Presented to the Interdisciplinary Studies Program:

UNIVERSITY OF OREGON
APPLIED INFORMATION MANAGEMENT

Applied Information Management and the Graduate School of the University of Oregon in partial fulfillment of the requirement for the degree of Master of Science

Best Practices for Secure BYOD Implementations

CAPSTONE REPORT

Andrew L. Rice
Technologist
A-dec, Inc.

University of Oregon
Applied Information Management Program

Fall 2016

Academic Extension
1277 University of Oregon
Eugene, OR 97403-1277
(800) 824-2714

Approved by

_____

Dr. Kara McFall
Director, AIM Program

BEST PRACTICES FOR SECURE BYOD IMPLEMENTATIONS

Andrew L. Rice

A-dec, Inc.

Abstract

The popularity of Bring Your Own Devices (BYOD) has increased dramatically over the last decade. BYOD bestows many benefits including increased productivity, flexibility, and employee satisfaction. However, BYOD also introduces new risks to the organization that must be understood and controlled. This annotated bibliography is comprised of literature published from 2012-2016 to help IT decision makers create policies and procedures to promote secure and flexible BYOD implementations.

Keywords: bring your own device (BYOD), security, mobile device management (MDM), smartphones

Table of Contents

Introduction to the Annotated Bibliography

Problem

The corporate security landscape has changed dramatically over the last decade, driven largely by two forces: (a) the widespread adoption of mobile devices, in particular smartphones and tablets; and (b) a trend that has come to be known as the "consumerization of IT" (Weiß & Leimeister, 2014, p.1). The most striking of these changes is the explosion of smart mobile devices. Research has found that of the nearly 92% of Americans who own a cellphone, 68% own a smartphone (Anderson, 2015). Tablet computer ownership, the other large piece of the mobile device market, has increased from less than 5% of American adults in 2010 to 45% in 2015 (Anderson, 2015). Both smartphones and tablets have the ability to access the Internet, and most have the ability to natively access corporate email resources (Yeboah-Boateng & Amanor, 2014). This type of access poses a problem for Information Technology (IT) departments (Olalre, Abdullah, Mahmod, & Abudullah, 2015).

In the early days of mobile devices, the Blackberry dominated. According to Don Kellogg of The Nielson Company (2010), Blackberry devices made up as much as 35% of smartphone sales as recently as 2010. Before the rise of the modern smartphone, the business world favored the Blackberry (Waterfill & Dilworth, 2014). All Blackberry devices were centrally managed through a Blackberry Enterprise Server (BES), offered a high level of application control, and had high-end encryption abilities (Nabi, Mohammed, & Nabi, 2015). Unfortunately for security-conscious IT departments, the mobile device market has changed and the Blackberry no longer rules; according to a 2015 study by The Nielson Company, users now overwhelmingly demand iPhones and Android devices ("Smartphone owners", 2015), which do not offer the same level of security and control as Blackberry devices (Gruman, 2015).

The second force at play is known as the "consumerization of IT" " (Weiß & Leimeister, 2014, p.1). As users become more familiar with consumer IT products, and the pace of advances in consumer technology accelerates, employees become frustrated that they cannot use the technology with which they are familiar at work (Weiß & Leimeister, 2014). Research has shown that once a user chooses a device, he or she feels motivated to use it in the work setting, because the user feels more proficient with the device (Giddens & Tripp, 2014).

This shift from corporate-provided devices to user-owned devices has come to be known as Bring Your Own Device (BYOD) (Giddens & Tripp, 2014). Widely embraced by users, corporate IT departments found themselves forced to embrace BYOD to avoid users creating their own unapproved workarounds, referred to as "feral information systems" (Kerr & Koch, 2014, p. 169). As far back as 2013, 71% of organizations had changed at least one process to allow the use of personal devices on corporate networks, and 68% of employees were already using personal mobile devices of all types for work (French, Guo, & Shim, 2014).

Some research indicates that allowing personal mobile device use can accrue benefits to the employer, including increased productivity (Weeger, Wang, & Geewald, 2016). French, Guo, and Shim (2014) note that 80% of users who use their own devices feel they are being more productive, and found a flexible and accommodating BYOD policy increases overall employee morale. Their research further suggests BYOD has the potential to save the organization money, as the user rather than the organization shoulders the cost of the devices, including purchase price and monthly charges (French, Guo, & Shim, 2014).

Nevertheless, all of these new and often unaccounted for devices pose risks, whether they are smartphones, tablets, or laptops. One recent study showed that 64% of companies had a user device containing sensitive data stolen, and few had plans to deal with the thefts (Morrow, 2012).

This is a form of data loss known as "data leakage" to which mobile devices are particularly susceptible (Olalre, Abdullah, Mahmod, & Abudullah, 2015, p. 4). Malware, defined as a superset of "bad software" including viruses and spyware that are designed to do harm to a computing devices (Christensson, 2006, para. 1), is also a potential source of data leakage (Olalre, Abdullah, Mahmod, & Abudullah, 2015). One study found that 50% of Android-based malware is used to collect data or track users' activities (Morrow, 2012).

Many of the threats posed by BYOD are linked to the user's behavior (Horton, 2015). For example, one study shows that 21% of workers used the same devices they used for accessing corporate resources to view pornography, and up to 25% of employees were unaware of the potential malware threat (Horton, 2015). Additionally, the study noted that 25% of employees would be too embarrassed to admit they had contracted malware in such a manner, and thus would not tell IT, introducing more risk to the corporate network (Horton, 2015). This kind of cross-pollination is just one example of the risks companies face when considering the adoption of BYOD practices (Zahadat, Blesser, Blackburn, & Olson, 2015, p. 26).

The financial impact of device theft and loss associated with BYOD is high; one estimate notes that the cost of one lost devices was as high as $4,800 when factoring in costs including compliance charges, productivity loss, and data loss (The Ponemon Institute, 2014). The same survey also noted that on average 3.19% of devices were lost or stolen each year, meaning a company with 1,000 user-owned mobile devices accessing company resources would face costs of over $150,000 a year due to these lost or stolen devices (The Ponemon Institute, 2014). The cost of malware associated with BYOD is also significant; the Ponemon Institute (2014) found that on average 4.13% of mobile devices are infected with malware and that when these infected devices were compromised it cost the company on average $3,903 per incident.

Devising sound policies to address the BYOD phenomenon in a proactive manner is necessary for the modern IT department (Waterfill & Dillworth, 2014). Employees bring personal devices of all types to work, and will continue to do so (Weeger, Wang, & Geewald, 2016, p. 1). The security threats of BYOD to organizations and the potential financial impact are substantial (Rose, 2013). The task of IT departments going forward is determining how to support BYOD in a way that promotes user productivity and job satisfaction, while at the same time protecting the enterprise from attacks originating both internally and externally.

Purpose

The purpose of this study is to provide an overview of the current academic literature on the subject of BYOD. The focus of this study is on several related topics including the history and scope of BYOD and issues that accompany the practice, user attitudes towards their devices and their organization's handling of the BYOD trend, and best practices for the implementation of security policies to minimize the risk to an organization posed by BYOD. This study seeks to provide organizational technology decision makers, implementers, and planners with a better understanding of the role of BYOD in their organizations. Finally, this work puts forward literature that addresses best practices to follow when designing corporate BYOD policies.

This paper presents literature that discusses the current state of BYOD and the security implications for organizations that fail to acknowledge this trend. Further literature is presented that discusses various aspects of BYOD security including potential legal and intellectual property risks. Additional sources include descriptions of user attitudes toward BYOD and how BYOD-related choices affect the employee/employer relationship.

Research Question

Main question. What are the best practices for designing and implementing a secure corporate BYOD policy that is still flexible enough for employees to reap the benefits?

Sub questions. What forces and historical examples are driving the need for a BYOD policy? How does a company's chosen BYOD policy affect the employee/employer relationship?

Audience

Proper mobile device management requires a top-down plan, and buy-in at all levels of the organization (Singh, 2012). This study is primarily targeted at IT decision makers, those that are responsible for making IT policy decisions and selling those decisions to executive leadership. This group includes managers within the IT department, directors of IT, Chief Information Security Officers (CISOs), and Chief Information Officers (CIOs). The study is also targeted at those within an IT department charged with assuring the function and security of the corporate network, to provide these stakeholders with a better understanding of the state of the field and the hurdles they may face in their own BYOD policy implementations. This group includes network administrators, security administrators, systems administrators, and the IT business analysts and project managers involved in gathering requirements and implementing new technology.

Search Report

Search strategy. Finding information about this topic is relatively straightforward. Initial searches using Google provide a great deal of information, but these results are primarily from newspapers or industry sources. While some of this information may be accurate, due to the lack of academic rigor and potential for bias these sources are excluded. However, these initial

searches are useful in shaping future inquiries and expanding the researcher's subject-related vocabulary.

The University of Oregon (UO) Libraries' site and Google Scholar are used to provide the bulk of sources related to the topic. These sites provide a variety of articles related to BYOD. The UO Libraries' site proves to be the more useful of the two search engines due to its enhanced set of tools, which makes refining searches simple and efficient. The university's subscription to a wide variety of databases means searches result in a large number of articles from peer-reviewed sources. The following is a list of databases from which relevant articles are obtained:

- Academic OneFile
- ArXiv.org
- EBSCO Host
- Elsevier Science Direct
- Factiva
- JSTOR
- Research Gate
- IEEE Xplore Digital Library
- ProQuest
- Sage Journals
- Springer Link

Google Scholar proves to be useful when searching for articles that are not available online at the university site. In addition, Google Scholar provides unique results, and the Google search yields a wider breadth of related articles for a given keyword. Finally, one article is retrieved by accessing the library of George Fox University, a Summit network partner.

For the purposes of this study, searches are limited to articles written in the past four years, except for sources that provide historical context. Additionally, resources that are solely focused on education are excluded. While there are many articles about BYOD adoption in educational institutions, the needs, desires, considerations, and trade-offs of the users are too different from private sector employers for there to be meaningful crossover for this study. However, BYOD in education is an interesting field full of its own promises and threats, and is worthy of future study.

Key terms. Early Google searches help to shape the keywords used during the search process. This limiting of keywords proves helpful in focusing on relevant articles. The following is a list of those keywords for this study:

- *Android and BYOD*
- *BlackBerry*
- *Blackberry Enterprise Server (BES)*
- *Bring Your Own Device*
- *BYOD*
- *BYOD AND CYOT*
- *BYOD and consumerization of IT*
- *BYOD cost*
- *BYOD malware*
- *BYOD laptops*
- *BYOD risks*
- *BYOD savings*
- *BYOD theft*

- *BYOD viruses*
- *Bring your own technology*
- *BYOT*
- *Choose your own technology*
- *CYOT*
- *Consumerization of IT*
- *Digital natives*
- *iPhone and BYOD*
- *Mobile device management*
- *Smartphones*
- *Tablets*

Documentation Method

Throughout the research project, Zotero is an invaluable tool for managing documents. A new folder is created for this study, and relevant articles are saved into three folders designating (a) possible resources for the annotated bibliography, (b) general references for the introduction and conclusions, and (c) for interesting references of doubtful quality. A new entry is then created for each promising article. Each entry includes a copy of the database page for the article and a copy of the article itself. Whenever possible, a Portable Document Format (PDF) version of the article is captured to ensure its availability in an easily readable format.

In addition to the article itself, an American Psychological Association (APA) formatted reference and the abstract for each entry are saved. The abstract is stored in the space provided by Zotero for easy future retrieval. References are collected from the databases when possible, or from the UO Libraries site. In cases when no citation is found, the bibliography-generating

function of Zotero is used, as well as the website Bibme.org. The citation is reviewed for accuracy, and edits are made when needed, which is necessary about 90% of the time. These references are stored within a note attached to each item.

Periodic backups of the Zotero database are made to the researcher's Microsoft OneDrive cloud storage space. In addition, working copies of this document are synchronized between the researcher's laptop and a cloud storage drive. Backup copies are occasionally emailed to the researcher's secondary email account as a tertiary method of backup.

Reference Evaluation

Reference evaluation criteria. All references included in this document are evaluated based on the guidelines outlined by the Center for Public Issues Education in the guide *Evaluating Information Sources* (2014). The five main criteria for reference evaluation are authority, timeliness, quality, relevancy, and lack of bias (CFPIE, 2014). Sources for this study are considered authoritative if they were published in a peer-reviewed journal or were presented at a major conference. When evaluating lesser-known publications, weight is given to the quality of the host site. For example, one source was disqualified because its host site was compromised by hackers.

Due to the rapidly changing nature of this field, sources are considered timely only if published after 2012. Sources are also checked for the quality of the overall article including spelling, grammar, flow, and punctuation. Sources are deemed relevant if they discuss BYOD and surrounding issues, with a focus on corporate IT. All sources are evaluated for potential bias. Supporting references are checked, and weight is given to articles that primarily cite other academic sources. In addition, industry sources or any sources whose authors have a potential financial motive for the publication are excluded.

Annotated Bibliography

The following annotated bibliography presents 15 articles that discuss the topic of BYOD in the corporate environment. References are presented that inform IT executives, managers, and key decision makers who are responsible for approving and implementing BYOD of the current state of the field. References are divided into three categories (a) BYOD security considerations, (b) BYOD and employee relations, and (c) BYOD implementation best practices.

Each of the following annotations are broken down into three parts (a) the full bibliographic citation in APA format, (b) the published article abstract, and (c) a summary of the article. Each abstract is presented as published, with minor edits in a few cases to correct glaring spelling or typographical errors. The article summaries present an overview of the author's salient points as they relate to BYOD.

Category A- BYOD Security Considerations

Dhingra, M. (2016). Legal issues in secure implementation of bring your own device (BYOD). *Procedia Computer Science, 78*, 179-184. doi:10.1016/j.procs.2016.02.030

Abstract. Nowadays use of smart phones, tablets, laptops has become an integral part of schedule of work in most organizations and corporations. Many of them are adopting a new policy of allowing the employees to use their own devices at workplace. Despite the economical and usage benefits, Bring Your Own Device policy can pose some serious security risks and have negative impacts depending on employee ethics and lack of safeguards in framing company regulations. This paper investigates the legal issues regarding the implementation of BYOD policy and suggests the solutions to overcome those incidental problems.

Summary. In this article, the author outlines the security issues inherent with BYOD. The author starts the article by providing statistics about the prevalence of BYOD, including Gartner's (Fielding, 2015) estimate that by 2017, 50% of companies will make BYOD a requirement and that by 2018 there will more than 1 billion BYO ("Bring Your Own") devices (p. 2). Of more concern, Gartner notes that only 30% of companies have approved BYOD policies and that more than 50% of employers rely on their employees to protect their personally owned devices.

The legal issues springing from this widespread use of BYOD are many. The author discusses such challenges as storing data securely on BYO devices, monitoring BYO devices, respecting employee privacy, handling breaches, and securely destroying data on employee devices. The author states that all of these risk mitigations need to be planned and employers need to develop policies surrounding their implementation.

The author reminds IT departments that BYOD policies will be different from those they have for company-owned devices and that the policies need to remain flexible. While security is important, it is often at odds with productivity, and employers must strike a careful balance.

This source is useful to this study for its review of BYOD security issues. In particular, this source provides a high-level review of BYOD issues described in an easily understandable manner. Directors of Information Technology or CIOs looking to educate upper management on the reasons for a BYOD policy will want to consider using this article as an educational tool.

Downer, K., & Bhattacharya, M. (2015, December). BYOD security: A new business challenge. In 2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity) (pp. 1128-1133). IEEE. doi:10.1109/SmartCity.2015.221

Abstract. Bring Your Own Device (BYOD) is a rapidly growing trend in businesses concerned with information technology. BYOD presents a unique list of security concerns for businesses implementing BYOD policies. Recent publications indicate a definite awareness of risks involved in incorporating BYOD into business, however it is still an underrated issue compared to other IT security concerns. This paper focuses on two key BYOD security issues: security challenges and available frameworks. A taxonomy specifically classifying BYOD security challenges is introduced alongside comprehensive frameworks and solutions which are also analysed to gauge their limitations.

Summary. In this article, the authors describe BYOD security challenges as having two main dimensions. The first dimension includes the facets of the organization that the introduction of user-owned devices impacts the most, which the authors identify as human resources and the management of IT equipment. The second dimension breaks the issues into primary concerns, key characteristics, similarities, and logical relationships (p. 1).

The authors further divide the equipment challenges into deployment challenges and technical challenges. Under deployment challenges, the authors suggest that organizations need to perform careful analysis before deciding what resources to make accessible to mobile devices. Once they understand deployment issues, they need to determine how they are going to control access to resources and assure that their policies

cover a wide range of BYO devices. Other challenges related to BYOD that the authors raise are monitoring employee-owned devices, maintaining secure connections between employee devices and organizational resources, and protecting data stored in the cloud. Under the category of human resources issues, the authors identify training as a key area of concern. They note that it is important for everyone to understand general BYOD policies, and for users privy to sensitive information to understand the restrictions that come with their access. The authors also caution that users may forget policies over time, necessitating periodic retraining. The authors also note that employers need to watch for users who strongly disagree with BYOD limitations, as they may seek to circumvent the BYOD security policies.

The authors then share elements of a BYOD security framework that includes mobile device management (MDM), the use of virtual desktops, and acceptable use policies. All of these security methods have drawbacks and must be thoroughly analyzed and considered before being implemented.

The article is useful to the current study for its discussion of BYOD security issues and its list of mitigating steps an organization can take to address the issues. Of particular interest is the discussion of the various recommended security measures and their associated drawbacks; it provides a helpful list for IT managers and directors involved in BYOD policy formation.

Mitrovic, Z., Veljkovic, I., Whyte, G., & Thompson, K. (2014, November). *Introducing BYOD in an organisation: The risk and customer services view points*. Paper presented at The 1st Namibia Customer Service Awards & Conference (pp. 1-26).

Abstract. With the recent technology advances and the rapid adoption of tablet computers and smartphones, it has become increasingly common for employees to use their own personal devices to perform various tasks in their work-place. This phenomenon is better known as Bring Your Own Device (BYOD). This new concept is seen as twofold: as not that simple to handle and, at the same time, many organisations are quickly adopting BYOD as it has been shown that it offers many positive effects such as increased job satisfaction, employee morale, better productivity and consumer services. However, permitting employees to utilise their own device of preference in the work-place also brings some risks often associated with the loss of control over organisational data. Hence, this study set to determine and assess the risk of introducing BYOD in an ICT organisation. The Case Study approach elicited that the secure use of the BYOD requires the introduction of mixed measures: technical (e.g. Mobile Device Management - MDM) and non-technical (e.g. ICT or BYOD security policies). This study also explored the customer services view related to the BYOD initiative and suggests that use of this initiative can leverage services. The contribution of this study, aimed at practitioners and academics, is seen as threefold as it can help organisations to successfully manage the introduction of BYOD for employees and customers satisfaction, create and implement appropriate policies and also assist the individuals to learn about the risks related to the use of BYOD in an organisation.

Summary. The authors of this study set out to correct what they see as a lack of understanding about the issues surrounding BYOD, particularly in their home country of South Africa. They begin by giving a brief overview of the current state of BYOD and defining its vital attributes; chief among these attributes are mobility and consumerization. The essence of mobility is that employees are now able to work from anywhere on devices meant to be used on the go. Consumerization is a trend in which users are introducing the latest (employee-owned) devices into their corporate infrastructures. These attributes lead to the benefits of BYOD, which they define as improved creativity, better sales efficiency through increased engagement with customers, and cost savings.

The next section discusses the risks associated with BYOD. Among the threats they mention are data leakage, infection via malware, and loss of management visibility. They note that some see these challenges as a replay of what happened when employers first started introducing laptops to their organizations, but the authors feel that BYOD poses bigger challenges due to the variety of devices BYOD introduces into the network and the fragmentation of device security levels.

The authors suggest several methods to mitigate the risks of BYOD: applying application control, educating employees, implementing security policies, developing a security culture, and implementing mobile device management (MDM). They argue that applications are the backbone of the mobile device experience and need to be carefully monitored and controlled, but in a manner that does not impact usability.

Employee education helps to address the problems introduced by the user, the weakest link in the security chain. A company needs to develop detailed security policies that

define the roles and responsibilities of each party and grant employees access to the devices, and then educate their users on these policies. Beyond setting policies, organizations should develop a culture of security that weaves information security measures into normal operating practices. Finally, organizations need to make use of MDM technology that builds in the control lost in BYOD.

This article is useful for the current study because of its discussion of BYOD security issues and the views of BYOD shared by the industry leaders they interview. The interview section in particular will be useful when looking to understand real life experiences other organizations have had with BYOD.

Olalere, M., Abdullah, M. T., Mahmod, R., & Abdullah, A. (2015). A review of bring your own device on security issues. SAGE Open, 5(2). doi:10.1177/2158244015580372

Abstract. Mobile computing has supplanted internet computing because of the proliferation of cloud-based applications and mobile devices (such as smartphones, palmtops, and tablets). As a result of this, workers bring their mobile devices to the workplace and use them for enterprise work. The policy of allowing the employees to work with their own personal mobile devices is called Bring Your Own Devices (BYOD). In this article, we discuss BYOD's background, prevalence, benefits, challenges, and possible security attacks. We then review contributions of academic researchers on BYOD. The Universiti Putra Malaysia online databases (such as IEEE Xplore digital library, Elsevier, Springer, ACM digital library) were used to search for peer-reviewed academic publications and other relevant publications on BYOD. The Google Scholar search engine was also used. Our thorough review shows that security issues comprise the most significant challenge confronting BYOD policy and that very

little has been done to tackle this security challenge. It is our hope that this review will provide a theoretical background for future research and enable researchers to identify researchable areas of BYOD.

Summary. The beginning of this article notes the prevalence of BYOD in the modern organization and highlights the extent to which BYOD is already occurring in developed and emerging economies. The authors cite studies that point to the benefits of BYOD, including increased employee contentment and cost savings.

In the next section, the authors address security, which, according to several sources, is the most pressing concern associated with BYOD. The authors note that desktop computers and mobile devices share 90% of the same issues. The top three security threats introduced by BYOD are distributed denial of services (DDoS) attacks, data-leakage, and malware.

This article is useful for this specific research because it highlights the prevalence of BYOD in organizations worldwide and highlights some of the security risks that are attendant with a BYOD implementation.

Utter, C., & Rea, A. (2015). The "bring your own device" conundrum for organizations and investigators: An examination of the policy and legal concerns in light of investigatory challenges. *The Journal of Digital Forensics, Security and Law: JDFSL, 10*(2), 55-71.

Abstract. In recent years, with the expansion of technology and the desire to downsize costs within the corporate culture, the technology trend has steered towards the integration of personally owned mobile devices (i.e. smartphones) within the corporate and enterprise environment. The movement, known as “Bring Your Own Device” (hereinafter referred to as “BYOD”), seeks to minimize or eliminate the need for two

separate and distinct mobile devices for one employee. While taken at face value this trend seems favorable, the corporate policy and legal implications of the implementation of BYOD are further complicated by significant investigatory issues that far outweigh the potential benefits of integrating a BYOD policy. In this paper we first set a context for the BYOD conundrum, then examine associated corporate policies, highlight the limitations to the digital investigator's reach regarding digital evidence and review the investigatory challenges presented to the involved parties (such as the forensic examiner) from a BYOD environment. We conclude by offering recommendations such as implementing finely crafted policies and procedures (such as incident response), utilizing Mobile Device Management and other software, corporate owned devices, and enforcing signed agreements.

Summary. The authors of this study note that BYOD comes with many benefits, including an increased interconnectedness amongst employees and a shifting of costs from the employer to the employees. They also point out that employees tend to acquire new technology faster than their company does; benefits then accrue to the company when employees use this new technology to do their jobs better and faster. Finally, the authors point out that the design and implementation of a BYOD policy is an opportunity for the organization to review current policies and retrain employees on information security matters.

The article describes some of the legal implications to consider when implementing a BYOD policy. The authors first discuss mobile devices and 4th Amendment protections. The authors also point out the risks of employees co-mingling personal data with work data, and warn there are risks to the company if personal data is accessed maliciously.

The authors warn that with BYOD, a company puts itself at the risk of data loss due to malicious deletion by an employee, particularly at the point of employee termination. To address these concerns, the authors suggest several steps. These include the implementation of mobile device management (MDM) and mobile application management (MAM), services that create mechanisms to separate corporate data from private data. They also suggest services such as the ability to wipe a device remotely. These services can also prevent compromised devices from accessing the network and prohibit users from installing dangerous applications. The authors note that proper user education and a well thought-out policy are keys to a successful BYOD implementation. The authors emphasize that users must understand that they do not have an expectation of privacy for corporate data on their devices, or for personal data they have chosen to co-mingle. The company also needs to establish their right to search or monitor the device to avoid lawsuits. Finally, the company must clearly define its role and acknowledge its responsibilities for support and privacy.

Despite the fact that this article is targeted at the needs of digital forensic examiners (DFEs), it serves as a strong overview of the legal risks companies face when implementing BYOD. Of particular interest to this study is the closing section, which identifies the key elements of a well thought out BYOD policy. This description will be useful to IT managers and decision makers looking to protect their companies from legal challenges while implementing a BYOD policy.

Vignesh, U., & Ahsa, S. (2015). Modifying security policies towards BYOD. *Procedia Computer Science, 50*, 511-516. doi:10.1016/j.procs.2015.04.023

Abstract. In the IT Consumerization phase, the organizations permit their employees to bring their personally owned device to workplace. This is achieved through enforcing policy or agreement - Bring Your Own Device. The BYOD policies adopted in numerous organizations are vague and generally immature. The prevailing security policies in BYOD are no more supportive for mobile devices like smartphones, tablets and laptops. The security policies must be modified to suit these devices. To mitigate this downside, 3-tier enhanced policy architecture is proposed which specifies the policies to be followed by the device, applications and organizations.

Summary. The authors of this article suggest a three-tier policy for BYOD management. In this model, the highest tier is the organizational policymaking level. Under this tier, the company establishes the employee's responsibility for backing up personal data, the company's right to ask the user to remove applications from his or her devices, and that devices that have had their built-in security circumvented (through a process called rooting or jailbreaking) are not allowed on the network. The company also needs to clarify responsibility for purchase, support, and repair of the devices. Finally, at this tier, the author recommends the creation of user roles that designate level of access. These roles can be based on technical knowledge or job function.

They second tier is the application level. Proper management at this tier requires the implementation of some form of Mobile Device Management (MDM) or Mobile Application Management (MAM). Technologies like MDM and/or MAM expands the

organization's ability to manage an employee-owned phone and offers services like data encryption, application control, and password policy enforcement.

The final tier is the device itself. The author notes that this tier is often the most overlooked, but that companies should pay attention to this layer. Important steps include ensuring device-level encryption and assuring the device is not compromised with fake security certificates.

This article is pertinent to this study for the high-level security policy it sets forth. Of particular note is the discussion of the organizational-level policy and the suggestion of defining user roles with different abilities. This information will be useful to IT directors or managers looking to construct usage guidelines.

Yeboah-Boateng, E. & Boaten, F. (2016, August). Bring-Your-Own-Device (BYOD): An evaluation of associated risks to corporate information security. *International Journal in IT and Engineering, 4*(8), 12-30. Retrieved October 23, 2016, from https://arxiv.org/abs/1609.01821

Abstract. This study evaluates the cyber-risks to Business Information Assets posed by the adoption of Bring-Your-Own-Device (BYOD) to the workplace. BYOD is an emerging trend where employees bring and use personal computing devices on the company's network to access applications and sensitive data like emails, calendar and scheduling applications, documents, etc. Employees are captivated by BYOD because they can have access to private items as well as perform certain job functions while being unrestricted to their desks. This is however usually done on the blind side of management or the system administrator; a situation that tends to expose vital and sensitive corporate information to various threats like unwanted network traffic, unknown applications,

malwares, and viruses. Expert opinions were elicited in this exploratory study. The study evaluated the characteristics of BYOD, assessed associated risks, threats and vulnerabilities. The findings indicate that little or no security measures were instituted to mitigate risks associated with BYOD. Though, profound benefits abound with BYOD adoption, they could be eroded by security threats and costs of mitigation in curing breaches. The most significant risk was found to be Data Loss which was in consonance with similar studies on Smartphone security risks. Some mitigation measures are then recommended.

Summary. In this article, the authors conduct a deep dive into security issues related to BYOD. These issues include improper data disclosure, data leakage, Phishing, improper decommissioning, network spoofing, and network congestion. The authors provide a series of steps to mitigate these issues, including backups and automatic locks to prevent data-leakage if the device is stolen; developing a clear understanding of application security settings to prevent unintentional data disclosures; the use of Secure Sockets Layer (SSL) and Virtual Private Network (VPN) to prevent malicious networks from stealing user data; and monitoring of devices for malware.

The authors share the outcome of their study in which they find some interesting results. For example, they found that 57% of respondents said BYOD was prohibited or that their companies did not have BYOD plans, but 86% of those surveyed admitted they were using personal devices for work. The survey also showed that information technology professionals have respect for the potential risks of their employers' BYOD implementations. The authors conclude by noting that while the security risks of BYOD are widely understood by technology professionals, the mitigation strategies are not. The

authors stress the importance of BYOD security education and suggest that management track the development of BYOD within their organization to guide its development in a direction positive to the company.

This article is useful for this study in that it provides useful data on the perceived security risks of BYOD. It also provides high-level mitigation strategies that IT security managers can implement to help to secure their networks.

Zahadat, N., Blessner, P., Blackburn, T., & Olson, B. (2015). BYOD security engineering: A framework and its analysis. Computers & Security, 55, 81-99. http://dx.doi.org/10.1016/j.cose.2015.06.011

Abstract. With the rapid increase of smartphones and tablets, security concerns have also been on the rise. Employees find it desirable to use personal mobile devices for their work and make no distinction between using their carriers' services versus their organizations' Wi-Fi. Bring Your Own Device (BYOD) is an extension of corporate networks and thus it is essential to secure BYODs to protect enterprise networks (Wang and Vangury, 2014). In this paper, risks of allowing BYOD balanced by its benefits will be examined. The paper has three overarching objectives. The first is to address the security concerns of BYOD, which necessitate technology, policy management, and people integration instead of the traditional technology alone approach. The second is to propose a BYOD Security Framework as the solution to BYOD security concerns. The x`framework has three pillars: People, Policy Management, and Technology. It will be demonstrated that these three pillars are necessary in order to secure BYOD implementations in enterprises. The final objective is to validate the framework. This is done via an empirical survey conducted on a pool of 114 industry security practitioners.

The resulting dataset is analyzed to determine the association between the level of the BYOD Security Framework elements being de facto implemented in organizations and the frequency of security breaches associated with BYOD in those organizations to confirm key elements of the framework.

Summary. This article describes the benefits of BYOD. Key benefits the authors mention are a lower burden in employee training on new devices, service in remote locations over nearly ubiquitous cell networks, and the ease of communication. They specifically highlight the benefits BYOD brings to the healthcare industry, including the fact that doctors can use one device even though they often work at multiple locations. In discussing the need for BYOD, the authors highlight the fact that many companies say no to BYOD initially, but soon find themselves unwitting participants as their employees connect their personal devices to company networks anyway. Therefore, the authors encourage companies to make sure their users are taking active roles in BYOD security adherence. They also caution that implementing onerous security standards can inhibit usability and functionality.

The authors present both a detailed BYOD security lifecycle and a BYOD security framework. The framework is broken down into seven steps: (a) plan, (b) identify, (c) protect, (d) detect, (e) respond, (f) recover, and (g) access and monitor. Throughout each step of the framework, the authors present detailed actions companies can take to implement BYOD in a secure fashion. Key recommendations are careful planning, providing education, developing a governance strategy, implementing mobile device management (MDM), device patching, and proper device de-provisioning. They make the case for using BYO devices to access applications on remote Virtual Machines. The

authors note that this practice solves many of the security issues inherent in BYOD, but they admit this solution can have high overhead.

This article is important to the current study because it offers a detailed framework that companies can use when considering the implementation of BYOD in their organizations. CIOs, CISOs, and IT managers would benefit greatly from reading this article and understanding key elements like the BYOD lifecycle, the security framework, and the implementation process.

Category B – BYOD and Employee Relations

Brodin, M. (2016). *BYOD vs. CYOD: What is the difference?* Paper presented at 9th IADIS International Conference Information Systems 2016. IADIS Press.

Abstract. During the last years mobile devices have become very popular to use both for work and pleasure. Different strategies have evolved to increase productivity and to satisfy the employees. In this paper, we look at the two most popular strategies and look at the strengths and weaknesses of those. This is done by a systematic literature review and semi-structured interviews with CIO's or equivalent roles. We conclude that BYOD and CYOD comes with similar strengths, but CYOD brings a little fewer security risks.

Summary. In this article, the author discusses the difference between Bring Your Own Device (BYOD), where the employees provide the device, and Choose Your Own Device (CYOD), where employees choose the device and the IT department buys and controls it. They note that these strategies are different from the traditional strategy of use what you are told (UWYT).

In discussing BYOD, the author notes many benefits including increased productivity, increased flexibility, and increased user satisfaction. He points to a study that notes that

BYOD users work more hours overall. He also notes that BYOD leads to the mixing of personal and private data and that employees bristle at the kind of security measures companies want to use to keep corporate data safe. These measures include encryption and remote wipe ability. The author notes that security awareness is a widespread issue and cites a study that reports that 40% of employees do not update their software and 25% of employees do not see why they should do so. Finally, the author cautions that BYOD may not save money as it drives up the cost of support.

The author contrasts BYOD to CYOD, where the organization buys the device and remains in control of it. CYOD carries many of the same time and flexibility advantages as BYOD, but with a higher level of control. Users are more likely to accept privacy and security controls when they do not own the device, and when the employee leaves the company the device is returned and can be wiped by the company. Another major benefit of CYOD, from the user's perspective, is that the user does not have to pay for the device. This article contributes to the current study in its discussion of BYOD versus CYOD and the examples the author relays from the various CIOs he interviewed. This article would be of interest to any CIO or IT director contemplating the implementation of BYOD or CYOD who wants to understand the attitudes and mindsets of users at companies that have already done so.

Kerr, D., & Koch, C. (2014, June). *A creative and useful tension? Large companies using "Bring Your Own Device"*. In International Working Conference on Transfer and Diffusion of IT (pp. 166-178). Springer Berlin Heidelberg.

Abstract. This paper looks at processes of embedding of computer systems in four organisational case studies in three different countries. A selective literature study of

implementation of computer systems leads the authors to suggest that seen from a top down managerial perspective employees may be assumed to accept and use new computer systems, for example an ERP system but what happens deep down in the organisation are a reshaping, domestication or appropriation of the software for example through developing workarounds. The authors further suggest that traditional implementation models may incorrectly assume that the computer systems has been embedded in the organisation because things appear to be running smoothly when in fact software and/or processes have been reshaped by employees to suit their local needs. These social shapings appear to be done for a multitude of reasons. However, from the qualitative case studies it appears that most workarounds are done to make work easier and/or to overcome perceived inflexibilities in existing enterprise mandated systems. The ubiquitous access to cloud technologies and an increasing workforce of tech savy (sic) "digital natives" using their own devices (BYOD) has exacerbated the situation.

Summary. The authors of this article examine the changing landscape of IT management and define two broad categories of technology. The first category is the traditional managerial-controlled, or structured technology that is implemented by the company and backed by the expertise of the IT department. The second category is domesticated technology. Domesticated technology is unstructured, implemented by the user, and limited by the user's expertise. The authors note that the introduction of domesticated technology did not start with BYOD, but existed prior, usually in the form of unapproved changes to corporate software systems.

In discussing IT domestication, the authors suggest that users make these tools their own and want to use them to do their jobs. If the current IT implementations are too inflexible

to meet their needs, the users will modify the tools in a way that allows them to meet their needs. These feral information systems (FIS) allow users to adapt IT systems to meet their needs and only use the components with which they are comfortable.

The authors share the results of four case studies in which they sought to understand the level of domestication present in each company. The first case was a large transportation company in Australia where the authors found that employees went to great lengths to avoid using the corporate ERP system. The second case focused on a university and how employees' use of cloud systems affected security and governance. Several IT officials at the school expressed concern that as users adapted technology to their own needs, the IT department was stuck playing catch up. The third case examined the IT environment at a training organization associating with a university in the UK and illustrated that a lack of feedback in systems often leads people to try to find workarounds. The fourth case examined a large Danish supermarket and, based on the analysis, the authors noted that users found third-party software to fill in perceived gaps in the organizational information systems.

The authors argue that domestication has been around for a long time, but that BYOD accelerates the inherent problems. Employees bring their own devices and then look for ways to complete their jobs on those devices, using technology with which they are already comfortable. The authors argue that this kind of domestication is here to stay and that IT departments need to embrace it.

The article is useful to the current study for its discussion of the paradigm shift in the industry from technology introduced and managed exclusively by the IT department to technology that is introduced by the end user. Of particular note is the description of

managerial-controlled implementations and domesticated technology. The key takeaway for management should be that the development of domesticated technology is unavoidable and should be understood and, when possible, accommodated.

Weeger, A., Wang, X., & Gewald, H. (2016). IT consumerization: BYOD-program acceptance and its impact on employer attractiveness. *Journal of Computer Information Systems*, *56*(1), 1-10.

Abstract. Many firms are considering 'bring-your-own-device' (BYOD) programs, under which their employees are allowed to bring their own devices to work and use them for both private and business purposes. This study examines what factors determine an employee's intention to participate in a corporate BYOD program and how such programs affect employer attractiveness. We approach our study of acceptance of corporate BYOD programs from the perspective of technology acceptance research. For this purpose, we propose a modified and extended UTAUT model. The model was tested by surveying students in their final term (n = 444). We show that performance expectancies have the strongest positive effect on intention, while perceived threats negatively impact intention. Finally, behavioural intention was positively associated with employer attractiveness, which leads to clear indications for companies considering establishing corporate BYOD programs. BYOD seems to play an increasingly important role in attracting and retaining future talent.

Summary. This article focuses on BYOD and its role in increasing an organization's attractiveness to current and future employees. The authors closely link BYOD to IT consumerization, which they define as the process "whereby IT first emerges in the consumer market and spreads into business organizations as employees push devices

used privately into the workplace" (p. 2). In response to this trend, and to prevent the rise of shadow IT infrastructure, companies implement a BYOD policy.

One of the most pertinent factors to emerge from the study is the discussion of threats employees perceive from BYOD. These include fears that the employee's data may be destroyed along with corporate data, the company may access and use the employee's personal data, a negative shift in the work/life balance may occur when the same device is used for personal and work purposes, and the employee may be held responsible for data loss or corruption events that are caused by his or her phone.

The researchers found that BYOD policies can positively influence an employer's attractiveness. Additional findings include that the biggest concern of future employees is being held responsible for the loss of business data and that students expect future employees to allow BYOD.

This resource is useful to the current study in that it highlights the importance of a BYOD policy and its impact on recruiting. It also highlights some of the biggest issues companies need to address when implementing BYOD policies in their organizations.

Weiß, F., & Leimeister, J. M. (2014). Why can't I use my iPhone at work?: Managing consumerization of IT at a multi-national organization. Journal of Information Technology Teaching Cases, 4(1), 11-19. doi:10.1057/jittc.2013.3

Abstract. As IT innovations in the last years emerged on the consumer market, employees are more experienced in the private than in the corporate use of innovative IT devices and applications. These employees, familiar with the benefits consumer products offer, expect those to be provided by their corporate IT. This trend, referred to as 'consumerization of IT', leads to more and more consumer innovations infiltrating

companies. In particular, mobile consumer devices are currently spreading into companies, strongly pushed by top management, and create several challenges to Chief Information Officers (CIOs) around the globe: 'What IT costs are associated with the use of mobile consumer devices?', 'How will corporate use of mobile consumer devices affect IT management?', and 'How to introduce an IT service for corporate as well as personal mobile consumer devices?'. OMEGA Group, a multi-national company with 50,000 employees, wants to leverage the potential of mobile consumer devices for corporate purposes. Therefore, these questions have to be addressed and answered by its CIO. The teaching case is designed to introduce the characteristics of consumerization and associated challenges for IT management. The case uses selected information systems methodologies and frameworks.

Summary. This article is written in narrative form and relates the experiences of "John," the CIO of the fictitious Omega Group. The story starts out with John and many of his co-workers asking why they cannot use their iPhones on the corporate network. John is even asked to approve the purchase of iPhones for the executive team as he heads into a meeting with his department heads about the state of mobile computing at the company. John and his colleagues discuss some of the potential issues with allowing employees to use personal devices on the corporate network, which include a possible increase in data costs, the difficulty involved in distributing corporate applications to multiple platforms, as well as the effort and cost required to provide support for a heterogeneous mix of devices. Information from a mobile device consultant helps them to realize the importance of taking the time to examine any system they are implementing and choosing any project vendors wisely. The consultant also stressed that the organization

should run a proof of concept and pilot phase for their BYOD implementation. Finally, the consultant encourages the company to understand BYOD costs upfront so that the costs do not spiral out of control.

This article is useful for this study in that it provides a look at a real-world scenario in which new technology is making its way into the organization. It also shares detailed survey numbers that any company considering BYOD should consider. These figures include the fact that 51% of employees feel their IT department is not responsive to their desires to use new technology, and that 45% of employees believe their devices are more useful than the devices provided by their companies.

Category C – BYOD Implementation Best Practices

French, A. M., Guo, C., & Shim, J. (2014). Current status, issues, and future of bring your own device (BYOD). *Communications of the Association for Information Systems, 35*(10), 191-197.

Abstract. This paper summarizes the panel discussion that occurred on the 2013 American Conference on Information Systems to discuss the current status, issues, and future direction of the use and adoption of bring your own device (BYOD). BYOD is widely used around the world. The invited panelists comprised five faculty members from the United States and Korea specializing in information systems. The covered BYOD topics included current use, real-world cases, adoption, pros and cons, issues (cultural, security, privacy), and future direction. The panel also corved [sic] bring your own service (BYOS) and bring your own apps (BYOA).

Summary. The authors of this article begin by providing a brief overview of the current state of BYOD. Among the interesting facts they share are that 15.8% of those who

embrace BYOD do so without the IT department's knowledge and 20.9% do so despite an anti-BYOD policy. They also mention that due to the relative newness of BYOD, some companies have been slow to react to the prospect of employees using their own devices to access organizational resources. Other employers have taken a wait-and-see approach to BYOD.

The authors provide a list of elements that will help drive a successful BYOD implementation. These elements include having an employee code of conduct, installing security programs on the devices, and developing device management rules. They emphasize the importance of the employee code of conduct and note it is important to mitigate the human risks of BYOD. These risks include users becoming distracted at work by their mobile devices or working at times they are not allowed to work. The authors also stress the importance of education in successfully implementing a BYOD policy.

The authors describe two different security models for BYOD: the hands-on and the hands-off security models. With the hands-on model security measures are taken on the devices, including installing management software that can monitor and track the device. The hands-off security model takes a different approach. Instead of installing tools on the devices, the IT department creates a platform that mobile device users can access to perform their work. The platform is usually accomplished through virtual desktops or application virtualization.

The authors end the article by noting that IT departments pondering BYOD need to expand their thinking beyond physical devices, as Bring Your own Application (BYOA) is a logical extension of BYOD. BYOA has its own set of security issues, but offers the

potential for increased productivity and savings as users access pre-existing internet services the organization can economically provide.

This article is useful to the current study for its discussion of the current state of BYOD and some of the implementation considerations of BYOD. Its classification of BYOD security methods is also valuable. This article offers high-level overviews of many BYOD-related topics and would be useful for educating management or the user base.

Pell, L. (2013). BYOD: Implementing the right policy. *University of Derby, UK*, 95-98.

Abstract. With the growing number of data endpoints connecting to an organisation's network, the need for a robust, secure policy is more relevant than ever. BYOD and the general consumerization of IT are presenting IT professionals with unique challenges. Is there a way to reap the benefits of BYOD whilst maintaining a rock solid data protection plan? This paper highlights the key areas that should be approached when considering the implementation of BYOD in your business.

Summary Pell starts this article by noting that when discussing BYOD, one must not limit thinking to smartphones alone. The definition of a device should be expanded to include tablets, online file services like DropBox that are capable of receiving and storing information, and other devices. Pell points to the wide variety of devices being used to access corporate networks, including over 1,500 different Android devices from 50 separate manufacturers (p. 95).

The author describes employer responsibility in organizations that allow BYOD, noting that data loss or theft can lead to large fines by regulatory agencies, along with whatever damage the loss itself will cause. Pell recommends that measures like remote deletion be put in place and that workers should be made aware of these security measures. Pell also

asserts that users must be required to accept the risks before using their personal devices for work. At the same time, the author notes that users have a right to keep their personal data private and that companies must implement plans that do as little harm as possible to personal data when managing corporate information.

To accomplish this goal, the author makes three recommendations. The first is the proper use of digital rights management (DRM). By implementing DRM, organizations can prevent sensitive corporate data from being accessed in an improper manner. Second, the author recommends Network Access Control (NAC), which prevents unauthorized devices from accessing the corporate network. Finally, the author recommends implementing application access control (AAC), which limits the applications that can be installed and run on a device.

This article contributes to this research topic by outlining the scope of BYOD and making concrete implementation recommendations. The author describes three questions to ask when designing a BYOD policy (p. 97): Will it help my employees do their jobs better? What will make them most productive? How much extra cost and additional IT support will be necessary to fulfill my employees' desires to use their own devices?

Waterfill, M. R., & Dilworth, C. A. (2014). BYOD: Where the employee and the enterprise intersect. *Employee Relations Law Journal*, *40*(2), 26-36.

Abstract. Employees are availing themselves of smart phones, tablets, and other personal handheld devices to perform the duties that encompass their employment. At this point, bring your own device programs --or "BYOD" should not be a question of "if" a company should implement, but a question of "how" to implement a program that will succeed in cutting costs, increasing efficiency, and improving employee relations and morale. The

authors of this article discuss the benefits and risks of BYOD, and advise companies to have the proper security architecture that enables it to quickly support personal devices and provide access to data without increasing risks.

Summary. This article begins by discussing the role of BYOD in the modern organization. The authors start with a brief discussion of the history of BYOD and highlight the risks and benefits of BYOD. Among the risks the authors identify is the speed with which devices can be provisioned and de-provisioned and the challenges faced in supplying users with the tools and support they need. Among the benefits the authors highlight are an increase in the flexibility of working hours and an increase in the overall level of collaboration.

The authors of this article provide recommendations for the successful implementation of a BYOD policy. They encourage employers to be upfront about the steps they plan to take to secure the users' phones and the rights and responsibilities of both the employee and the employer. The authors provide a sample user agreement, which would serve as a solid foundation for an organization crafting its own BYOD user agreement. Finally, the authors caution that BYOD can have overtime implications for non-exempt employees. They encourage companies to limit BYOD to exempt employees only, or to restrict access for non-exempt employees after hours.

This article is useful to this study for its examination of the legal implications of BYOD. The BYOD user agreement is particularly helpful, as it clearly defines the rights and responsibilities of both parties in the BYOD agreement and gives managers a useful starting point from which to create their own agreements.

Conclusion

Researchers tie the beginning of the BYOD phenomenon to the launch of the iPhone in 2007 (Zahadat, Blesser, Blackburn, & Olson, 2015). Since this time, IT departments have seen a massive influx of user-owned devices accessing organizational resources, a trend that is only expected to grow in the future (Weeger, Wang, & Geewald, 2016). Companies that allow BYOD realize many acknowledged benefits, including more flexible working hours and increased employee creativity and satisfaction (Vignesh & Asha, 2015). However, allowing employees to connect their personal devices to organizational resources also has downsides that every company needs to carefully consider when deciding on their BYOD strategies. Potential issues include an increased risk of data leakage, loss of control over the devices connected to the corporate network, and an unfavorable shift in their employees' work/life balance (Waterfill & Dillworth, 2014).

This study features sources that highlight these issues and provide valuable information to those involved in planning and implementing BYOD at their organizations, thus allowing them to find strategies that balance security and usability. These sources are presented in three categories: (a) Forces driving BYOD, (b) BYOD and the employee/employer relationship, and (c) Best practices for secure BYOD implementations.

Forces Driving BYOD

While mobile devices have been around for some time, early devices like the Blackberry were limited in functionality and were easily controlled by corporate IT departments (Waterfill & Dillworth, 2014). Most IT departments had a Use What You Are Told policy (UWYAT), in which they controlled the mobile devices that could be used on the network and selected the devices each employee was issued (Brodin, 2016). This dynamic changed with the introduction

of what many consider to be the first true smartphone, the iPhone, in 2007 (Mitrovic, Veljkovic, Whyte, & Thompson, 2014).

Since this time the pace of technological change has accelerated, and the best technology no longer originates with the IT department; rather, it is introduced to the organization by the end-users themselves (Weeger, Wang, & Geewald, 2016). Users prefer their personal devices to corporate-issued devices, and many use them on corporate networks without the approval of their IT department (Weiß & Leimeister, 2014, p.1). This problem is widespread, and efforts to prevent BYOD often fail. As French, Guo, and Shim (2014) note, 15.8% of employees bring their own devices even though BYOD is not supported by their IT department, and 20.9% of users do so even if there is an express anti-BYOD policy. These types of statistics are of concern to corporate IT departments. The situation is even more worrisome when taking into account that 40% of users never update their devices, thus missing vital security patches, and 25% of users do not understand the need for updates (Brodin, 2016).

Even when BYOD policies are supported by an employer, organizations experience problems introduced by the very fact that the devices are mobile. While mobility is one of the key advantages of smartphones, tablets, and laptops, these mobile devices are much easier to lose or to use on unsecured networks, which can lead to data leakage when the devices are not controlled by the company (Olalre, Abdullah, Mahmod, & Abudullah, 2015). Data leakage has the potential to be damaging due to the loss of important data and potential legal implications (Yeboah-Boateng & Boaten, 2016). Resources cited in this paper show examples of laws, such as the Secure Communications Act in the United States (Waterfill & Dillworth, 2014), that levy large fines on companies that accidentally disclose information.

Some organizations pursue a BYOD strategy hoping to save money (French, Guo, & Shim, 2014). These savings come as an organization shifts the costs of purchasing the device and the monthly charge to the employee (Utter & Rhea, 2015). However, whether an organization realizes actual savings through BYOD is debatable; while there may be initial savings, the amount of support required increases dramatically, which may erase the savings (Brodin, 2016).

Finally, when considering BYOD, it is important to remember that it encompasses more than just physical devices. Pell (2013) encourages the expansion of the definition of BYOD to include applications and cloud services like Dropbox. Utter and Rea (2015) note that physical devices and services that can store and transmit corporate data need to be understood and provisions need to be made to safely integrate them into the corporate environment. Specific policies that describe the rights and responsibilities of all parties are required (Mitrovic, Veljkovic, Whyte, & Thompson, 2014). Zahadat, Blesser, Blackburn, and Olson (2015) note that these policies are not meant to be static and recommend that IT departments revisit them over time to account for new devices and services.

BYOD and the Employee/Employer Relationship

While many reasons are given for a company to adopt a BYOD initiative, one area deserves special attention: how an employer's attitude toward BYOD affects the relationships with their employees (Weeger, Wang, & Geewald, 2016). Weeger, Wang, and Geewald (2015) note that a favorable policy towards BYOD can make an organization more attractive to potential employees. Further, they note that traditional students entering the workforce for the first time have spent their whole lives under the influences of IT consumerization, which means they are used to getting the newest technology as soon as it is available and now as end users they introduce the latest technology into their organizations (Weiß & Leimeister, 2014). With the

consumerization of IT, these first-time job seekers expect future employers to allow employees to use their personal devices at work (Weiß & Leimeister, 2014).

Companies that have not allowed BYOD, or even expressly forbidden it, oftentimes find themselves overrun with user-owned devices despite their policies (French, Guo, & Shim, 2014). This situation leads to the development of what Kerr and Koch (2014) call "feral information systems" (FISs), which they define as IT artifacts or software outside the accepted infrastructure that is used as a workaround (p. 166). While FISs are not a new phenomenon, their potential for growth increases with BYOD (Kerr & Koch, 2014). Feral information systems pose a real danger; Weiß and Leimeister (2014) note that FISs result from employees attempting to accomplish their assigned tasks while feeling constrained by the approved corporate infrastructure.

Instead of ignoring the BYOD phenomenon, Olalre, Abdullah, Mahmod, & Abudullah (2015) recommend that companies instead realize its benefits and embrace it as a tool that will bring them future success. Studies have shown that employees who use BYOD are more productive, including one study of Intel employees that claims a daily productivity gain of 57 minutes (Zahadat, Blesser, Blackburn, & Olson, 2015). Other studies show that users are happier overall when they are able to use their own devices at work, and that they tend to feel more comfortable with their own devices rather than company-provided devices (Weeger, Wang, & Geewald, 2016).

For all of the benefits the employee and employer can realize from BYOD, some caution must be taken (French, Guo, & Shim, 2014). Weeger, Wang, and Geewald (2016) note that BYOD can cause an unfavorable shift in an employee's work/life balance. Even more important, Warterfill and Dillworth (2014) note that BYOD can have serious overtime implications as non-

exempt employees who check email or perform other work-related activities outside of their normal working hours require compensation. This problem leads to the recommendation that BYOD be limited to exempt employees only (Waterfill & Dillworth, 2014).

Mitrovic, Veljkovic, Whyte, and Thompson (2014) also note the importance for companies of clearly delineating the roles and responsibilities of both the employee and the company in a BYOD relationship. Employees need to know the risks that come with enrolling their phones in the corporate BYOD program, and what they are at risk of losing if, for example, their IT department has to conduct a remote wipe. Employees must also know to what extent their IT departments will monitor their activities (Dhingra, 2016). Utter and Rhea (2015) assert that companies must understand the importance of ensuring respect for employee privacy and that care is taken with private data on corporate servers. Finally, employees need to know how much risk they are assuming with BYOD and how the company will respond if a security incident occurs (Pell, 2013). Weeger, Wang, and Geewald (2016) found that one of the main factors influencing an employee's decision not to participate in a BYOD program is the fear of repercussions in the event of data loss. A good BYOD policy will help to ease these fears (Weeger, Wang, & Geewald, 2016).

Best Practices for Secure BYOD Implementations

Once a company decides to pursue a BYOD strategy, the challenge is making the practice of BYOD secure (Dhingra, 2016). The risks are many, and fall into two categories: (a) risks to corporate IT infrastructure, and (b) risks to data (Olalre, Abdullah, Mahmod, & Abudullah, 2015). The risks to corporate IT infrastructure largely mirror the risk corporate IT departments have always faced from threats such as malware, network resource overload, and distributed denial of service (DDoS) attacks, with one study suggesting a 90% rate of crossover (Olalre,

Abdullah, Mahmod, & Abudullah, 2015). Risks to data include data leakage, in which sensitive corporate data is unwittingly sent out of the organization (Olalre, Abdullah, Mahmod, & Abudullah, 2015), or when the device containing sensitive information is lost or stolen (Yeboah-Boateng & Boaten, 2016). Yeboah-Boateng and Boaten (2016) also discuss incidental data disclosure, in which applications on devices leak information without the user's knowledge.

While one of the main benefits of BYOD is the flexibility and creativity it provides to employees (French, Guo, & Shim, 2014), security is often the enemy of usability (Zahadat, Blesser, Blackburn, & Olson, 2015). Information Technology departments need to temper their desire for total control over user-owned devices and accommodate BYOD as much as practical to benefit from it fully. The first step to mitigate BYOD security issues is developing a comprehensive BYOD policy (Utter & Rhea, 2015). The policy should be detailed and list the types of devices and access allowed, security measures the company will take with regard to BYOD, and the rights and responsibilities of both the employee and the company. Waterfill and Dillworth (2014) suggest having users sign an agreement that clearly communicates all of these details. Organizations also need to decide if they want to implement a single policy or develop user roles that allow for differing levels of access (Downer & Bhattacharya, 2015). Vignesh and Asha (2015) recommend a four-tier system of security for BYOD, with three tiers of increasing rights and responsibilities and a fourth tier for guest users.

For maximum effectiveness BYOD policies should cover all phases of the device's lifecycle, from the first time the device connects to the network to when it is finally disconnected (Zahadat, Blesser, Blackburn, & Olson, 2015). These policies should cover the implementation of application controls, the configuration of device encryption, and plans to destroy corporate data in the event that the device is lost or stolen (Zahadat, Blesser, Blackburn, & Olson, 2015).

Once these policies are crafted, it is important they be revisited annually at a minimum, and updated periodically to keep up with current trends and threats (Zahadat, Blesser, Blackburn, & Olson, 2015).

Securing the devices themselves is another challenge (Brodin, 2016). Specially designed software packages and services called Mobile Device Management (MDM) and Mobile Application Management (MAM) allow corporate IT departments to manage, track, and assert a measure of control over the device (Utter & Rhea, 2015). Mobile Device Management enables the organization to automatically control server settings, deploy SSL certificates, enforce corporate security policies, and remotely wipe devices (Utter & Rhea, 2015). Some see MDM as a relatively blunt tool and instead use MAM systems, which focus on the data, not the device (Utter & Rhea, 2015). These systems typically employ *siloing*, a technique that prevents the comingling of private and corporate data (Utter & Rhea, 2015). Other important steps to secure users' devices include enabling device encryption and preventing devices that have had their basic security systems overridden and their operating systems opened up to dangerous software form participating in BYOD (Vignesh & Asha, 2015).

Companies also need to understand what happens to a device once it is no longer being used by the employee (Zahadat, Blesser, Blackburn, & Olson, 2015). Yeboah-Boateng and Boaten (2016) note that over 100 million devices are resold each year, and they point to a study in which the authors purchased 26 business smartphones on eBay and recovered personal data from 11 of them. This situation presents a substantial risk, and organizations must plan for the destruction of corporate data when a device is decommissioned (Zahadat, Blesser, Blackburn, & Olson, 2015)

If a company is looking for a more hands-off approach to BYOD security, they can choose instead to use techniques like application virtualization or virtual desktops (French, Guo, & Shim, 2014). These methods provide an environment for employees to do work off their mobile devices, which has the advantage that the data is never on the device (Downer & Bhattacharya, 2015). However, these techniques are often expensive and difficult to maintain, and can push employees back to the one size fits all model they were looking to escape with BYOD (Zahadat, Blesser, Blackburn, & Olson, 2015).

Companies that are not yet ready to fully embrace BYOD but who are open to allowing users more freedom in device choice may want to consider a "choose your own device" (CYOD) strategy (Brodin, 2016). When implementing CYOD, the organization chooses a variety of approved devices and lets the user select from these approved models (Zahadat, Blesser, Blackburn, & Olson, 2015). The employee is awarded some choice of what device to carry and does not have to use separate devices for work and personal use (Zahadat, Blesser, Blackburn, & Olson, 2015). The company pays for the device and service fees, but support is greatly simplified, and there is no question where the device goes when it is no longer being used by the employee (Zahadat, Blesser, Blackburn, & Olson, 2015).

Finally, the most important component when implementing BYOD is education (Utter & Rhea, 2015). Employees need to be educated on the magnitude of potential threats and their role in preventing them, as they are often the weak link in the BYOD equation (Brodin, 2016). It is also vital to understand that education is not a simple one-time event, but rather an ongoing initiative that continually sharpens users' security skills and maintains user awareness of new threats and security techniques (Zahadat, Blesser, Blackburn, & Olson, 2015). Mitrovic, Veljkovic, Whyte, and Thompson (2014) suggest that BYOD education should be part of a larger

security culture fostered at the organization. Instituting a security culture ensures that employees understand that security is not just the job of the IT team, but is the responsibility of everyone at the company (Zahadat, Blesser, Blackburn, & Olson, 2015). One benefit of this kind of collective mindset is that everyone works together to maintain security of the company resources and knowledge is shared with the wider community (Zahadat, Blesser, Blackburn, & Olson, 2015).

Summary

BYOD is no longer a hypothetical idea, as employees at many companies are using their personal devices on the corporate network, with or without their employer's knowledge (French, Guo, & Shim, 2014). Employees want to use their own devices for work purposes, and multiple studies have shown that they will find a way, even if this means circumventing security measures put into place to prevent access to company resources via personal devices and ignoring policies that bar BYOD (French, Guo, & Shim, 2014; Weeger, Wang, & Geewald, 2016). While there are many risks inherent in letting users access the corporate network via user-owned devices, there are also many benefits (Mitrovic, Veljkovic, Whyte, & Thompson, 2014). If an organization makes the decision to allow BYOD, it is important they carefully consider all the ramifications, both positive and negative (French, Guo, & Shim, 2014). The CIOs, CISOs, IT directors, and other IT decision makers responsible for enacting BYOD policies can ensure a more secure BYOD implementation by developing detailed policy frameworks and rich toolsets (Zahadat, Blesser, Blackburn, & Olson, 2015). These steps, combined with continued employee education, will allow an organization to reap the benefits of BYOD while at the same time limiting exposure to security risks (Mitrovic, Veljkovic, Whyte, & Thompson, 2014; Utter & Rhea, 2015; Zahadat, Blesser, Blackburn, & Olson, 2015).

References

Anderson, M. (2015, September 29). Technology device ownership: 2015. Retrieved October 31, 2016, from http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015

Brodin, M. (2016). *BYOD vs. CYOD: What is the difference?* Paper presented at 9th IADIS International Conference Information Systems 2016. IADIS Press.

Center for Public Issues Education (2014, August). Evaluating Information Sources. Retrieved from http://www.piecenter.com/wp-content/uploads/2014/08/evaluateinfo.pdf.

Christensson, P. (2006). Malware Definition. Retrieved 2016, Nov 20, from http://techterms.com/definition/malware

Dhingra, M. (2016). Legal issues in secure implementation of bring your own device (BYOD). *Procedia Computer Science, 78*, 179-184. doi:10.1016/j.procs.2016.02.030

Downer, K., & Bhattacharya, M. (2015, December). *BYOD security: A new business challenge*. In 2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity) (pp. 1128-1133). IEEE. doi:10.1109/SmartCity.2015.221

Fielding, L. (2015, June 25). BYOD top 6 trends you need to know about in 2015. Retrieved November 28, 2016, from https://macquarietelecomgroup.com/news/byod-top-6-trends/

French, A. M., Guo, C., & Shim, J. (2014). Current status, issues, and future of bring your own device (BYOD). *Communications of the Association for Information Systems, 35* (10), 191-197.

Giddens, L., & Tripp, J. (2014). *It's my tool, I know how to use it: A theory of the impact of BYOD on device competence and job satisfaction*. In Americas Conference on Information Systems (AMCIS), Savannah, GA, USA.

Gruman, G. (2015, October 06). Mobile security: IOS vs. Android vs. BlackBerry vs. Windows Phone. Retrieved November 13, 2016, from http://www.infoworld.com/article/2987635/mobile-security/mobile-security-ios-vs-android-vs-blackberry-vs-windows-phone.html

Horton, R. (2015). Not safe for work. *Computer Fraud & Security, 2015*(3), 18-20.

Kerr, D., & Koch, C. (2014, June). *A creative and useful tension? Large companies using "Bring Your Own Device".* In International Working Conference on Transfer and Diffusion of IT (pp. 166-1 78). Springer Berlin Heidelberg.

Kellogg, D. (2010, June 04). IPhone vs. Android. Retrieved November 02, 2016, from http://www.nielsen.com/us/en/insights/news/2010/iphone-vs-android.html

Mitrovic, Z., Veljkovic, I., Whyte, G., & Thompson, K. (2014, November). *Introducing BYOD in an organisation: The risk and customer services view points.* Paper presented at The 1st Namibia Customer Service Awards & Conference (pp. 1-26).

Morrow, B. (2012). BYOD security challenges: Control and protect your most sensitive data. *Network Security, 2012*(12), 5-8.

Nabi, R. M., Mohammed, R. A., & Nabi, R. M. (2015). Smartphones platform security a comparison study. *International Journal, 5*(11).

Olalere, M., Abdullah, M. T., Mahmod, R., & Abdullah, A. (2015). A review of bring your own device on security issues. *SAGE Open, 5*(2). doi:10.1177/2158244015580372

Pell, L. (2013). BYOD: Implementing the right policy. *University of Derby, UK*, 95-98.

Rose, C. (2013). BYOD: An examination of bring your own device in business. *The Review of Business Information Systems, 17*(2), 65.

Singh, N. (2012). BYOD genie is out of the bottle–"Devil or angel". *Journal of Business Management & Social Sciences Research, 1*(3), 1-12.

Smartphone owners are as diverse as their devices. (2015, March 05). Retrieved November 2, 2016, from http://www.nielsen.com/us/en/insights/news/2015/smartphone-owners-are-as-diverse-as-their-devices.html

The Ponemon Institute. (2014, March). The cost of insecure mobile devices in the workplace. Retrieved November 13, 2016, from http://www.ponemon.org/local/upload/file/AT&T Mobility Report FINAL 2.pdf

Utter, C., & Rea, A. (2015). The "bring your own device" conundrum for organizations and investigators: An examination of the policy and legal concerns in light of investigatory challenges. *The Journal of Digital Forensics, Security and Law: JDFSL, 10*(2), 55-71.

Vignesh, U., & Ahsa, S. (2015). Modifying security policies towards BYOD. *Procedia Computer Science, 50*, 511-516. doi:10.1016/j.procs.2015.04.023

Waterfill, M. R., & Dilworth, C. A. (2014). BYOD: Where the employee and the enterprise intersect. *Employee Relations Law Journal, 40*(2), 26-36.

Weeger, A., Wang, X., & Gewald, H. (2016). IT consumerization: BYOD-program acceptance and its impact on employer attractiveness. *Journal of Computer Information Systems, 56*(1), 1-10.

Weiß, F., & Leimeister, J. M. (2014). Why can't I use my iPhone at work?: Managing consumerization of IT at a multi-national organization. *Journal of Information Technology Teaching Cases, 4*(1), 11-19. doi:10.1057/jittc.2013.3

Yeboah-Boateng, E. & Amanor, P. (2014, April). Phishing, SMiShing, & Vishing: An assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences, 5*(4), 297-302

Yeboah-Boateng, E. & Boaten F. (2016, August). Bring-Your-Own-Device (BYOD): An evaluation of associated risks to corporate information security. *International Journal in IT and Engineering, 4*(8), 12-30. Retrieved October 23, 2016, from https://arxiv.org/abs/1609.01821

Zahadat, N., Blessner, P., Blackburn, T., & Olson, B. (2015). BYOD security engineering: A framework and its analysis. *Computers & Security, 55*, 81-99. http://dx.doi.org/10.1016/j.cose.2015.06.011