Does BYOD increase risks or drive benefits?

Ashwin Pillay
Department of Information Systems,
University of Melbourne
Parkville, Victoria.

Eric Nham
Department of Information Systems,
University of Melbourne
Parkville, Victoria.

Gloria Tan
Department of Information Systems,
University of Melbourne
Parkville, Victoria.

Harrik Diaki
Department of Information Systems,
University of Melbourne
Parkville, Victoria.

Samanthi Senanayake
Department of Information Systems,
University of Melbourne
Parkville, Victoria.

Saurabh Deshpande
Department of Information Systems,
University of Melbourne
Parkville, Victoria.

Abstract

This paper looks at the benefits and risks associated with bring your own device (BYOD), a practice that is becoming common to many organisations. Literature reviews of established academic journals were conducted to illustrate key points, arguments, and supporting evidence to draw conclusions.

The paper has found that BYOD is an inevitable part of modern organizations' business practice. Its adoption will continue to rise due to its effectiveness in supporting business operations. The paper also found that there are substantial risks in BYOD that can be harmful to organizations, and thus its ability to control BYOD is crucial in the prevention and mitigation of these risks.

The paper contributes to current literature by emphasizing that in order to fully realize the potential ongoing benefits of BYOD, control strategies must be applied, and that the human factor must be taken into account as it plays a pivotal role in the effectiveness of these security measures.

Introduction

Bring Your Own Device (BYOD) is the "strategy that allows employees, business partners and other users to use a personally selected and purchased client device to execute enterprise applications and access data" (Gartner 2013). The most commonly used personal mobile devices for BYOD include smart phones, tablets, and laptops.

The trend of BYOD stems from the perception that it can improve the agility and productivity of work practices amongst employees in an enterprise. These benefits result in the continuous uprise of BYOD practice but can also lead to the introduction of security breaches. The risks associated with BYOD can range from interoperability among devices to sensitive data leakage. A Deloitte (2013) survey found that the increased usage of mobile devices in the workplace ranked as the second biggest security risk among organizations. These risks, if not properly assessed and managed may result in harmful consequences to the organisation's business. This paper examines both the benefits and the risks of BYOD practice in depth to determine whether or not BYOD would be a suitable solution for an organisation. The scope of this paper is limited to security risks associated with BYOD.

For the preceding reasons, the research question that the paper explores is:

> *"Does BYOD increase risks or drive benefits?"*

In order to answer this question, the paper begins with two major sections; each section outlines the benefits and risks of BYOD based on literature reviews of academic journals and industry papers. In addition, a discussion on security countermeasures was included. These countermeasure strategies were based on the risks mentioned in the main discussion and will be formed in respect to the three key areas of risk management, which are: control, mitigation, and prevention. The paper also explores the limitations and further research that can be taken to further develop the topic of security risks of BYOD.

Literature Review

BYOD Benefits

Costs Savings

The key reason why many organisations have moved into a BYOD environment is because there are strong cost savings in the decline of hardware investment (Wood 2012). BYOD enables the organisation to shift the investment costs of desktop hardware onto their employees. Furthermore employees have a desire to upgrade their hardware aggressively speeding up the adoption of cutting-edge technology (Calder 2013). The running and lifecycle replacement costs of the hardware are no longer paid by the organisation (Wood 2012), likewise it is common for the employee to pay most of the running costs of their purchased preferred device (Calder 2013).

Support costs are further reduced in BYOD implementations. According to Rains (2012), research conducted by HDI Research Corner exhibited that over 40 percent of 844 organisations in 35 industries required their employees to contact the vendor directly for personal device support. Only 35 percent of the organisations surveyed operated internal support centres for BYOD devices.

Although the cost of hardware acquisition, refresh and support may be reduced, the cost of security will increase as seen in a survey conducted by Forrester Consulting which included 202 BYOD decision-makers in enterprises in the UK, US, France and Germany. The survey shows that although the expense of purchasing and supporting end user devices is reduced when BYOD was implemented, the costs of "application security, back-end infrastructure and regulatory compliance tends to increase" (SC Magazine 2012). Therefore, it is argued that the costs reductions in implementing BYOD are only a fake face value; when the costs of ensuring the security of company information will increase.

Accessibility to data

Mobile technologies have been recognised to improve an employees' productivity (Ahuja 2012). BYOD mobile devices have enabled employees to access company data without being restricted to a fixed location. The improved communication and accessibility to data allows organisations to improve the products and services offered and to increase their value to the customers (Calder 2013; Management Services 2012). BYOD drives business growth through empowering employees to access the corporate network around the clock from their personal devices (Tzoumas 2013). With an unparalleled level of connectivity between employees and the office, real time communication dramatically increases operational efficiency (Management Services 2012).

Employee Satisfaction

The BYOD policy also allows employees to choose the technologies which best suits their roles. For example, marketing executives would use a MacBook, whereas Sales Representatives would most likely use a tablet for recording meeting notes. Thus, this can create a greater satisfaction for employees towards working with IT rather than against it (Mont 2012).

When a BYOD policy is implemented in an organisation, employees tend to look after their devices to a higher degree, as there is often a greater sense of personal ownership involved, leading to hardware cost reduction and maintenance (Mont 2012). This leads to a higher productivity as workers are more comfortable with devices they are at ease working with. A recent study by Acorn Marketing and Research commissioned by VMware titled the "New Way of Work Study" found that 64 percent of employees in multinational companies across the Asian and Australian region reported that their productivity had increased due to efficiency and ease of use by selecting personal devices for work purposes which in turn lead to greater employee happiness and satisfaction (Mont 2012).

Employee Productivity

According to the latest research by Cisco, more and more organisations are now adopting a BYOD practice, in which 95 percent of organisations allow employee-owned devices in the workplace (as cited in Mont 2012). Employees working off their personal devices are more likely to work outside office hours, who could deal with basic administration tasks, thus resulting in quicker turn around on daily employee action items. Employees today are also much more technically savvy than ever before, hence BYOD is a preferred choice of employees. Stieglitz and Brockman (2012) found that, "mobile enterprises can increase workforce productivity by providing employees with real-time access to data in various situations (e.g., while in business meetings) and by faster provisioning of ad hoc communication possibilities." Another survey by Capgemini Consulting also highlighted that employees who use mobile devices for both work and personal added an extra 240 more work hours than employees who did not (Capgemini 2011). Supporting these results, are views of CIOs and Chief Security Officers such as David Ottenheimer, president of information security at Flying Penguin who states, "If you give employees a workspace they are able to own and run with, in turn employees will be more productive" (Mont 2012).

BYOD Risks

Loss of data

One of the most important risks associated with BYOD is loss of data due to devices being lost or stolen from or outside the work place. The ease and convenience offered by the size of the smart devices makes them easy to drop or misplace (Calder 2012). With almost 2.4 billion units of smart phones and tablets sold in 2013 (Gartner 2013), these devices are becoming popular targets for thieves because of their high value and compact size.

Additionally, according to a UK based study when employees change their mobile phones or sell the current device to upgrade to a newer one, confidential and sensitive information is passed on to unauthorised users (McAfee 2012). Experts suggest lost or stolen BYODs is the number one risk not only because data is lost, but also because data is lost at crucial times thus hindering them from competitive advantage over others (Gest 2013).

Another critical factor about data leakage associated with BYOD is the difficulty of detecting the leakage before it's too late. This prevents the opportunity of taking counter measures to minimize the impact, which might be possible at the early stage of diagnosis. Gwen Hassan, manager of corporate compliance for Navistar claims that this problem intensifies when executives use their own devices to handle company data who do not understand the technology thus they do not know where the gap exists (Mont 2012).

Lack of control over data and devices

Employees' misuse and abuse of company IT resources is increased in a BYOD environment. Employees intentionally bypass the security restrictions (e.g. password protection, IT practices and policies) for the convenience of using their own devices thereby compromising the security of company IT resources. Because of this, when personally owned devices that have bypassed these policies set by the organisations are stolen, the data cannot be wiped out remotely (Potts 2012). On the other hand, organizations find it difficult to audit and monitor whether the authorized employee is using company information on BYOD as opposed to someone else (Gatewood 2012). Moreover, tech savvy employees can bypass proxy servers and use corporate resources to access sites, which are not permitted in company network such as Facebook.com. Users may install applications to enable remote access to work PC with the intention of working from home. Though these instances may not mean to harm it might open the corporate network up to attack (Potts 2012) which can then "potentially allow unknown users to access sensitive company data" (Tzoumas 2013).

Organisations that have adopted BYOD have the underlying threat of losing the control over their data if they are being accessed outside the organisation jurisdiction or network. Employees tend to use cloud to store data and fail to realise the implications on data control and ownership. Employees of around 30% of organisations worldwide use cloud services such as Dropbox, iCloud, and Google Docs to store and access data (McAfee 2012). Organisations fear the auto-synchronisation offered by Apple to its iCloud via iTunes as one of the serious data control violation methods. Owing to the synchronisation the "document is no longer under the organisation's control" (Howie 2012). Furthermore, emails that are accessed over the cellular network via a BYOD are no longer in the organisation's control and are prone to phishing attacks (Phifer 2013).

IBM recently banned employees from using personal devices to view company data because of its concern over leakage of data citing that "Apple's data pipeline between users and the voice-activated personal assistant – Siri could compromise security" (Mont 2012). According to Rick Dakin, CEO of IT Governance Company, it is becoming "far too common" for executives to use mobile devices such as iPads full of sensitive sales data on an airplane's "insecure WiFi" (Mont 2012).

Vulnerabilities due to installation of malicious software

According to TendLabs 5,000 malicious Android apps were found in the first quarter of 2012 increased two folds in just one month of the second quarter. The research also states that these malicious apps were downloaded 700,000 times before they were removed by Google from Google Play (Information Management September/October 2012). These malicious apps are downloaded by employees for personal use, which creates vulnerabilities in the devices, making the devices prone to attacks. Employees tend to "feel entitled to do as they please, including removing security features" from their devices (Gest 2013).

The technical aspect of Android also has negative implications towards BYOD. To be able to stand out amongst the competition, Android mobile phone and tablet manufacturers customize the OS with applications (apps). Likewise the various mobile carriers also have their custom apps installed onto the device. Since security is not the top priority of these apps, the devices are prone to external threats via these apps. The backward compatibility of the apps also poses threat to the various versions of Android OS (Gowda 2013).

BYOD may bring malware and viruses to the office network, which increases the possibility of data leakage. Cisco identified the threat to "company data from viruses, malware, and network intrusion was by far the biggest downside of BYOD" (Cisco 2012). This vulnerability increases because the IT department does not have full control over personal devices and they may not be aware of when and where employees use them. This means that "accidental malware downloads or computer viruses are not only commonplace, but can easily spread to an entire company's network in a matter of seconds" (Tzoumas 2013). Notwithstanding the fact that paralysing the systems, these malicious software may also open back doors to enter the servers and to steal company data sitting in the systems quite unknowingly. Thus, BYOD can be an easy target for hackers to enter into a company's system by means of sending malicious software to employee's personal device through email or app downloading (Ahmad 2013).

Methodology

The BYOD risk management perspective was developed through an extensive literature review on content from high quality information systems journals, white papers, and online industry articles. Papers from the *MIS Quarterly Executive* and *The Information Management Journal* were reviewed as well as studies from Gartner and Deloitte. The University of Melbourne Library and Google Scholar search engines were utilised with the key words: BYOD, 'bring your own device,' risk, mobile device, personal device, benefit. Articles related to the themes of risk management and benefits of BYOD were analyzed.

Discussion

Controlling BYOD Risks

From the literature review, BYOD can create both substantial benefits and risks. It is therefore important to look at how the identification of BYOD risks can help the organization to apply the most appropriate countermeasures. Based on the risks previously identified, this section includes applicable countermeasures to prevent, mitigate, and control these risks.

Security Policies

Though 74% of participants of a Deloitte Survey perceived the increase of usage of mobile devices as a top vulnerability, only 52% had policies specific to mobile and BYOD, and around 10% did not refer to BYOD risks at all (Deloitte 2013). Putting security policies into place is one area of improvement for organizations to control BYOD risk since they inform employees of standardized security practices to follow. For example, an organization can determine what sort of data should not be accessed on personal devices, what data can be accessed through terminal sessions (e.g. VMware View, Citrix vApp), and what data can be processed and stored through encryption (Jirasek 2013). Companies can also specify what devices are acceptable for BYOD via policy.

Security Culture

Security culture is comprised of the collective behavior, interactions, and ways of thinking among employees toward security and minimizing risk. As different value systems can impact the way individuals view and act on security issues, it can be important to create a "Security Obedient Culture" (Thomson 2010) for employees to understand the importance of, and their role in, protecting information assets. Some employees may deem security measures as obstacles and unimportant for getting their work done that they decide to overlook policies. Consequently, this human error can lead to security breaches. By encouraging an organizational culture that focuses on the significance of security, employees can conduct their jobs and utilize BYODs in a manner that supports minimizing risk and protecting information assets.

Security Strategy

Results from an A.T. Kearney (2012) study indicate "A well-designed BYOD strategy and implementation will ensure that personal IT devices boost employee productivity and satisfaction without increasing costs." A clear BYOD strategy plan can include the identification and assessment of opportunities and risks, selection of an appropriate platform selection, establishment of policies and controls, business continuity, mitigation and recovery plans, and can drive innovation, employee satisfaction, cost reduction, and protect assets (Gartner 2013). Deloitte (2013) also points out, “Prevention is an important first step; however, no organisation can be 100% safe from attack. Robust detection and advance preparation and planning may help stop a breach from turning into a crisis.”

Security Controls

In line with strategy, in order to reduce BYOD risks, informal, formal and technical controls can be applied to threats and associated vulnerabilities. Formal controls can include policies while informal controls can include education and training, and technical controls could be mobile device management (MDM), Citrix or encryption software (Ahmad 2013). As mentioned earlier, policies can also enforce access controls to determine and regulate who can access what sort of data.

Security, Education, Training and Awareness (SETA)

In a recent Deloitte survey, only “70% of the TMT [Technology, Media, Telecommunications] organizations surveyed rate their employees’ lack of security awareness as an ‘average’ or ‘high’ vulnerability” and this poses a huge information security risk (Deloitte 2013). SETA programs can help promote and monitor the security measures taken within the organization. Survey results from Crossler and Belanger (2009), “show that education in the use of security tools is necessary in order to improve usage.” Customized programs can be created to cater to people who have different age, experience, and gender attributes to instruct employees of company risks and security countermeasures.

Limitations and Further Research

The risks mentioned are discussed in context of what and how they are impacting to the organisation. However, since different risks target different aspects of BYOD means that they have different level of significance. Ranking these risks is beneficial for further discussion on how organisations have or have not appropriately addressed each of them.

Also, the paper discussion concentrates only on the organisations’ point of view. The risks and benefits mentioned are majorly targeting the organisation as a whole rather than employee specific. Employee specific risks such as MDM and loss of personal data can be included for further discussion.

To expand on the topic of BYOD risks and benefits, future research can investigate how organizations actually assess and rank BYOD risks (e.g. What methodologies, processes, tools are being used, if any?) and how organizations recognize BYOD benefits (e.g. Are they tracking costs and employee satisfaction and productivity? How are they doing this? How often?). This information could be useful because if a company is going about assessing and ranking their risks incorrectly, then the strategies and controls they put into place may not be the most effective or cost-saving.

Additional research can explore the factors that influence how individual employees, business units, and organizations perceive BYOD risks. This could help determine what individuals or departments to target first when constructing a BYOD strategy.

Furthermore, more studies can be conducted to survey what strategies and controls have been considered the most effective for organizations dealing with BYOD risks. Is it more important for a company to establish SETA programs or to create policies? Is it beneficial to run a pilot with select users? Or perhaps a focus on security culture is more important to encourage employees to follow security practices and to report security incidents.

Conclusion

There has been a shift among organizations to move towards BYOD but this raises the question as to whether or not BYOD brings more benefits or more risks to the organization? It is therefore important to conduct a thorough study of the benefits as well as the risks an enterprise would be exposed to through BYOD. Though BYOD carries several risks (i.e. data leakage and data loss) there are also many ways companies can control the BYOD movement through security policy, culture, strategy, controls and SETA to achieve potential benefits such as accessibility to data, employee satisfaction, and productivity. Furthermore, literature shows that the "human element is one of the biggest sources of information security risk" (Deloitte 2013) and it is imperative for employees to be well-versed on the subject of information security including what the best practices are and how to deal with incidents. Therefore, when answering the research question:

> *"Does BYOD increase risks or drive benefits?"*

it can be concluded that BYOD risks have to be carefully identified, assessed, monitored and controlled, specifically addressing the importance of the human element, in order to continuously reap benefits.

References

Ahmad, Atif 2013, "Information Security Risk Management", Information Systems Security Consulting lecture on 6 July 2013, University of Melbourne, Parkville.

Ahuja, M, Sarker, S, Sarker, S, Xiao, X 2012. 'Managing Employees' Use of Mobile Technologies to Minimize Work-Life Balance Impacts', *MIS Quaterly Executive*, Vol. 11 Issue 4, p143-157.

A.T. Kearney 2012, "Bring Your Own Device" Shakes Up IT Departments. A.T. Kearney, Inc.

Calder, 2013, 'Is the BYOD Movement Worth the Risks?', *Credit Control*, vol. 34 Issue 3, p65-70.

Capgemini 2011, Bring Your Own Device: It's all about Employee Satisfaction and Productivity, Not Costs! Paris: Capgemini Consulting.

Cisco 2012, Survey Report: "BYOD: A Global Perspective Harnessing Employee-Led Innovation", CISCO IBSG

Crossler, R.E. and Belanger, F. 2009. "The Effects of Security Education Training and Awareness Programs and Individual Characteristics on End User Security Tool Usage", *Journal of Information System Security* 5(3), pp. 3-22

Deloitte 2013, *TMT Global Security Risk Study*. Deloitte Touche Tohmatsu Limited

Gartner 2013, viewed 14 July 2013, <http://www.gartner.com/newsroom/id/2408515>

Gest, J. 2013, "Managing BYOD", *Smart Business Houston*, 7(11) p. 20

Jirasek, Vladmir 2013, "Security Think Tank: Embrace BYOD, but be wary of the risks," *Computer Weekly* website, viewed on 16 July 2013: <http://www.computerweekly.com/opinion/Security-Think-Tank-Embrace-BYOD-but-be-wary-of-the-risks>

Gatewood, B. 2012, "The Nuts and Bolts of Making BYOD Work", *Information Management Journal,* 46(6), p26-30

Gowda, M. 2013, 'BYOD Security: What is Android fragmentation and how does it affect Enterprise Security and why agentless makes super sense?', Agentless BYOD Discovery & Control, viewed 14 July 2013, < http://i7nw.com/byod-security-android-fragmentation/>

Howie, J. 2012, 'BYOD Security: Bring your own device – but secure it first!', *Windows IT Pro*, pp. 37-45

Information Management 2012, "BYOD Security Risks on the Rise"

Management Services 2012. 'Mobile technology for increased productivity and profitability', *Management Services, Fall 2012*, Vol. 56 Issue 3, p15-17.

McAfee 2012, 'Putting IT Back in Control of BYOD', *Osterman Research Inc.*, USA

Mont, J. 2012, The Risks and Benefits of Employee-Owned Devices. *Compliance and Technology*, 48-52.

Mont, J. 2013, The Benefits and Risks of Mobile Devices. *ERM & Internal Controls - Compliance* , 38-39.

Parker, D. 2007, “Risks of Risk-Based Security”, *Communications of the ACM*, 50(3), p. 120

Phifer, L 2013, ‘Bring your own danger’, *Information Security,* pp. 29-35.

Potts, M. 2012, The state of Information Security,2012, 7, July 2012, Pages 9–11

Rains, J 2012, *Bring Your Own Device (BYOD): Hot or Not?*, United Business Media , London,viewed 15 July 2013,
< https://news.citrixonline.com/wp-content/uploads/2012/04/BYOD-Hot-or-Not.pdf >.

SC Magazine 2012, “BYOD: OMG! Or A-OK?” Haymarket Business Publications, pp. 18-23

Shedden, P., Scheepers, R., Smith, W., and Ahmad, A. 2011, “Incorporating a knowledge perspective into security risk assessments,” *Vine*, 41(2), pp. 152-166

Shedden, P., Ruighaver, A.B., Ahmad, A., 2010, “Risk Management Standards – The Perception of Ease of Use”, *Journal of Information Systems Security*. 6(3).

Siponen, M. 2006, “Information Security Standards Focus on the Existence of Process, Not Its Content,” *Communications of the ACM,* 49(8)

Spears, J. and Barki, H. 2010, “User Participation in Information Systems Security Risk Management,” *MIS Quarterly*, 34(3), pp. 503-522

Stieglitz, S. and Brockmann, T. 2012, “Increasing Organizational Performance by Transforming into a Mobile Enterprise”, *MIS Quarterly Executive,* 11(4), pp. 189-204

Thomson, K. 2010, “Information Security Conscience: a precondition to an Information Security Culture?” *Journal of Information System Security*, pp. 3-19

Tzoumas, C. 2013, The BYOD World. *BusinessWest,* 30, 45.

Wood, A. 2012, ‘BYOD: The Pros and Cons for End Users and the Business’, *Credit Control*, vol. 33 Issue 7/8, p68-70.

Vidalis, S., Jones, A., and Blyth, A. 2004, “Assessing cyber-threats in the information environment”, *Network Security,* pp. 10-16

Yap, J. 2012, *BYOD boosts staff's productivity, job satisfaction*, ZD website, viewed on 15 July 2013:
<http://www.zdnet.com/byod-boosts-staffs-productivity-job-satisfaction-2062304237/>