. The Educational and Financial organisations seem to reserve a reactive approach, and therefore have inadequate security and privacy policies, controls, awareness programs and training for BYOD.

All three organisations share common issues relating to achieving information security and privacy in BYOD environments. The findings obtained revealed that, of the three organisations, only the Technology Giant has a high level of commitment towards BYOD information security, with no significant efforts been made by the Educational and Financial organisations towards BYOD information security. Moreover, all the three organisations have poor or no commitment of any kind to BYOD privacy.

Finally, the findings from the three organisations demonstrate that lack of sufficient and explicit BYOD policies, procedures, and awareness training programs can

influence the information security and privacy practices of organisations. Therefore, effective security and privacy measures comprising of policies, techniques, and awareness training programs specifically relating to BYOD need to be implemented by organisations to combat potential threats and vulnerabilities in BYOD environments. The next section highlights the importance of an effective BYOD security and privacy policy.

Managing BYOD using explicit policies

While many vendor-based technical solutions to manage BYOD exist, explicit policies and procedures that address security and privacy to support these technical solutions are lacking (Acronis, 2013), (Guan, 2012), (ZixCorp, 2013). Heimerl (2012), and Culnan and Williams (2009) stress that information security and privacy in an organisation should be a complex system which consists of technical systems, as well as policies, procedures, and other aspects that support the technical systems. Various research articles have emphasised information security and privacy policies as effective means of dealing with information security and privacy problems in organisations, as well as supplementing technical security and privacy controls.

An explicit and well-written BYOD policy can be the first step in bringing control to security and privacy in BYOD environments. BYOD users should follow some general guidelines when accessing and using organisational information resources. A starting point in drafting BYOD policies should involve the consultation of information security policies and standards manual, information privacy principles, mobile and portable computing policy, information asset ownership policy, and HR policies/code of conduct (IsecT, 2012). The BYOD policy detailed requirements should state that:

a. The organisation and BYOD employees share responsibilities for information security and privacy.
b. The policy does not affect organisational ownership of corporate information on BYOD devices, likewise the ownership of personal information by the BYOD users.
c. Jailbroken and rooted devices are not allowed to be used as BYOD. They are considered as security and privacy compromised devices, therefore exposed to threats and vulnerabilities.
d. Corporate information should only be accessed, modified, processed, stored and communicated on BYOD devices subject to successful device enrolment/on-boarding.
e. Information that is classified as highly confidential, as well as data in large quantity (i.e. 5 Gigabyte or more) is not permitted to be accessed, modified, or stored on BYOD devices.
f. BYOD employees should only use the methods of authentication such as user-ID, and passwords approved by the IT management of the organisation.
g. All BYOD devices must use a password lock-screen pattern that automatically locks the device when idle.
h. The organisation has the right to control its information on BYOD devices, and to limit or block BYOD devices access to corporate information resources and assets.
i. BYOD users are encouraged not to download, or install any malicious content or apps on their devices. In a case whereby a security or privacy incident occurs as a result of downloaded malicious content/apps, the device owner is fully liable.
j. Mobile antivirus software should be properly installed and fully running on all BYOD devices.
k. BYOD users are responsible for backing up their device data, but only using encrypted hard drives. Users are also liable for exposure of their backed-up data.
l. IT help desk may not always have the available resources to support different devices with different operating systems, therefore BYOD users will only be able to receive the support and expertise available at any given time.
m. Lost or stolen BYOD devices should be reported to the IT help desk, or the information security department within 24 hours maximum.
n. BYOD devices may be remotely wiped, usually with the consent of the owner when he/she reports his/her device is vulnerable/infected, or lost/stolen, or terminates his/her employment. Likewise, BYOD devices may be remotely wiped without the consent of the owner when IT suspects or detects a data or policy breach, a malware or virus threat, or an attack launched on/through the device.
o. To maintain BYOD users' privacy and avoid organisational management access to personal information on devices, BYOD users are advised to separate personal data from work data in separate folders/directories on their devices using identifiers.
p. BYOD users are required to take extreme caution not to infringe the organisation and other employees' privacy rights, by taking pictures or making audio/video recordings at work.
q. For all BYOD users, appropriate disciplinary action, which includes the termination of employment, can result in the event of non-compliance with the BYOD policy.

Security and privacy is a continuous process that requires attention, administration, review, and flexibility. For BYOD security and privacy to be successful in organisations, each organisational entity needs to understand and execute their duties adequately and in a timely manner. The information security and privacy management or personnel in organisations should be responsible for maintaining the BYOD security and privacy policies, including raising awareness/training among employees, and advising on counter-measures. In addition, they should be responsible for authenticating and authorising BYOD devices, as well as the monitoring of networks for unauthorised access, traffic and other threats. The IT Department should be responsible for managing corporate data security and privacy, and also configuring

and enforcing technical security and privacy controls on authorised devices to minimise the risks of data loss or exposure. The IT help desk should be responsible for providing support to BYOD devices on work-related matters only.

Overall, information security and privacy incidents affecting BYOD devices should be reported promptly to either the information security and privacy department/personnel, or the IT department or help desk. All employees using personal devices should be responsible for complying with BYOD policies at all times, and internal audits should be conducted regularly to assess compliance.

CONCLUSIONS

Preventing employees from bringing different types of devices into the workplace is difficult and will only worsen with computerised wristwatches and glasses proposed in the near future. With more than half of BYOD organisations reporting a variety of security and privacy threats, information and security polices require re-evaluation. Management, employees, policies, standards, procedures, and best practices, all play an important role in organisational information security and privacy. Organisations allowing or intending to permit BYOD must take a holistic approach with information security and privacy, and incorporate it diligently into each of their processes and methods. As discussed earlier, one of the major factors that can positively influence, and potentially reduce BYOD security and privacy incidents in organisations is a information security and privacy policy that accommodates BYOD. An understanding of how to weave different aspects of information security and privacy functions and processes to protect confidential information in BYOD environments is highly recommended for organisations.

REFERENCES

Acronis. (2013). Acronis Survey Shows Nearly 60 Percent of Companies are Vulnerable to BYOD Risks Retrieved 29th July, 2014, from http://www.acronis.com/en-us/pr/2013/07/17-08-07.html

AirTight Networks. (2010). WPA2 Hole 196 Vulnerability. Retrieved 6th May, 2013, from www.airtightnetworks.com/WPA2-Hole196

Alcatel-Lucent. (2013). Kindsight Security Labs: Malware Report – Q4 2013. Retrieved 26th July, 2014, from http://www.alcatel-lucent.com/solutions/kindsight-security

AMTA. (2013). The Mobile Phone Industry Statement. Retrieved 7th May, 2013, from www.amta.org.au/pages/amta/The.Mobile.Phone.Industry.Statement

Ashford, W. (2012). Nearly half of firms supporting BYOD report data breaches. Retrieved 27th July, 2014, from http://www.computerweekly.com/news/2240161202/Nearly-half-of-firms-supporting-BYOD-report-data-breaches.

BeyondTrust. (2013). Best Practices for Securing Remote and Mobile Devices. Retrieved 27th July, 2014, from http://www.beyondtrust.com/Content/whitepapers/Best-Practices-for-Securing-Remote-and-Mobile-Devices-WP.pdf

Braue, D. (2007). Lost mobile phones: a survival guide. Retrieved 7th May, 2013, from www.cnet.com.au/lost-mobile-phones-a-survival-guide-339276173.htm

Cisco Networks. (2012). Cisco Study: IT Saying Yes to BYOD, Targeted News Service. Retrieved from http://0-search.proquest.com.prospero.murdoch.edu.au/docview/1013951859? accountid=12629

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: Lessons from the choicepoint and TJX data breaches. MIS quarterly, 33(4), 673-687.

Dawson, K. (2012). Origins of BYOD Suggest a Way Forward. Retrieved 21st May, 2013, from www.businessagility.com/author.asp?section_id=1671&doc_id=237434

Dodge, R. C. (2007). Phishing for user security awareness. Computers & security, 26, 73-80.

Felt, A. P., Finifter, M., Chin, E., Hanna, S., & Wagner, D. (2011). A survey of mobile malware in the wild. Paper presented at the Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices.

Fiberlink. (2012). Harris Survey Exposes Concerns About Employee Privacy for BYOD: Fiberlink-commissioned Poll Shows Nearly 80% of Business Users Alarmed about Employer Oversight into Location Tracking, Apps and More. Retrieved 29th July, 2014, from http://www.maas360.com/news/press-releases/2012/harris-survey-exposes-concerns-about-employee-privacy-for-byod/

Gens, F., Levitas, D., & Segal, R. (2011). 2011 Consumerization of IT Study: Closing the "Consumerization Gap". Framingham: International Data Corporation (IDC).

Goode, A. (2010). Managing mobile security: How are we doing? Network Security, 2010(2), 12-15. doi: http://dx.doi.org/10.1016/S1353-4858(10)70025-8.

Greenaway, K. E., & Chan, Y. E. (2005). Theoretical explanations for firms' information privacy behaviors. Journal of the Association for Information Systems, 6(6), 171-189.

Guan, L. (2012). Established BYOD management policies needed. Government News, 32(2), 9.

Harkins, M. (2013). Mobile: Learn from Intel's CISO on Securing Employee-Owned Devices. Retrieved 21st May, 2013, from www.govinfosecurity.com/webinars/mobile-learn-from-intels-ciso-on-securing-employee-owned-devices-w-264.

Heimerl, J.-L. (2012). The Evolution of Information Security. http://www.securityweek.com/evolution-information-security

Imperva. (2013). Imperva's Hacker Intelligence Summary Report: The Anatomy of an Anonymous Attack. Retrieved 3rd May, 2013, from http://www.imperva.com/docs/hii_the_anatomy_of_an_anonymous_attack.pdf

IsecT. (2012). Information security policy: BYOD (Bring Your Own Device). Retrieved 2nd August, 2014, from http://www.iso27001security.com/ISO27k_Model_policy_on_BYOD_security.pdf

Joinson, A. N., & Paine, C. B. (2007). Self-disclosure, privacy and the Internet. Oxford handbook of Internet psychology, 237-252.

Kaneshige, T. (2012). BYOD Stirs Up Legal Problems. Retrieved 29th July, 2014, from http://www.cio.com/article/2396210/byod/byod-stirs-up-legal-problems.html

Masin, J. (2013). Peer-To-Peer (P2P) File Sharing Risks. Retrieved 7th May, 2013, from http://www.securedocs.com/blog/2013/02/peer-to-peer-p2p-file-sharing-risks/