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

IDENTIFYING BEST PRACTICES FOR A BYOD POLICY

CAPSTONE REPORT

Joshua M. King
End-User Computing Engineer
CoBiz Financial

University of Oregon
Applied Information
Management
Program

December 2015

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

Approved by

_____

Dr. Kara McFall
Lecturer, AIM Program

Identifying Best Practices for a BYOD Policy

Joshua M. King

CoBiz Financial

Abstract

Increasing numbers of employers permit employees to use personal devices to perform work-related tasks, posing security risks. This annotated bibliography includes literature that identifies best practices for analysis, design, and implementation of bring your own device (BYOD) policies. Research results impact CIOs/CTOs, security professionals, IT operations management, compliance and audit teams, and end users interested in BYOD.

Keywords: byod, bring your own device, byot, bring your own technology, byod benefits, byod risks and disadvantages, byod risk mitigation strategies, security, mobile security, mobile computing

Table of Contents

Introduction to the Annotated Bibliography

Problem

Technology departments face challenges in allowing bring-your-own-technology (BYOT) policies, also known as bring-your-own-device (BYOD) policies (Miller, Voas, & Hurlburt, 2012). There are benefits and risks to the organization of allowing employees, also referred to as end-users, to take advantage of their personal devices for company use. Employees want to utilize their personally-owned mobile devices (cell phones and/or tablets) and their home computers (laptops and/or desktops) to access company networks and data, or use their company owned devices for personal usage (Johnson & Filkins, 2012). Webroot (2014) surveyed 2,100 employees and the survey results indicated that 41% of them were using a personal smart phone or tablet for work purposes.

There are advantages to organizations that have developed BYOD policies, including the benefit that the organizations gain by avoiding the upfront costs of the devices (Mitrovic, Veljkovic, Whyte, & Thompson, 2014) and the need to account for these costs when hiring or retaining employees (Ghosh, Gajar, & Rai, 2013). The benefits to the employees are that they can purchase the devices they are comfortable using while extending the functionality, making the corporate programs and data readily available to them without the need for separate employer-provided devices (Ghosh et al., 2013). Generally, the devices owned by the employees are newer, with cutting edge technology, thus increasing productivity, efficiency, and employee morale (Ghosh et al., 2013). An organization with a BYOD policy allows the employees to take advantage of devices they may already own, in turn reducing the number of physical devices assigned to an employee and reducing the time to keep them maintained (Mitrovic et al., 2014).

The main disadvantage to BYOD policies is the challenge of enforcing organizational security policies. Miller et al. (2012) state that "the security concerns for BYOD are largely a replay of security issues that arose when laptops became common" (p. 2). The desire of employees to use personal devices, including laptops, for work purposes exposes the employers to the potential security threats and vulnerabilities posed by the operating systems of the devices; Apple iOS and Android for example are vulnerable to malicious software (Li & Clark, 2013) and may be compromised, which could result in lost company data, trade secrets, or identity theft (Allam, Flowerday, & Flowerday, 2014). While new security risks are continually posed, Li and Clark (2013) note that "typical users have neither the necessary understanding of the available security mechanisms nor the ability to properly utilize those protection mechanisms to their full benefit" on their personal devices (p. 78).

Several vendors are already available to support BYOD policies such as MobileIron, Samsung Knox, Microsoft Intune, and VMWare Airwatch (Armando, Costa, Verderame, & Merlo, 2014). Having multiple mobile device management (MDM) vendors to investigate for policy enforcement helps in keeping costs competitive and shifts the burden of enforcing an organization's complex security policy for BYOD to the vendor partner (Armando et al., 2014).

One potential disadvantage for employees accepting a company BYOD policy is the fear of losing family and other personal photos stored on their personal devices caused by remote wipes sent from their organizations (Ackerman, 2013). Organizations resort to a remote wipe when a device is lost or stolen or if an employee ends their employment with the organization (Fiorenza, 2013). Overall, the trend is towards employees who are either unaware of the risk posed by their employers' BYOD policies, or who choose to accept the risks in favor of the

convenience and other benefits they enjoy by employing their own devices for company use, or who are unaware of the risks their personal devices have on the employers' infrastructure.

The trend in BYOD continues to grow (Ackerman, 2013; Chang, Ho, & Chang, 2014; Johnson & Filkins, 2012; Mitrovic et al., 2014; Webroot, 2014). As the number of employees employing their own devices for business purposes and workplace devices for personal use continues to grow, there is a need to identify best practices to address the concerns posed by BYOD to both employers and employees.

Purpose Statement

The purpose of this study is to present literature that identifies best practices in implementing BYOD policies in the workplace. Literature is presented that identifies the history of BYOD and the benefits to both employees and employers that have resulted in a surge of BYOD practices and policies. Sources that describe case studies are included that identify best practices and lessons learned from the empirical analysis of successful organizational implementations of BYOD policies. Literature is presented that identifies disadvantages, security risks, and more general risks associated with implementing BYOD policies in the workplace. Finally, sources are identified that provide mitigation strategies necessary to eliminate or reduce the risk of BYOD policies to the organization.

Research Question

Main question. What are best practices in implementing BYOD policies in the workplace?

Sub-questions. What are the risks and issues associated with implementing BYOD polices in the workplace? Are there mitigation plans that can be implemented to reduce the potential risks of allowing employees to utilize their own personal devices for work purposes?

Audience

There are a number of individuals and groups that will benefit from this literature research. As CIOs/CTOs build strategic plans for their organizations, this research will empower them with the knowledge to make executive decisions related to BYOD policies. This is also a resource for security professionals to understand the potential risks of a BYOD policy and mitigation strategies that can be employed to reduce the risks.

IT operations management can use the research to plan and implement BYOD policies when tasked to do so, or they can use the research to build business cases to deliver to other stakeholders such as IT security, compliance, and the CIO/CTO in regard to the benefits and disadvantages proposed BYOD policies will have on business operations.

A compliance team or auditor team may already have pre-determined opinions about a BYOD policy. Governance policies that enforce compliance have an extreme influence on the technology used within an organization (Crossler, Long, Loraas, & Trinkle, 2014). This research has the potential to assist organizations with altering their current compliance policies to accommodate BYOD.

Search Report

Search strategy. The term bring your own device (BYOD) is a request from employees that would prefer to use their personal devices to connect with their employers' networks and data. The search strategy begins with a generic search on Google using the keywords BYOD and bring your own device. Additional keywords identified from search results including BYOT, bring your own technology, security, and mobile cloud computing are then applied in order to refine the returned results. Search results are filtered with priority given to peer-reviewed journals, articles with full text available online, and year of publication of the articles between

2010 and 2015. Using the keyword *BYOD* along with the filters reduces the search results from 6,286 to 861.

Keywords. Keywords are listed in the order in which they are used to filter content through the search engines and databases. The total number of returned items for the keyword search in the University or Oregon Library without any additional filters is listed within the parentheses.

- BYOD (6,286) – bring your own device (240)
- BYOT (37,332) – bring your own technology (23)
- Security (762,221)
- Mobile cloud computing (2,540)
- BYOD & security (282)
- BYOD & security breach (8)
- BYOD & enterprise (96)

Search engines and databases. The search engines utilized to locate data are the University of Oregon Library, Safari Books Online, Google Scholar, and Google. Relevant articles are identified from the following databases within the University of Oregon Library:

- Journal of Global Research in Computer Science (JGRCS)
- IEEE Xplore
- ProQuest ebrary
- JSTOR
- Journal of Information Systems
- Computers and Security

Reference evaluation criteria. The Center for Public Issues Education (2014) states that not all information is valid, useful or accurate and each reference should be checked for authority, timeliness, quality, relevancy, and bias. Each of the evaluation categories is applied to the references cited.

***Authority*.** Resources are only valid if the article is peer-reviewed or if the author is from a reputable organization in the fields of technology, security, or device management.

***Timeliness*.** Articles are discarded if they pre-date 2010 even if they are relevant to the problem as the technology has changed significantly in the last five years.

***Quality*.** Each article is reviewed for quality to ensure the writing is clear and the flow and structure of the document are logical. Articles are selected that reflect the absence of errors related to grammar, spelling, and punctuation. Some articles may not have authors who write in US English, and thus accommodations will be made for the different spelling of some words.

***Relevancy*.** The titles and abstracts of the articles must provide relevant insight into the research topics related to BYOD policies and practices.

***Bias*.** The author of the articles must maintain a non-biased opinion on the subject of BYOD as evidenced by the presentation of various perspectives rather than a single viewpoint. Articles are not selected that are authored by those who are selling related products or services.

Documentation approach. Sources are stored within the Zotero plugin used in Mozilla Firefox. Storing sources in Zotero is accomplished by either adding the source using the *Save to Zotero* button in Firefox or with the *Store Copy of File…* function. The *Store Copy of File…* function imports the file into Zotero and then the *Retrieve Metadata for PDF* feature is used to log the source's information including title, author(s), date published, and URL, or else each field must be manually updated. Each source within Zotero is validated to ensure the title, author,

date, and URL are structured according to APA 6 guidelines. The tags section is used for keywords and categories; some keywords are created by Zotero while others are manually added by the author. All of the categories are manually added. The categories are *BYOD Risks and Disadvantages*, *BYOD Mitigation Strategies*, and *BYOD Benefits*. The *View PDF* or *View Online* functions provide the ability to open the sources saved in the application directly from Zotero.

Annotated Bibliography

The following Annotated Bibliography is a collection of 15 references that investigate benefits, risks, and disadvantages of and best practices for implementing a BYOD policy. References have been organized into one of three categories: BYOD benefits, BYOD risks and disadvantages, and BYOD risk mitigation strategies. Each annotation consists of three sections: the full bibliographic citation, an abstract, and a summary. The abstract is either from the author(s) or from the introduction sections of the article directly. The summary consists solely of gathered information from the article without prejudice of its content.

BYOD Benefits

Ackerman, E. (2013). The bring-your-own-device dilemma [Resources at work]. *IEEE Spectrum*, *50*(8), 22–22. http://dx.doi.org/10.1109/MSPEC.2013.6565553

Abstract. The smartphone revolution opened the floodgates to the BYOD (bring your own device) trend among workers. Carrying two devices is cumbersome, and many people simply preferred to use their new devices over corporate- issued phones or laptops.

Summary. Ackerman's article describes the dilemma that IT departments are facing. The main approach to the information Ackerman gathered is through empirical analysis of other case studies and surveys. A Forrester research survey found almost 10,000 individuals in 17 countries who acknowledge their usage of personal devices for work purposes. Ackerman also cites a study by Kaspersky Lab that identified one in three businesses that allow personal devices to be used for professional purposes and one in five businesses that admitted to data loss as a result of these policies. The article also highlights an investigation into the BYOD rollout program at Intel, which worked

towards a compromise with their employees to encourage secure technology habits. Ackerman disclosed that the return on investment (ROI) from Intel's deployment was still under review but found that there was a potential soft return measured by their employees claiming the BYOD saved them 57 minutes per day. In the closing remarks, Ackerman mentions a potential solution for software containers used on business applications on personal devices to secure the company information while being less intrusive on personal data.

This article is useful for this specific research study because it provides a concrete example of the benefits of an organizational BYOD policy in the form of soft ROI benefits created by greater employee efficiency in their daily lives. Ackerman also captures best practices such as increasing the user awareness of the issues posed by downloading pirated videos or lending a company device to others such as family members; these best practices can be delivered to employees through or in conjunction with acceptable use policies and mobile management software. The policy provides an organization's technology department with acknowledgement from the users that while an individual user may own a device, the user will protect the organization's data when using the device.

Fiorenza, P. (2013). Mobile technology forces study of bring your own device. *Public Manager, 42*(1), 12-14.

Abstract. With employee mobility transitioning from an amenity to a necessity in today's workplace, there has never been a higher demand for mobile technology. Due to emerging organizational pressures to implement a mobile strategy, GovLoop recently partnered with Cisco Systems Inc to explore one of the most pressing and important

trends facing government today: how to effectively -- and securely -- implement a bring-your-own-device (BYOD) initiative. Their research is presented in a report, Exploring Bring Your Own Device in the Public Sector. The report is an important read for any organization considering implementing a BYOD program at their agency. It is a practical, hands-on guide to help agencies craft a BYOD strategy. The survey -- administered to the GovLoop community -- was designed to understand the common challenges and roadblocks for BYOD adoption in the public sector. Survey respondents were predominantly from the federal government (6%) with the rest of the respondents being closely divided between state (18%) and local (20%) governments.

Summary. This article includes the successful deployment of a BYOD policy in the City of Minneapolis and a call for other public sectors to follow suit. Fiorenza conducted a survey to understand the challenges and roadblocks caused by the acceptance and implementation of a BYOD policy in the public sectors. Sixty-two percent of the survey respondents were federal government employees, 18% were state government employees, and 20% worked for local governments. The results of the research indicate that the benefits were (a) familiarity level the individual had with his or her own device, (b) improved productivity, (c) cost savings, (d) convenience of only carrying one device, (e) employee satisfaction, and (f) employee engagement. Fiorenza concluded with several best practices including (a) a well-crafted BYOD policy, (b) transparency with security processes, (c) established ownership of the data residing on the device, (d) the management and regulation of the device and applications, and (e) technical support for the devices.

This article is useful for this specific research study because Fiorenza validates through the survey results specific BYOD benefits for both employers and employees and identifies best practices for employers implementing BYOD policies. One key best practice is to back up the individuals' data prior to enrolling their devices into a MDM solution.

Mitrovic, Z., Veljkovic, I., Whyte, G., & Thompson, K. (2014). *Introducing BYOD in an organisation: The risk and customer services viewpoints*. Paper presented at The 1st Namibia Customer Service Awards & Conference, in Windhoek, Namibia. Retrieved from http://ir.polytechnic.edu.na/handle/10628/522

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 customer's 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. This article is an empirical study conducted for an information and communications technology (ICT) organization in South Africa and the Western Cape to identify BYOD risks the organizations faced. Mitrovic et al. elaborate on the benefits of a BYOD initiative: (a) ability for employees who aspire for the latest products to remain current on device technology; (b) ability of employees to work from anywhere;(c) employees' familiarity with their own personal products; (d) employers' ability to attract and maintain top talent through flexible policies, thus fulfilling a strategic need; (e) improved efficiency; (f) more enthusiastic and engaged employees; (g) improved employee creativity; (h) increased sales with a better equipped sales force; (i) lowered costs based on employees covering the costs of devices and software; (j) reduction in the number of technical devices an employee must carry; and (k) reduction in organizational infrastructure expenses. The authors name risks of BYOD including three main concerns: (a) data leaks, (b) ownership of and visibility concerns about company data, and (c) loss or theft of devices. The authors identify possible solutions for mitigating risks and challenges in the implementation and maintenance process of BYOD initiatives including (a) utilizing application security, (b) educating employees, (c) modifying security policies, (d) implementing a security conscious culture, and (e) developing mobile device management (MDM) solutions.

This article is useful for this specific research study because the authors identify specific benefits that arise from the implementation of a BYOD policy, risks and challenges of allowing employees to utilize their own devices for work purposes, and specific BYOD policies that mitigate the associated risks.

BYOD Risks and Disadvantages

Earley, S., Harmon, R., Lee, M. R., & Mithas, S. (2014). From BYOD to BYOA, phishing, and botnets. *IT Professional, 16*(5), 16–18. http://dx.doi.org/10.1109/MITP.2014.69

Abstract. Not too long ago, desktop computers were provisioned for users, and applications were carefully vetted and controlled. Now, CIOs are dealing with laptops, smartphones, tablets, and a raft of new tools and technologies that present significant security, reliability, and IP protection challenges. Moreover, users have come to expect an information experience on par with that of their personal lives. Clearly, new policies must be enacted and new tools deployed to reduce risks and keep up with growing user expectations, but balancing accessibility and security has proven to be a significant challenge.

Summary. The article by Earley et al. examines the potential risks associated with a BYOD policy for organizations. Individuals expect their technical experiences to be inline with the technical experiences provided by personal social applications like Google, Facebook, LinkedIn, Twitter, Pinterest, Skype, and Dropbox. These technical users have high expectations for the software applications they use in their work roles to be comparable to their personal social applications in terms of availability and simplicity. Earley et al. elaborate that there are also risks associated with personal applications, devices, and networks. The authors conduct a case study to illustrate the effectiveness of

a malicious application in gaining access to devices where the attack is enabled by end-users that are allowed to have additional permissions on their workplace devices including providing access to restricted device resources such as global positioning, contacts, and device information. The case study results were a 97 % rate of successful access by the malicious application, with experiments that illustrated an attack approach that ultimately gained access through persuasion. The authors recommend the implementation of technical approaches including virtualization, walled gardens, and limited separation and the implementation of BYOD policies, user training, and additional monitoring and management tools to assist in increasing accessibility to enhance the technical experiences of employees on work devices, yet controlling the risks posed by expanded accessibility.

This article is useful for this specific research study because it illustrates the risks posed by allowing increased accessibility to work devices, provides specific technical approaches IT departments can take to mitigate these risks, and provides recommendations for BYOD policies, training, and monitoring and management tools that help to balance employees' desire for enhanced technical experiences on their work devices with the risks posed by the increased accessibility required to provide them.

Johnson, K. & Filkins, B.L. (2012). *SANS mobility/BYOD security survey*. Retrieved from http://www.sans.org/reading_room/analysts_program/mobility-sec-survey.pdf

Abstract. Mobile devices are more pervasive in businesses today than in previous generations of computing (desktops and laptops). Mobile apps on these devices are used for both personal and business purposes. According to the International Association for the Wireless Telecommunications Industry (CTIA) report released in the fourth quarter of

2011, there were more mobile devices in the United States than people! These devices and their apps have become foundational tools for today's workforce, and they are more complex in their operating systems, security, use cases and ownership. They are being integrated into the daily business processes and operations of organizations, improving productivity and becoming a critical, yet complex, component of the computing environment. At the same time, mobile devices have become more and more powerful, often exceeding PC performance, app diversity and capabilities found in organizations today. Smart devices have also caught the attention of attackers who are now commonly targeting their rich apps and their access to even more valuable backend data such as bank accounts, corporate (organizational) intellectual property and personal health information. For this reason, there has been a marked increase in mobile malware, which rose 155 percent in 2011, according to a report by Juniper Networks. Now, organizations are warming up to the idea that they need to establish security and compliance policies to support mobility, including the growing use of employee-owned BYOD (Bring Your Own Device) devices and apps. The question is, how far along are they in developing those policies, and what do those policies contain? To understand and address risk in this growing mobile segment, SANS performed its first annual mobility survey of more than 500 IT professionals. The intent of this nonscientific survey was to determine the type of mobile device usage allowed for enterprise applications and what level of policies and controls enterprises have around this type of usage.

Summary. The article by Johnson and Filkins (2012) is a survey-based report. They surveyed 500 IT professionals from varying organization sizes: fewer than 100 employees, 100-499 employees, 500-1999 employees, and 2000 or more employees. The

organizations also reflected varying reaches: single country, multinational, and global organizations. The survey results deliver information regarding (a) policy implementations for BYOD, (b) the understanding demonstrated by employers of the amount of personal employee devices that are interacting with the company's network and internal data, (c) the platforms of the devices utilized by their employees, and (d) several best practices including user awareness and technical controls. The survey results indicate that organizations are attempting to adapt quickly to the threats posed and deliver BYOD solutions and policies.

This article is useful for this specific research study because the survey results and associated analysis provided by the authors lend support to the necessity of BYOD policies as 51.8% of businesses were not fully aware of the devices that were accessing their network and only 49% felt their policies met the basic security concerns. In addition, the authors provide useful tips for building and delivering BYOD policy best practices, including (a) know what devices the end users are using to access company information and resources, (b) understand the current policy for mobile devices, if any, (c) identify the current controls in place, (c) align company policies with applicable laws and regulations to which the organization must adhere, (d) know which security risks can be mitigated with technology and those that are enforced through a policy, and (e) test to ensure the policy and controls in place work as intended.

Li, Q., & Clark, G. (2013). Mobile security: A look ahead. *IEEE Security Privacy, 11*(1), 78–81. http://dx.doi.org/10.1109/MSP.2013.15

Abstract. Fueled by widespread adoption of employee-owned devices in the workplace and the explosion of mobile applications, mobile device security is under heavy debate in

both the academic and industry security communities. Businesses and government agencies are struggling to find some sense of control at a time when employee-owned devices now access some of the most sensitive data in an organization. Various approaches and solutions have been proposed, ranging from device-based intrusion detection systems, execution isolation through application sandboxing and bare metal hypervisors, ontology-based firewalls, behavior-based detection, to cloud-based protection through the use of VPN technology. The challenge of heterogeneous hardware and software platforms, such as iOS vs. Android OS, adds yet another layer of complexity to creating a comprehensive solution. The authors provide an overview of the current threats based on data collected from observing the interaction of 75 million users with the Internet. Extrapolating this data gives an insight into what threats wait on the horizon.

Summary. The article presented by Li and Clark (2013) provides a look inside the risks associated with mobile devices. Compromised mobile devices can be used: (a) to sell personal or corporate data, (b) as gateways into other trusted networks, (c) to place them into larger botnets, and (d) for premium-rate short message service (SMS) messages, also known as text messages. The complexity and enormous growth rate of mobile devices and the sophistication of the community of developers are far beyond the current control of the information security industry. Various approaches to provide mobile device security include intrusion detection systems (IDS), intrusion prevention systems (IPS), sandboxing applications, baremetal hypervisors, ontology firewalls, cloud based VPN, and behavior-based detection learning algorithms. Li and Clark call for the development of an infrastructure that reflects a collective initiative from the community, including

private networks, Internet service providers (ISPs), and other sources, and that is proactive rather than reactive in identifying and restricting the spread of malicious applications.

This article is useful for this specific research study because it identifies the need for an advanced set of tools to address the security risks and disadvantages created by the widespread push to use personal devices for work purposes and on employer networks. The rapid growth of mobile applications, which numbered approximately one million in 2013 at the time the article was published (Li & Clark, 2013), places a strain on the ability to keep heuristic algorithms used for analysis performed on the application code to identify malicious activity current. This information is useful for employers as it identifies additional security risks when allowing an end user to connect with company internal networks.

Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). BYOD: Security and privacy considerations. *IT Professional*, *14*(5), 53–55. http://dx.doi.org/10.1109/MITP.2012.93

Abstract. Clearly, there are several important advantages for employees and employers when employees bring their own devices to work. But there are also significant concerns about security privacy. Companies and individuals involved, or thinking about getting involved with BYOD should think carefully about the risks as well as the rewards.

Summary. In this article, the authors propose that BYOD is inevitable. Miller et al. (2012) state that 46% of US adults, as of February 2012, owned at least one smartphone, and of that number, most of the individuals were between the ages of 18-34. The authors explain the ease with which individuals can migrate from multiple devices to a single device for both professional and personal use. This use enables end-users to only learn

one platform and the set of tools used on the device instead of being forced to learn and carry multiple devices. Miller et al. also claim that there are security concerns with employees using their personal devices for work purposes and privacy concerns for employees who have more to lose with regard to privacy than their employers stand to lose with regard to security. The authors predict that the next generations will expect BYOD policies in place to protect their security when using personal devices for professional purposes.

This article is useful for this specific research study because it defines the dual nature of the risks associated with BYOD policies: the protection of the organization's data and networks, and the privacy and security of the employee's information on the device. Separation and security of the two sets of information is a concern that should be considered in a BYOD policy. Miller et al. (2012) remind employers that desire BYOD practices that BYOD security concerns are very similar to the security concerns that were identified when laptops first became popular.

BYOD Risk Mitigation Strategies

Allam, S., Flowerday, S. V., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers & Security, 42*, 56–65. http://dx.doi.org/10.1016/j.cose.2014.01.005

Abstract. Smartphone information security awareness describes the knowledge, attitude and behaviour that employees apply to the security of the organisational information that they access, process and store on their smartphone devices. The surge in the number of smartphone devices connecting to organisational systems and used to process organisational data has enabled a new level of operational efficiency. While employees

are aware of the benefits they enjoy by bringing their personal devices into the workplace, managers too are aware of the benefits of having a constantly connected workforce. Unfortunately, those aware of the risks to information security do not share an equal level of enthusiasm. These devices are owned by employees who are not adequately skilled to configure the security settings for acceptable security of that information. Moreover, routine information security awareness programmes, even if applied, gradually fade into the daily rush of operations from the day they are completed. This paper explores the factors, which influence these oscillating levels of information security awareness. By applying an adapted version of an awareness model from the domain of accident prevention, the factors, which cause diminishing awareness levels, are exposed. Subsequently, information security awareness emerges as a symptom of such factors. Through geometrical modelling of the boundaries and pressures that govern our daily operations, an awareness model emerges. This model ensures that organisations are better equipped to monitor their information security awareness position, their boundaries and the daily pressures affecting the organisation, thus allowing them to design better integrated policies and procedures to encourage safe operating limits. The model is evaluated using a theory evaluation framework through an expert review process.

Summary. This article provides the results of a study of individuals/employees to determine their perceived understanding of their abilities to make security-conscious decisions on mobile devices. The awareness boundary model is used within its three boundary conditions: (a) unacceptable workloads, e.g., an employee may remove passwords from the smartphone to reduce his or her work effort; (b) economic failure, e.g., when the costs of using a smartphone exceed the benefits; and (c) functional

acceptance, e.g., the optimum policy to obtain the widest acceptance and use. A boundary triangle is created to represent the three boundaries: workload boundary, productivity boundary, and functional acceptance. By placing the desired needs of a BYOD policy into the model, the authors assert that each of the boundaries must be met to achieve the highest level of acceptance and compliance with the BYOD policy. Security awareness was found to be dependent on: (a) productivity and workload levels of the smartphone, (b) pressure applied by management to increase the utilization of the smartphones, and (c) pressure applied by employees to reduce the effort it takes to complete their job functions from smartphones, and (d) "the resulting pressure applied from policy and procedure in relation to the organization's distance from the functional acceptance boundary" (Allam et al., 2014 p. 9).

This article is useful for this specific research study because it builds a qualitative model that can be used when building best practices for a BYOD policy. When an employer knows the current BYOD policies and procedures and the related concerns of the employer and employee, the employer can create, maintain, or modify an effective BYOD policy to meet the needs of the organization in an optimal and widely used fashion. A BYOD policy that employees accept and with which they comply reduces the security risks caused by employees that use workarounds on their devices.

Armando, A., Costa, G., Verderame, L., & Merlo, A. (2014). Securing the "bring your own device" paradigm. *Computer*, *47*(6), 48–56. http://dx.doi.org/10.1109/MC.2014.164

Abstract. The current mobile application distribution model cannot cope with the complex security requirements of the emerging "bring your own device" (BYOD) paradigm. A secure metamarket architecture supports the definition and enforcement of

BYOD policies and offers a promising prototype implementation tested under realistic conditions.

Summary. This article expands on the security risks associated with a BYOD paradigm in an organization. Armando et al. elaborate on the vulnerabilities exploited by code producers (developers) in two of the most widely used application stores, Apple Store and Google Play store. Two proposed risk mitigation strategies are introduced (a) secure metamarket (SMM), and (b) security-by-contract (SxC) model. As the the SxC model suffers from several problems, Armando et al. develop workflows for the SMM model along with a prototype called BYODroid. BYODroid is limited to the Android operating system and the Google Play store, but the SMM model proposes solutions in delivering a secure BYOD mechanism for (a) policy specifications, (b) policy validations with the application in question, (c) application code validation, and (d) restriction abilities if any of the rules are not met according to the organization's BYOD policies. An experimental test using the US government's BYOD security policy was conducted on 860 applications found in the Android store with three main policy rules; (a) applications cannot save files locally to the device, (b) once applications are terminated the temporary data must be deleted, and (c) Bluetooth data transfers are restricted. The results provided evidence that the implementation of a security layer has a minimal impact on the performance of the device and that the code enforcements to restrict the storage of files locally or transfer of files via Bluetooth were effective.

This article is useful for this specific research study because it delivers potential risk mitigation strategies available for implementation into an organization's BYOD policy, along with third party vendors that have created products that may assist in developing

and executing these strategies. The results of the experimental prototype indicate that a set of security controls installed correctly may mitigate data loss with minimal degradation in performance on the mobile device.

Chang, J. M., Ho, P.-C., & Chang, T.-C. (2014). Securing BYOD. *IT Professional*, *16*(5), 9–11. http://dx.doi.org/10.1109/MITP.2014.76

Abstract. Today's IT departments are concerned with the popularity of BYOD, because mixing personal and enterprise data presents security threats to corporate proprietary information. IT departments must develop company security policies that let employees access sensitive resources using personal devices.

Summary. The article created by Chang et al. examines the challenges faced within IT departments with respect to BYOD practices and proposed solutions. In the article, security issues, malicious software, and management on the device were declared as a few of the challenges. The authors utilized studies and surveys conducted by organizations such as Intel, IBM, Webroot, Sophos, Ubuntu, and the U.S. White House. The results of each study/survey articulated the desire of employees for BYOD and the challenges facing the IT departments who have to regulate BYOD. Chang et al. covered possible solutions such as mobile device management (MDM), mobile application management (MAM), and mobile content management (MCM) tools. They conclude the article with the assertion that a BYOD policy is required in order to maintain security control over company data and in the long run promote a positive ROI. The technologies used to enforce the policies should be carefully evaluated based on performance, separation of personal and organizational data, usability, and enforceability and should be updated constantly.

This article is useful for this specific research study because the results of the authors' research indicate that the respondents experienced increases in productivity of greater than 20% as a result of BYOD. The authors provide possible solutions for mitigating the security risks associated with a BYOD policy, including the implementation and enforcement of policies through a MDM solution and virtualization technologies. The authors provide a solution for separating the personal and organizational data on the device through (a) dual boot, a configuration of two operating systems running on a single device, (b) hypervisors running two instances of virtualized operating systems, (c) hypervisors running virtualized applications on the personal operating system, or (d) remote desktop connections to systems within the organization's datacenter.

Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S. (2014). Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems, 28*(1), 209–226. http://dx.doi.org/10.2308/isys-50704

Abstract. The purpose of this study is to examine the factors that determine whether employees follow Bring Your Own Device (BYOD) policies through the lens of the Protection Motivation Theory. BYOD is rapidly becoming the norm rather than the exception. As a result, firms are establishing BYOD policies to address the risk inherent in allowing individuals to use their own devices to access or store company data. This paper reports the results of a survey of accounting students, non-accounting students, and full-time employees. Results demonstrate that participants' intentions to comply with a BYOD policy were primarily motivated by Self Efficacy and Response Efficacy. Further, Threat Severity was more salient for accountants than non-accountants, perhaps due to

their sensitivity to confidential data. Finally, when actual compliance behavior was considered, costs to comply were much more salient to employees and could be strong deterrents to full compliance. These findings have important theoretical and practical implications.

Summary. This research article by Crossler et al. (2014) evaluates 444 individuals (167 accounting undergraduates, 83 M.B.A. students, and 194 employees) in their response to either a hypothetical BYOD policy (if the participant was a student who had never followed a BYOD policy) or a current company policy. This study employed the protection motivation theory (PMT) to create hypotheses about whether or not the student/employee intended to or would actually comply with the BYOD policy. Five categories were used as mitigation tactics: (a) threat susceptibility, (b) threat severity, (c) response efficacy, (d) self-efficacy, and (e) response costs. Threat susceptibility, the probability the threat will affect the student/employee, and threat severity, the consequences of the potential threat, were identified as having a positive relationship to compliance with a BYOD policy. Response efficacy, the result of their actions, and self-efficacy, the belief the student/employee has the intentions to comply, also had positive relationships with intentions and actual compliance with a BYOD policy. The response cost, which is calculated as the desire to complete a task compared to the cost associated with the work or the resulting product exhibited a negative relationship with a BYOD policy. As the cost of the work performed or the resulting product increased, the authors discovered that the desire to complete the task decreased.

This article is useful for this specific research study because it assists in identifying the best delivery methodology for end user BYOD processes, procedures, and policies to

provide the highest possible positive returns. In particular, the author's findings indicate that taking advantage of the protection motivation theory results in a higher end user intent to comply and actual compliance with policies. These findings can be used as best practices when building user education into the BYOD policy.

Disterer, G., & Kleiner, C. (2013). BYOD Bring your own device. *Procedia Technology, 9*, 43–53. http://dx.doi.org/10.1016/j.protcy.2013.12.005

Abstract. Using modern devices like smartphones and tablets offers a wide variety of advantages; this has made them very popular as consumer devices in private life. Using them in the workplace is also popular. However, who wants to carry around and handle two devices; one for personal use, and one for work-related tasks? That is why "dual use", using one single device for private and business applications, may represent a proper solution. The result is "Bring Your Own Device," or BYOD, which describes the circumstance in which users make their own personal devices available for company use. For companies, this brings some opportunities and risks. We describe and discuss organizational issues, technical approaches, and solutions.

Summary. This article demonstrates the explosive growth in the use of mobile devices and highlights the trend of integrating the use of the devices directly into the professional lives of individuals. As the use of mobile devices is ingrained into the daily lives of employees, employees are returning with the plea to work from a single device instead of having one for work and one for personal use. The article articulates the risks associated with BYOD opportunities and the complexity of implementing a BYOD policy. Disterer et al. (2013) provide seven potential BYOD concepts and solutions: (a) virtual desktops, (b) session virtualization, (c) web applications, (d) application virtualization, (e) hybrid

applications, (f) native applications, and (g) virtual machines. Each approach delivers advantages and disadvantages along with technical requirements and use case scenarios. Regardless of the solution, policies for the associated platform and device are required for secure use, such as a policy stating that the device must not be compromised by malware, remote wipe capabilities must be available if data is stored locally.

This article is useful for this specific research study because it compares several technical approaches for BYOD that organizations can evaluate and apply. Seven options are identified: (a) virtual desktops, a remote session that hosts and processes the information but requires high bandwidth and low latency; (b) session virtualization, also known as terminal applications, which are server hosted applications with lower bandwidth requirements; (c) web applications, which are hosted on web servers and can be available in the public Internet; (d) application virtualization, which are sandboxed applications delivered to the device and executed locally; (e) hybrid applications, which are web applications that may run as native applications; (f) native application, which are thick installations applied directly on the device; and (g) virtual machines, virtual desktops that are run locally from the device instead of the server. The authors note that choosing an option is dependent on the application, external and internal network connections, device platform, security requirements, and delivery mechanisms, and provide guidance in determining the most appropriate solution given these parameters.

Ghosh, A., Gajar, P. K., & Rai, S. (2013). Bring your own device (BYOD): Security risks and mitigating strategies. *Journal of Global Research in Computer Science*, *4*(4), 62–70.

Abstract. The growth of mobile technology, with regard to availability of 3G/4G services and devices like Smartphone’s has created new phenomenon for communication

and data processing ability to do business. One such phenomenon that has emerged in the business environment is BYOD (Bring Your Own Device), which means that employees use their personal device to access company resources for work, inside or outside organizational environment. This new phenomenon brings with itself new opportunities but has many risks associated with it. Using mobile devices for personal as well as professional work brings with itself risks that need to be mitigated. The aim of this work is to provide various mobility strategies, defenses and measures, control aspect, management and governance aspect to look forth in implementing a BYOD strategy in an organization.

Summary. Ghosh et al (2013) identify the growing push of employees who wish to use their personal devices for work purposes. The BYOD concept was not possible until the realization of further advancements in mobile network connectivity, easier accessibility of company applications through the web, and the increased processing power of mobile devices. Benefits of BYOD range from improved employee morale to reduction in user training when implementing a BYOD policy, but BYOD does not come without additional risks and other challenges. The article introduces four security strategies: (a) here is your own device (HYOD), a complete company-provided solution including the device and support; (b) choose your own device (CYOD), a company-provided solution that allows the end user to select the device; (c) bring your own device (BYOD), where employees purchase their own device and employer policies for use must be followed; and (d) on your own device (OYOD), a solution in which employees own their devices but the organization does not provide support or policies for device use. Based on the security strategy that an organization selects, additional policies are then determined: (a)

the roles and responsibilities for managing and securing the device, (b) inventory and enrollment of the device, (c) application testing, (d) ability to apply security settings, (e) ability to update security settings, and (f) user training.

This article is useful for this specific research study because it supplies control objectives for a BYOD policy and lists each of the five components into identifiable tables for use by organizations that are implementing or modifying their BYOD policies. The authors also provide recommendations for mobile device management architecture to enforce the security objectives, including (a) identification and access control, (b) data protection, (c) application security, (d) integrity control, and (e) compliance.

Webroot. (2014). *Fixing the disconnect between employer and employee for BYOD (bring your own device)*. Retrieved from http://www.webroot.com/shared/pdf/WebrootBYODSecurityReport2014.pdf

Abstract. It's no surprise that there are many articles and papers on Bring Your Own Device (BYOD) that will advise employers on how to secure employee devices. With the exponential growth in malware and potentially unwanted apps (PUA's) during 2013, particularly on the Android™ platform, the stakes and risks have never been higher. BYOD security management adds complications that businesses have not faced before the devices are owned by employees and contain the owners' personal data. Webroot believes there is a large disconnect between how employees are using mobile security and the ways that organizations are implementing BYOD. Before conflicts start to erode the considerable gains BYOD brings to both parties, we are uncovering the realities of this disconnect to better inform employers on how to work with employees using personal or employer issued devices. To explore this disconnect, Webroot commissioned

a two-part research survey looking at employee and employer BYOD attitudes and concerns around securing personal mobile devices. The first survey took place in late 2013 and explored what employees want out of BYOD, while the second survey, conducted in March 2014, looked at what employers want for securing mobile devices. While there are some striking areas of agreement, there are also signs that many employees do not take adequate steps to protect company information, a weakness that could result in critical security breakdowns. There is also evidence that employers often only pay lip service to consulting with employees over BYOD security. This can create problems given the large number of personal devices being used for work purposes.

As a result of these research surveys, Webroot has developed an employee BYOD Bill of Rights. This tool serves as a guideline that employers can use to help bridge the security gap between employees' preferences and the security requirements of their organizations.

Summary. This article provides the results of a survey conducted by Webroot of 2,100 individuals. Of those surveyed, 41% indicated they use a mobile device for work purposes. Webroot collected information about additional security installed on the personal devices used for work purposes and the employee concerns related to (a) employer access to personal data, (b) the risk of personal data being wiped, (c) location tracking, (d) impact of security measures on device performance, and (e) increased battery consumption. Webroot also surveyed employers on their BYOD policies; the results indicate that 98% of them have BYOD security policies in place.

The survey results provide additional details on employer security concerns, remote wipe policies, and the existence of employee BYOD bills of rights. Webroot concludes with seven recommendations to fix the disconnect between employees and employers when it

comes to BYOD policies. These seven recommendations are: (a) employees/employers must have mobile device security enabled, (b) employers must educate employees about the risks of allowing BYOD and the benefits of securing BYOD devices, (c) employers should build transparent security solutions, (d) employers should address the concerns of personal privacy and security, (e) employers must protect against browser data security breaches, (f) employers must consistently enforce BYOD policies, and (g) employers can simplify the management of BYOD with mandated security policies.

This article is useful for this specific research study because it addresses specific BYOD risks and mitigation strategies to reduce an organization's vulnerabilities. To address the security concerns of both employees and the employer, a BYOD bill of rights can be used to create a transparent agreement to ensure the employee is aware of the security policies that will be enforced and the obligations the employee must uphold in the acceptable use policy.

Vignesh, U., & Asha, S. (2015). Modifying security policies towards BYOD. *Procedia Computer Science, 50*, 511–516. http://dx.doi.org/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 validate the importance of a BYOD policy with survey results from Intel and the SANS Institute. Vignesh and Asha identify a BYOD security model with three levels: (a) the organizational level, which delivers the permissions, training and network access levels; (b) the application level, which is handled with mobile device management (MDM), mobile application management (MAM) and mobile content management (MCM) for devices with locally store data; and (c) the device level, which provides enforcement of certificate authority, data encryption, multiuser access, and rooting access.

This article is useful for this specific research study because the authors identify specific risks and associated mitigation strategies for BYOD, including company application access, company network access and company data loss prevention. The authors decompose BYOD policies into distinct levels as best practices when developing BYOD risk mitigation strategies. The article provides specific security policies at the organizational, application, and device levels, which can be developed and enforced by BYOD policy and a mobile device management solution to address BYOD risks.

Conclusion

Introduction

As increasing numbers of employers tolerate employees using their personal devices at work (Armando et al., 2014), these organizations must align their BYOD policies with the organizational goals. In order to implement effective BYOD policies, those tasked with implementing and overseeing these policies must leverage lessons learned and best practices established by others. This literature review will assist those who are tasked with building BYOD policies while addressing the concerns raised from CIO/CTO's, IT security professionals, IT operational managers, and compliance teams. Selected literature in this study also identifies the concerns raised by employees that will be taking advantage of the BYOD policies, as well as offering best practices to address the employee concerns. The results identified within the literature review are categorized in three sections: (a) BYOD benefits, (b) BYOD risks and disadvantages, and (c) BYOD risk mitigation strategies.

BYOD Benefits

BYOD policies became necessary as a result of employees requesting the ability to use their personally owned devices for company use. An initial set of early adopters consisted of executives with early versions of the iPhone, and later Android devices. According to a 2013 Forrester Research study of 10,000 people, more than half of employees in the survey owned the devices they were using for work (Ackerman, 2013). Allowing employees to use their own devices for work purposes greatly reduces the capital overhead for an organization by reducing the number of devices the organization must procure for their employees and the training requirements, as the employees are more familiar with their own devices (Ghosh et al., 2013). Additionally, the devices the employees are requesting to use are often newer, with more

advanced technology available, and the employee-owned devices result in an employees taking extra care for their safeguard (Ghosh et al., 2013).

An additional benefit of allowing BYOD use is an increase in productivity. In a study conducted by Intel, the results indicated that the biggest benefit of a BYOD policy was an increase in the employees' productivity levels, which showed increases in excess of 20% (Chang et al., 2014). Allowing employees to take advantage of mobile devices opens the available applications to more than a million apps, enabling the employees to select specific apps to meet their needs (Armando et al., 2014). These employees increase their efficiency, productivity, and flexibility (Crossler et al., 2014), and 79% of employees believe that a BYOD policy could have a positive impact on their satisfaction and engagement (Fiorenza, 2013). An Intel director of consumerization was able to identify a soft return on investment (ROI) through feedback from their employees stating that the ability to use their personal devices saved 57 minutes per workday (Ackerman, 2013). As the desire for BYOD is driven from the employees, it is beneficial to listen to the employee feedback as the policies and procedures are created, maintained, and enforced (Allam et al., 2014).

BYOD Risks and Disadvantages

There were a number of risks and disadvantages associated with BYOD identified in the literature reviews. A study conducted by PricewaterhouseCoopers identified that one in three small businesses and 75% of large businesses were already allowing employees to connect personal devices to their company networks without risk mitigation steps in place (Allam et al. 2014). Vignesh and Asha (2015) note that the BYOD policies in use in most organizations are vague and typically immature. The lack of risk mitigation is particularly concerning when considering that the number of Android malware samples increased by more than 10 times

between July 2012 and January 2014, an increase of about 505,000 new malware samples (Chang et al., 2014). Webroot (2014) also notes the explosive growth of potentially unwanted apps (PUAs) that occurred in just one year (2013), particularly on the Android platform. The continuing growth of malware increases the risk that organizations take without proper BYOD policies in place. As the organizations are already defending against malicious attacks to their networks from other sources, employees' personal devices create another means from which malicious code can attack (Crossler et al., 2014).

Employees and employers have fundamental disagreements on the restrictions that should be placed on personal devices used for work purposes. Employers want to control the devices that connect to their networks, while many employees refuse to allow others privileged access to their personal devices such as admin, root, remote-wipe, or find my iPhone (Ackerman, 2013). A related concern for employers is the fact that many employees may not be taking advantage of the security tools built into their personal devices; a study by Cisco identified that the usage of a password was neglected by almost 40% of smartphone users (Allam et al., 2014). With approximately one million applications for mobile devices and a growth rate greater than the industry's ability to interrogate the applications for embedded malicious code (Li & Clark, 2013), company data is vulnerable through BYOD use and has a higher potential of being compromised, which may lead to data loss, identity theft, or lost corporate trade secrets (Allam et al., 2014).

BYOD Risk Mitigation Strategies

This research study identified various risk mitigation strategies and best practices related to the analysis, development, and implementation of BYOD policies. One option to avoid risk is to force the employee to use a company owned and managed device, but this approach may be

met with resistance and the employee may use workarounds as using a company-owned device may be considered inconvenient (Chang et al., 2014). Earley et al. (2014) note "the trick is to use transparent approaches and a light touch, rather than intrusive approaches that will only encourage workarounds" (p.3). An acceptable use policy may be used alone or in conjunction with installed software for managing the device (Ackerman, 2013).

If a software option is chosen, then a mobile device management (MDM) application can enforce the policies required by the organization prior to providing the employee's device with access to the company network (Chang et al., 2014). Chang et al. (2014) state that the "BYOD policies include identifying which devices can be used in the company network, listing both allowed and banned apps, and describing classes of data that shouldn't be stored locally after being used by a mobile app" (p.2). A whitelist and blacklist of applications should be maintained with an understanding that the blacklisted applications will never be installed on a managed device (Ghosh et al., 2013). Fiorenza (2013) recommends that the user back up his or her personal information prior to and during enrollment in the MDM in case the device is lost or stolen and a full-wipe command needs to be performed. The MDM should adhere to the company security policy to enforce passwords and screen lock capabilities (Chang et al., 2014).

Several options for mitigating the risk to company data posed by BYOD were identified in the research. The U.S. White House suggests three virtualization methods: (a) remotely access the computing resources so the data is not stored on the personal devices, (b) implement a walled garden that separates the personal and corporate apps processes, and (c) apply limited separation of the employee personal and corporate data with a requirement of security controls (Chang et al., 2014). Ackerman (2013) suggests "keeping corporate data on the device in a separate software container (which allows the user's and the business's programs to run simultaneously

without accessing each other's data)" (p. 1). Software is available such as Aurasium to perform code analysis on the applications; SCanDroid, a heuristic application that detects known malicious data flows; or secure metamarket (SMM), which is a process that investigates the applications installed on the device to ensure they meet the required security policies individually and as a group (Armando et al., 2014). Crossler et al. (2014) recommend,

> mandatory installation of security software, configuration of auto-update for software updates and security patches, the creation of security codes, the use of VPN protocols when using public Wi-Fi connections, the encryption of all company data, and the enabling of remote deletion capabilities. (p.2)

The final recommendations involve the employees and their responsibilities in adhering to the security policies. In order to best understand how to address each employee, Allam et al. (2014) adapted an Awareness Boundary Model to help determine the correct amount of security awareness to provide to a specific set of employees to ensure that their productivity, workload, and functional acceptance of the policy are at optimal levels. An organization's BYOD training program should also focus on informing the employee of the costs associated with BYOD policy compliance, the costs associated with non-compliance, and how security threats affect them personally (Crossler et al., 2014).

Summary

The use of BYOD is becoming increasingly more widespread, and due to security risks organizations should also have and enforce BYOD policies (Ackerman, 2013; Chang, Ho, & Chang, 2014; Johnson & Filkins, 2012; Mitrovic et al., 2014; Webroot, 2014). An effective BYOD policy requires investigation, knowledge, understanding, and employee feedback prior to enforcing the policies for employees (Ackerman, 2013). The benefits of BYOD include

increased employee morale, productivity, and efficiency, as well as the ability for employees to work from any location at any time (Mitrovic et al., 2014). These benefits can be best achieved by identifying the security risks associated with BYOD, and mitigating the risks to acceptable standards (Crossler et al., 2014). One of the most important best practices is to balance the flexibility provided by BYOD with necessary security policies that do not negate the end users' abilities to perform their jobs (Earley et al., 2014).

References

Ackerman, E. (2013). The bring-your-own-device dilemma: Employees and businesses seek to balance privacy and security. *IEEE Spectrum, 50*(8), 22–22. http://dx.doi.org/10.1109/MSPEC.2013.6565553

Allam, S., Flowerday, S. V., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers & Security, 42*, 56–65. http://dx.doi.org/10.1016/j.cose.2014.01.005

Armando, A., Costa, G., Verderame, L., & Merlo, A. (2014). Securing the "bring your own device" paradigm. *Computer, 47*(6), 48–56. http://dx.doi.org/10.1109/MC.2014.164

Center for Public Issues Education. (2014.). *Evaluating information sources*. Retrieved from http://ce.uoregon.edu/aim/Capstone1Perm/evaluateinfo.pdf

Chang, J. M., Ho, P.-C., & Chang, T.-C. (2014). Securing BYOD. *IT Professional, 16*(5), 9–11. http://dx.doi.org/10.1109/MITP.2014.76

Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S. (2014). Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems, 28*(1), 209–226. http://dx.doi.org/10.2308/isys-50704

Disterer, G., & Kleiner, C. (2013). BYOD Bring your own device. *Procedia Technology, 9*, 43–53. http://dx.doi.org/10.1016/j.protcy.2013.12.005

Earley, S., Harmon, R., Lee, M. R., & Mithas, S. (2014). From BYOD to BYOA, Phishing, and Botnets. *IT Professional, 16*(5), 16–18. http://dx.doi.org/10.1109/MITP.2014.69

Fiorenza, P. (2013). Mobile technology forces study of bring your own device. *Public Manager, 42*(1), 12-14.

Ghosh, A., Gajar, P. K., & Rai, S. (2013). Bring your own device (BYOD): Security risks and mitigating strategies. *Journal of Global Research in Computer Science, 4*(4), 62–70.

Johnson, K. & Filkins, B.L. (2012). SANS mobility/BYOD security survey. Retrieved from http://www.sans.org/reading_room/analysts_program/mobility-sec-survey.pdf

Li, Q., & Clark, G. (2013). Mobile security: A look ahead. *IEEE Security Privacy, 11*(1), 78–81. http://dx.doi.org/10.1109/MSP.2013.15

Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). BYOD: Security and privacy considerations. *IT Professional, 14*(5), 53–55. http://dx.doi.org/10.1109/MITP.2012.93

Mitrovic, Z., Veljkovic, I., Whyte, G., & Thompson, K. (2014). *Introducing BYOD in an organisation: The risk and customer services viewpoints.* Paper presented at The 1st Namibia Customer Service Awards & Conference, in Windhoek, Namibia. Retrieved from http://ir.polytechnic.edu.na/handle/10628/522

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

Webroot. (2014). *Fixing the disconnect between employer and employee for BYOD (bring your own device)*. Retrieved from http://www.webroot.com/shared/pdf/WebrootBYODSecurityReport2014.pdf