https://doi.org/10.48009/2_iis_2013_195-201
Issues in Information Systems
Volume 14, Issue 2, pp.195-201, 2013

BYOD ISSUES AND STRATEGIES IN ORGANIZATIONS

Marzie Astani, Winona State University, Ph.D. mastani@winona.edu
Kathy Ready, Winona State University, Ph.D. kready@winona.edu
Mussie Tessema, Winona State University, Ph.D. mtessema@winona.edu

ABSTRACT

Managing organizations' networks has become increasingly complex with the "Bring Your Own Device" or BYOD phenomenon. BYOD is no longer an option for most organizations; rather it's the standard for business in the digital era. It is important to have well-defined policies for what's supported and accessed in organizations. This research study highlights findings from an organizational survey conducted in the upper Midwest region about organizational strategies in coping with BYOD. Recommendations are made to benefit other organizations in adopting strategies for BYOD.

Keywords: BYOD, mobile security, mobile malware, BYOD strategies and mobile device management technology

INTRODUCTION

The rapid growth of information technology is expected to provide better availability, accessibility, and mobility of data in a cost saving manner for organizations' employees. Mobile devices such as smartphones and tablets give flexibility to employees to access their work from anywhere. This new trend of allowing employees to bring their own personal devices and access their own company work from anywhere is called "Bring Your Own Device" or BYOD. Many organizations are adopting BYOD strategy since they recognize that employees have grown up with mobile devices and view these devices as the primary means of connecting, interacting with others, and increasingly using their mobile devices for work-related purposes. Eighty-eight percent of IT directors involved in a recent survey (300 were involved) believe employee morale is improved with an organization's BYOD policy [9]. Clearly, the mobile-centric workplace is here to stay.

However, in another survey [4], seventy-five percent of IT managers stated that they are concerned about BYOD and they expect increased security issues in the organization from allowing consumer-focused mobile devices in the office. For IT organizations, BYOD means supporting a variety of devices and their operating systems, and maintaining an expected level of service. The effect of granting enterprise access to personal devices has direct implications on security, information ownership, device/network control, and even helpdesk resources. The security challenges could include understanding who and what is on the network, keeping the network malware-free, determining the level of information that can be stored on a BYOD endpoint, and providing proper enforcement of access policies to maintain compliance and audit requirements.

Mobility - meaning working away from a traditional office setting or fixed location - has become a common requirement for today's knowledge worker. According to Forrester [6], nearly 60 percent of organizations support a BYOD program today. In addition, a report by Cisco [2] states that forty-seven percent of employees in the companies are officially designated as "mobile workers." These devices are mainly the result of employee initiative. They are integrating mobility into how they work on a daily basis. These employees are granted mobility privileges by the IT department based on employee request. In fact, according to Cisco ninety percent of full-time American workers use their personal smartphones for work purposes. These knowledge workers are using multiple mobile devices such as laptops, smartphones, and tablet computers to help them accomplish their tasks. Some experts, such as Accenture chief technology strategist and managing director Gary Curtis [7], are supportive of BYOD and believe that this phenomenon should be viewed as an opportunity not a problem since it extends the enterprise through

communication, collaboration, and social media, and real-time data. However, in spite of all these benefits some organizations are not supportive of BYOD for the reason that they do not want to control what applications people put on their personal device, but they do want to control which applications can be used over the corporate network. In some instances, authentication of the device is a precursor to the user's connection to the corporate network to ensure access to confidential data [4]. Organizations must consider a network policy management system that addresses the following concerns and interoperates with external mobile device management applications that monitor device usage:

- Instant messaging
- Video and photography storage
- Email and texting
- Internet browsing on and off corporate premises
- Device tracking
- Wiping of devices or containers

In this paper, we provide findings on the use of BYOD and organizations' strategies currently adopted by upper Midwest firms. This introduction section is followed by a literature review on the use and concerns of BYOD devices, research questions and methodology. Finally, the discussion of findings will be followed by recommendations and a conclusion.

LITERATURE REVIEW

BYOD is a rapidly evolving challenge to organizations and information technology (IT) cultures. Instead of having all computing devices supplied by the employers, employees are bringing their own smartphones, tablets, and laptops into the work environment. There isn't an industry that isn't putting the mobile revolution to work. The following are a few examples of what they're doing to accommodate BYOD [11]:

- **Enterprise -** Everyone wants to stay connected to the office now. So enterprises are leveraging authentication methods and policies they currently use for IT-managed laptops, and extending them to personal devices. BYOD has shifted the security paradigm from managing every aspect of the device, to just managing enterprise apps and data, such as email and attachments.
- **Healthcare -** Given all of the sensitive information and regulatory requirements at hospitals, it may be the last place you might expect BYOD to be embraced. However, a growing number of doctors and staff are using mobile devices for tasks such as patient monitoring, asset tracking, and consultation. By actively managing and securing BYOD for employees and guests, hospital IT teams can ensure compliance for HIPAA and audits while mitigating privacy concerns – while also accommodating patients, and their visitors, that want to use the hospital's guest network.
- **Education -** Higher education practically invented BYOD. Colleges and universities have had to support student-owned devices for many years and have done an excellent job leveraging BYOD to transform the teaching and learning environment. Now, these same institutions are extending BYOD to faculty and staff. In K-12, schools are providing shared resources and allowing students to bring their own device to support 1:1 student to device initiatives. IT needs a simple, secure, and easy solution that lets everyone self-register their devices and have access to school resources, regardless of what they're using. There are often content licensing implications that need to be considered if curriculum or testing and learning apps are made available to student's personal devices.
- **Retail -** Retail spaces are completely transforming as a result of mobile devices. While most of these devices used by staff are issued by IT - such as iPads for mobile point-of-sale (POS) – there is a growing

> trend to also allow BYOD in stores for certain employees. But the big story for BYOD in retail is for shoppers. Armed with smartphones, shoppers are price checking and reading product reviews while in the store – a Google/Think Mobile survey found that 77% of all smartphone users browse while shopping. Wi-Fi networks can gather information about shoppers; improving the customer experience with real-time product information and special promotions to establish long-term social media connections.

An effective BYOD program can be a source of increased employee satisfaction and productivity [7]. However, dealing with security and establishing trust in BYOD devices is very complex and a good security program must be the foundation of BYOD in organizations. Otherwise, sensitive corporate data may be exposed to outsiders and even stored on thousands of user-owned devices with inadequate controls, leading to data breaches [12]. According to a recent study of 671 IT security professionals by Ponemon [8], 47 percent of respondents concluded that more than half of employees in their organizations are using personal mobile devices in the workplace, up from 33 percent of respondents in 2011. Yet, while more employees are using personal devices, 29% of IT professionals indicated that employers were not taking steps to secure employee-owned devices, up from 21% in 2011. Some firms are taking measures to ensure information security of organization such as employees who are authorized to use company-owned mobile devices by the IT department are required to have anti-virus and mobile device management (MDM) software installed on their personal mobile devices. The MDM software will store all company-related information, including calendars, emails and other company applications in one area that is password-protected and secure. When personal devices are used by employees for work purposes, the IT department must install this software prior to usage of personal devices [12]. The IT department does not allow employees to use cloud-based applications or backup that allows company-related data to be transferred to unsecure storage locations. Personal devices are not authorized to be synchronized to other devices in employees' homes. Also, any modifications of the devices hardware or software, other than authorized and routine updates, are prohibited unless approved by the IT department. Employees may not access unsecure Internet sites. The policies need to be enforced by organizations.

One of the companies that implemented a BYOD strategy is Intel, the semiconductor giant, which has more than 39,000 devices registered on its network and about 70 percent of them are personal devices. With the involvement of numerous departments, a strategy was developed within six months. Then the company spent another nine months addressing legal and human resources issues. The objective was to establish a program that was an enabler of productivity and had the necessary safeguards and protections. This meant addressing an array of complex issues and creating an end-user service-level agreement that made it clear users were voluntarily using BYOD rather than Intel demanding it (the company continues to supply equipment to some employees). Today, Intel's BYOD program supports about 30,000 employees and offers 40 proprietary applications that range from travel tools that can help schedule a shuttle or flight to conference room finders. The company uses a variety of software and security tools including an internal app store, mobile device management (MDM) software, and has multiple levels of controls in place. In addition, it maintains a list of approved devices and ensures that they meet certain requirements. Other devices are blocked from the network. According to Intel [7], workers saved 57 minutes/day on average as a result of BYOD, which totals 5 million hours annually.

Globally, the U.S. is the overall leader in BYOD adoption and policy; however, Asian and Latin American companies encourage extensive BYOD. European countries are very cautious and restrictive about adopting BYOD [2]. The growing number of devices per user is, to a large degree, the result of BYOD. For example, 42 percent of smartphones and 38 percent of laptops used in the workplace are employee-owned. This shows that BYOD, far from being an emerging trend, is already well-entrenched in corporations throughout the world. IT leaders expect strong growth for BYOD in the next two years. An interesting point here is that although many of the employees use their personal mobile devices for the work purposes, but they are not compensated. According to one report, seventy percent of workers in the banking industry use their own smartphones for work every day [2]. Also, the

report shows that ninety percent of Americans who use their own smartphones for work don't receive any sort of stipend or allowance to pay for a smartphone, even if they use it for work.

Although BYOD initiatives can bring a multitude of benefits to businesses, security remains a major concern for all organizations, let alone companies with limited IT resources. Mobile security experts believe that it is crucial to develop a policy that governs how corporate IT staff can gain control over a personal and corporate mobile devices maintain up-to-date, corporate-approved (and preferably corporate-managed) security software installed to guard against malware and other security risks. In 2010, more than one million smartphones were infected with a "zombie" virus hidden in bogus anti-virus applications in China. In another case, in Lithuania, a worm connected the infected iPhones devices to a server, enabling criminals to control the phones remotely [13].

Most organizations that allow employees to bring their own devices are experiencing high rates of mobile threats, including lost or stolen devices, malware and compromised company data. A survey of mobile-security decision makers in companies with 10 or more employees in the U.S., UK, and Australia [1], found that more than half reported mobile threats. Sixty-one percent of survey respondents said they required additional IT resources to manage mobile security, resulting in higher costs. Further, sixty-three percent of surveyed companies reported significant increases in demand for help desk support to repair, replace or manage the security of smartphones and tablets in the company. Eighty-two percent of respondent in this study believe that mobile devices create a high security risk within the corporate environment. In addition, 45 percent reported lost or stolen devices in the past year. The stolen/lost mobile devices has been pointed out in another study done by a Credent Technologies survey that shows New Yorkers left 60,000 mobile phones in taxicabs in 2009 alone [5].

Among security measures to protect mobile devices password protection is a relatively simple technique. Organizations need to take this security measure before the company-owned mobile devices are distributed. It clearly gets more complicated when the mobile devices are employee-owned. According to a report, forty percent of smartphones are without passwords. However, passwords aren't the only basic practice that people tend to skip. Greater number of workers in sensitive industries such as legal, healthcare, and banking, reported connecting their mobile devices to unsecured Wi-Fi networks in public places, a well-known security vulnerability [2]. In addition, it's important to understand the full nature of the mobile malware that can launch events such as advanced persistent threats and denial-of-service attacks, and then create measures to address these issues. This often requires introducing new network components that assist in identifying these devices and enforcing network access privileges. The IT departments will also need to consider application accessibility per user and per device, enforcement of policies, automated policy enforcement, and IT and helpdesk overload and levels of visibility [5].

RESEARCH METHODOLOGY

After reviewing the literature, a questionnaire was developed as a basis for collecting data in this study. The instrument was composed of four categories of information: 1) Respondent Information, 2) Company Information, 3) BYOD Background Information, and 4) BYOD Experience. Categories three and four were composed of Yes/No and rating questions. The participants were expected to use a 5-point Likert scale (5 = very important and 1 = not important at all) to rate the options available in the survey items/questions. This provided a benchmark for assessing organizations' BYOD status and strategies. Fifty-two managers from organizations in the Upper Midwest region of the U.S were randomly selected to participate in this research study and provide input about their BYOD policies. The size of these organizations (based on their number of employees) varied from small to large. The collected data were analyzed and the results along with discussions are presented below.

RESULTS AND DISCUSSION

The survey items provided information about the participating organizations' type, size, and items concerning BYOD policies. Table 1 presents the type and number of organizations involved in this research study. As shown, the majority of organizations are from the service sector (32 out of 52, over 61 percent). The service sector includes financial firms (10 percent), healthcare organizations (8 percent), and educational organizations (6 percent). Retail sector is the next largest represented in our study (11 or 21 percent), followed by manufacturing sector (9 or over 17 percent).

Six of these organizations (twelve percent) employed more than 10,000 employees and were considered large companies. Forty-two of companies (sixteen organizations) in this study employed 500 to 10,000 employees and were regarded as the medium-size organizations. The majority, twenty-four (forty-six percent) of the organizations were small, employing less than 500 employees. To find out about the status of BYOD in these organizations, the answers to the survey items/questions were analyzed. Table 2 shows the percentage for the survey items based on the answers received.

Table 1. Types of organizations

Service (including financial, education, and healthcare)	32
Retail	11
Manufacturing	9

Table 2 presents some of the findings of the study. As shown, seventy-seven percent of the employers allow the employees to use their mobile devices for work purposes. This is supported by the literature stating that nearly 60 percent of organizations nationwide support BYOD programs today [5]. This is very encouraging since as mentioned above, nearly half of companies involved in our study are small organizations and may not have a sophisticated IT department to deal with the complex security issues of BYOD. Furthermore, the organizations in this study are from the Upper Midwest region and perhaps, more conservative and protective of their information assets, however they still support BYOD. As presented, majority of these companies are in the service sector and one would assume that mobility would be valued more in this sector, e.g., smartphones would be used for service calls. According to the results, the majority of these companies (sixty-three percent of the employers involved in this study) purchase the mobile devices for their employees. However, only a small percentage of these organizations provide training regarding BYOD for their employees, which is aligned with the findings stated in the literature.

Forty percent of the respondents in the survey said their organizations have purchased mobile device management (MDM), which is not surprising considering that the majority of the organizations involved are supportive of BYOD. Fifty-eight percent of the respondents stated that "BYOD has impacted organization's approach to data security" which is expected since most of the employers involved in this study support BYOD. Yet, another expected finding of this survey is that fifty-two percent stated that "password protection is most critical for MDM system."

The results of this survey indicate that fifty-six percent of employers provide security training concerning mobile devices for their employees. This shows that employers are very cautious about the companies' networks and the information assets.

Table 2. Percentage of Survey Items

Survey Item	**Percentage**
Employer doesn't allow mobile device to be used for business purposes	77
Certain groups of employees do BYOD	27

Company has purchased MDM	40
Training regarding BYOD	28
BYOD in response to rising cost	23
BYOD has impacted organization's approach to data security	58
Lost/stolen mobile device	35
Penetration of corporate Wi-Fi networks	33
Mobile device missing during past 12 months	31
Password policy enforcement is the most critical for MDM	52
Remote lock & wipe are critical for MDM	42
Malware protection critical for MDM	42
Organization addresses mobile security through training programs	56
Mobile devices are employer-owned	63
Employer reimburses employee for mobile device used for work purposes	29
Use Smartphone/tablet for work purposes per week constantly	33
Smartphones/tablets are password protected	73
Bluetooth discoverable mode disabled on smartphone/tablet	48
Employees watch recreational videos on smartphone/tablet	50

Seventy-three percent of the survey participants said that their "Smartphones/tablets are password protected" and forty-eight percent stated "Bluetooth discoverable mode is disabled on smartphone/tablet." These results confirm the point made above. Another interesting result of this survey is that fifty percent of participants watch recreational videos on their smartphones/tablets. We can guess that some of these mobile devices are company-owned.

As was mentioned in the literature review, the lost/stolen mobile devices are one of the major security concerns for organizations, whether company-owned or personal. Although our research results show that this security issue is not a major concern for our companies compared to was expressed in the literature review for New Yorkers (thirty-five percent VS. sixty-eight percent), it still is a security risk to which organizations should pay attention.

CONCLUSIONS

This research study explored the BYOD status for some organizations in the Upper Midwest region of the United States. Our results showed that only twenty-seven percent of the responding organizations in our sample support BYOD. Although, we expected that the results would show a higher number of organizations supporting BYOD, the result seems logical considering that the majority of our companies were small and may not have resources to support a sound BYOD program. A larger sample size should be considered for future studies about BYOD to have more reliable results.

Our study shows that most of the concerns such as security risks (e.g., stolen mobile devices) are valid concerns. Organizations need to purchase an MDM system to monitor mobile devices, in addition to providing training programs for employees regarding BYOD. A successful BYOD program allows employees to be productive outside of their workplace and work schedule, extending the employee's work hours and giving them flexibility. Finally, organizations need to have a formal BYOD policy and enforce it.

REFERENCES

1. BYOD Threats Require Additional IT Resources. http://www.eweek.com/mobile, (accessed March 25, 2013).
2. BYOD: A Global Perspective; Hrnessing Employee-led Innovation. http://resources.idgenterprise.com/original/AST-0074924_BYOD_Horizons-Global.pdf, (accessed March 4, 2013).
3. Cisco, The Cisco BYOD Smart Solution, 2012, http://www.cisco.com/en/US/products/hw/vpndevc/index.html, (accessed June 18, 2013).
4. Conquering today's bring-your-own-device challenges: A framework for successful BYOD initiatives. Aruba White Paper. http://www.arubaNetworks.com, (accessed April 15, 2013).
5. Cook, Matthew, G. Wiatrak, Bruce, and Olsen, Keith. 5 Top BYOD Threats for 2013. InformationWeek Report. http://www.InformationWeek.com, (accessed March 25, 2013).
6. Forrester Report. http://www.forrester.com/home?cmpid=mkt:ppc:goo:ForresterResearchhome&gclid, (accessed April 22, 2013).
7. Greengard, Samuel. How Smart Companies Manage BYOD. http://www.ciscomcon.com, (accessed May 2, 2013).
8. Ponemon Institute, 2013 State of the Endpoint, sponsored by Lumension, December 2012, http://www.ponemon.org/news-2/46, (accessed June 23, 2013).
9. Reisinger, Don. BYOD Taking the Enterprise by Storm. http://www.CIOInsight.com (accessed April 29, SHRM, News Letter (accessed April 13, 2013). http://www.shrm.org/templatestools/samples/policies/pages/bringyourowndevicepolicy.aspx,
10. 2013).
11. The definitive Guide to BYOD. http://resources.idgenterprise.com/original/AST-0088062_BYOD_Brochure.pdf, (accessed June 26, 2013).
12. Trusted Computing Group. ARCHITECT'S GUIDE:BYOD Security Using TCG Technology. http://www.trustedcomputinggroup.org, (accessed April 12, 2013).
13. Zielinski, David. Smart Phones Create New Security Threats for HR. SHRM HR Technology Discipline, January 2011.