Bring Your Own Device (BYOD), Best Practices in a Business Environment

James S. McKinney

ICTN 6865: Fundamental Network Security

Dr. Phil Lunsford

25 November 2016

Bring Your Own Device (BYOD), Best Practices in a Business Environment

Abstract

Bring Your Own Device (BYOD) is a trending business strategy that allows employees to utilize up-to-date electronic devices that they are already comfortable with. Employers benefit from increased employee satisfaction and the reduced cost of providing and maintaining electronic devices. The application of Best Practices can help a business to profit from the BYOD approach while managing the risk. Mitigating the risks associated with BYOD such as increased potential for data leakage and the exploitation of vulnerabilities introduces a host of challenges for the Information Assurance (IA) department. Establishing an acceptable device list that identifies allowed platforms and IOS versions serves to manage the diversity of end points and minimizes threats associated with outdated software. In addition a Network Access Control (NAC) should be implemented to authenticate users and validate device security.

Introduction

Incorporating recognized best practices when implementing a Bring Your Own Device (BYOD) business strategy, could mitigate the inherent risk involved with this increasingly popular solution. "All in all, [BYOD] is about being innovative and helping your employees to work better," says Mark Coates, EMEA VP at Good Technology (Evens 2015). Accessing the potential pros and cons of BYOD and conducting an initial risk assessment are key aspects to determining if a BYOD course of action is plausible. Identifying and understanding the environment is crucial when contemplating a change of this magnitude. The establishment of boundaries, coupled with the creation of associated policies to integrate new devices is an integral part of any migration plan. That being said, only a deterministic evaluation of all applicable areas will allow for the correct decision to be made on the best way forward.

Why BYOD

Bringing your own device to work is not new but on the other hand is not old either. The concept and practice has been around for a few years and is increasing in popularity. When talking about BYOD there are two areas that have to be focused on. There is BYOD in the business environment where the individual devices are utilized by employees in their day to day activities, and there is BYOD in the work

place where employees bring their own devices for personal use. This aspect is important for security concerns but is not going to be covered in this document. Even though employees may not be set up to connect to company resources does not mean they won't attempt to connect. For this reason you must protect organizational assets from the devices designated for use with organization infrastructure and those that are not. There are primarily three areas that are considered benefits of a BYOD solution.

Employment satisfaction and retention is a focal area of the human resources (HR) department in a lot of cases. Business' work hard to find quality employees and there is a cost to bringing new employees on board. There are some that follow the philosophy that a good wage should be incentive enough but that is not always the case. Whereas a good salary is important, a large portion of an individual's time is spent at work and there is something to be said of the quality of life at that time. Being able to use the preferred technology that is well known to that individual adds to the job satisfaction. The ability to attract and keep the higher quality employee that gives an institution the most return on their investment is very important. The individual that can increase productivity and add to the knowledge base is a hot commodity. That is why it is important to work towards developing and maintaining a good employee retention program; employee satisfaction is one part of that program.

Productivity and innovation has to be taken into consideration when addressing the benefits of BYOD. The more content an individual is, the more productive they are. Today's employees want to work with cutting edge technology that they have become accustomed to in their personal lives. The other side to productivity is process and equipment familiarity. You can issue a new employee a corporate device that is locked down and controlled by internal security staff but the learning curve from an employee stand point is going to reduce his or her productivity. In contrast, if an employee comes in and is allowed to use the device that they use on regular bases the only thing to learn is how to incorporate that into a device they already know how to use.

BYOD feasibility

Determining if a BYOD solution is the appropriate strategy for any particular environment not only can be, but should be, a very detailed process. There is a lot of information available to detail the benefits and negatives of BYOD. Both benefits and negatives may or may not apply depending on the implementation and environment. There are a few of areas that need to be looked at in order to determine the impact on each when attempting to make an informed decision. Each area most likely has sub areas and all should be attended to. A broad look at the areas listed below would be a good place to start. The closer you look, the more areas that need to be addressed will present themselves:

- **Staff:** Is the IT staff robust enough to handle the increased responsibilities generated as a result of a BYOD solution? The introduction of a myriad of devices operating on diverse operating systems will create a surge in helpdesk calls that are not covered in the documented knowledge base used by technicians at tier one. An increase in mobile devices utilization will most likely cause a change in infrastructure and the introduction of technologies that may have not been present prior. There will also be an increase to the security policies and procedures that will increase the duties and responsibilities of the data center administrators. Does the IA department posses the experience and expertise to design, develop and implement the security requirements associated with a BYOD solution.
- **Network infrastructure and communications capacity:** What is the current state of the network? There will be an increase of network devices if the BYOD program is implemented efficiently. The use of an internal wireless LAN to process day to day traffic locally will not require an increase to bandwidth and will decrease the price of the organizational data plan. The installation of wireless access points (WAP) will be necessary to insure free roaming with no loss of connectivity throughout the local area. With the ability to communicate more freely, there should also be an increase to the external communication capability as well.
- **Security:** There cannot be enough said about security. To what extent security will need to be changed is directly related to the sensitivity of data and to what extent BYOD will be used. A comprehensive analysis of the policy, procedures and infrastructure is required to make this determination.
- **Cost:** BYOD is promoted as providing cost savings however, this factor is not necessarily a given. A cost analysis has to be conducted to determine if implementing a BYOD strategy is cost effective or not. To accomplish this there are multiple areas that have to be looked at. The annual cost of employee supplied devices, coverage plans and licenses as applicable. This potential savings could be offset by any plans to reimburse employees for coverage and roaming fees incurred while performing business related activities. If a reimbursement program is going to be used, the usage patterns have to be evaluated to develop an accurate projection. There is the annual cost of the life cycle management program and logistical cost to maintain this equipment. These estimated costs need to be balanced against any projected cost for resources required to ensure the integrity of organizational data and assets. The cost for securing devices will vary, for instance between a financial institute or medical facility and a retail store. All area considered and cost compiled will provide the data required to determine the level of cost savings.

Implementing BYOD

After the lengthy assessment process the decision to move forward brings you to the starting point where the BYOD program can be developed. The first step would be to define the objectives of the new BYOD program. What is expected by rolling out this new strategy? When that is complete it is important to engage the stakeholders i.e., management officials to insure that the program objectives are in line with the organizational business objectives. Stakeholder compliance is important to ensure unfettered support during the development, implementation and monitoring phases of this new program. The next step is to define and establish the program parameters.

Early on granting access to a BYOD program was limited due to the increased security risk, the more devices to worry about the more opportunities for compromise. The security protocols and processes that are available today allow an organization to extend the access to a greater number of employees. "Every employee can benefit from the increased productivity, flexibility, and efficiency that mobility offers." [11] The first step in any BYOD implementation would be to develop the policies that govern the program. Listed below are few areas that should be covered but should not be considered all inclusive. "There is no right BYOD policy." [7] Policies should be developed based on environmental and organizational business goals:

- **Acceptable use:** If you have been in the IT field or even utilized a company IT asset, you are familiar with the "acceptable use" policy. There are always those who will push the boundaries of what they can get away with. For this reason it is important to minimize vague verbiage and be comprehensive in outlining the behavior that will be accepted. This document should specify the repercussions for violations.
- **Device list:** There is an abundance of different devices on the market today which may make it necessary to define an acceptable device list. The benefits of a BYOD solution should not be overshadowed by the cost of supporting all of the devices available. If available resources allow it, that is good, but more than likely the pool of acceptable devices will need to be limited. At a minimum the operating systems that should be covered are Apple iOS, Android, and Microsoft IOS.
- **Data plans:** This policy will need to answer the question of what will be funded by the organization. Will there be a reimbursement program where the employee will submit expense reports or possibly a stipend will can be offered. There also is the alternative of offering no reimbursement or stipend relying on the employee's desire to use their own device to persuade

them to not be concerned with the cost. Either way it needs to be documented so that the employee knows upfront what the policy is.

- **Compliance:** This document should detail any and all regulations that govern the safe guarding of a specific type of data collected, used or stored by the organization. An example of this is the Health Insurance Probability and Accountability Act (HIPAA). HIPAA regulates the handling and care of data in a medical environment. HIPAA is a federal regulation and is in addition to any local security policies.
- **Applications:** Individuals download applications onto their mobile device for various reasons. Some research the validity and security in these applications and some do not. It would be a daunting task to list the all of the applications that are not authorized so a better route would be to list authorized types of applications. Examples of these applications include applications that scan IP ranges. Another would be any application that is used to store or share information and is not provided by the organization.
- **Privacy:** It should be outlined what information will be collected from an individual device. This information should be limited to device specific information only. The employee should be reassured that no personal data will be collected as it is not pertinent to the security of the device.
- **Training:** Construct new blocks of instruction to provide required training necessary to incorporate security issues associated with the BYOD implementation. This is where any additional areas of training are developed to insure the employee is knowledgeable in the handling of their device when operating in the business environment.
- **Services:** Services should be made available on an as needed base. Only those services required to perform an individual's job should be granted thus limiting accessibility to sensitive services and data. Deny by default will increase insurance that services not required are not granted.
- **Security:** This is probably the most important policy or set of policies. The details and number of policies needed will be dictated by the environment and sensitive nature of data stored. "In general, security (mainly) involves the combination of confidentiality, integrity and availability." [2]

The White House put out a "Toolkit" for government agencies interested in developing their own BYOD program. This document provides government specific areas of concern for a BYOD implementation along with three documented case studies of government agencies that developed a BYOD pilot program. As a part of the toolkit, examples of recommended policies are provided. These policies include:

- Sample #1: Policy and Guidelines for Government-Provided Mobile Device Usage
- Sample #2: Bring Your Own Device – Policy and Rules of Behavior
- Sample #3: Mobile Information Technology Device Policy
- Sample #4: Wireless Communication Reimbursement Program
- Sample #5: Portable Wireless Network Access Device Policy

Now that the boundaries and protocols have been established, define a portion of the organization to be used as a pilot test bed for the new program. This will allow for the testing of policies and procedures while minimizing the vulnerabilities with either. This group should include all areas of access and complexity that might exists after the full deployment. This is important to insure broadest testing of the BYOD program. Some key areas of concern when rolling out the program are listed below:

- **Simplify enrollment:** Complexity here often leads to non-compliance. Enrollment should be easy with minimal user interface. The device should be secured and configured during the enrollment process incorporating the signing of the Acceptable Use Policy (AUP). To ensure isolation of organizational data, all active syncs on the device should be cleared prior to enrollment. Authentication needs to be utilized during the enrollment process. This can be accomplished with a onetime pass code or through an existing organizational directory such as Active Directory (AD). The IT staff should be able to identify and isolate all rouge devices attempting to access resources prior to authentication.
- **Locate unregistered devices:** It would be rare to find an organization where not even one employee found a way to use their own device at work. It is important to locate all personally owned devices on the corporate infrastructure so that they can be incorporated into the BYOD program with all necessary security settings and restrictions. This is not a onetime activity either, this scan should be done on a regular basis to insure compliance and minimize vulnerabilities.
- **Manage devices:** This is important due to the fact that one individual may have multiple devices connected at one time. "A recent survey by iPass found that the average mobile worker now carries 3.5 mobile devices, which might include smartphones, laptops, and tablets." [4] For this reason it is important to insure that only the enrolled device is granted access to organization resources. There should be a pairing of users to devices to insure that one cannot authenticate without the other. Another purpose behind managing devices is to insure that scaling of the network as a result of the increased device count, does not compromise the network infrastructure. Managing devices and monitoring usage will provide the network engineers the

required information to scale the network as needed to keep up with increasing demand while optimizing resources.

- **Data usage:** Data usage should be monitored. Emphasize the importance of using WiFi when available. An automatic WiFi configuration would be beneficial in this case. If the data plan is paid by the organization, it would be prudent to track usage. In addition data rates should be negotiated with carriers. It is possible to get a better rate based on volume. If the plan is to reimburse the employee for data usage, it would be prudent to insure company related usage corresponds with employee expense reports. If the data plan provides a stipend, employees would appreciate a warning when they approach the threshold where if exceeded they will be responsible for any additional charges. Set thresholds and send out warning when those thresholds are approaching.
- **Organizational data:** It is a good idea to manage the organizational data that is downloaded, copied or transferred to a personal device. When caring for sensitive data, the disposition of that data is a key security concern. If a copy is made, all activity, coupled with the final disposition of that copy, has to be documented. A Virtual Desktop Infrastructure (VDI) would allow an employee to utilize data as needed without having to download and store the data on the end user device. A VDI infrastructure would allow the flexibility to use a preferred device for all applications not handling sensitive data while offering a secure environment when accountability is critical.
- **Keep data separate:** It is important that the personal data belonging to the employee is kept separate from the organizational data. This protects both the employer and the employee. It is also important to assure the employee that their privacy is a concern of the organization. An emphasis on separation as a tool to protect them serves as a tool to protect organizational data also.
- **Bandwidth management:** With more devices being brought onto the organizational WiFi infrastructure, Quality of Service (QoS) will become an issue. A strategy to limit bandwidth based on duties and responsibilities assign to a user/device pairing, will optimize available bandwidth resources. A higher bandwidth allocation where voice and video is required and a rate limit where only basic applications are used, will work towards improving network reliability.

The development of the BYOD program must also include a migration plan that will allow for transition with minimal impact to the business operations. This too will be tested and evaluated when the established inner organizational pilot program is rolled out to the few employees selected. The pilot program should not run to long, but long enough to collect the data required for conducting an evaluation

of the BYOD program. Continuous monitoring should begin as soon as the program is initiated. Monitoring is an important aspect of the program. This process will also be evaluated to insure program compliance and security vulnerabilities can be identified and resolved as early as possible. All data collected through the evaluation of the pilot program should be placed in a repository for analysis. Use this data to analyze the effectiveness of policies and procedures, impact to the infrastructure and user satisfaction. Improved productivity as a result of user satisfaction is a big benefit to a BYOD strategy, but it cannot come at the expense of information security. Refine the BYOD program as needed and develop an organizational migration plan.

Conclusion

BYOD is becoming more feasible with the improvements to technologies. They provide more secure communications along with improved security for the handling and processing of data. Corporations, government agencies, financial institutions, and health care providers who deal with sensitive and or classified information are now looking closer at BYOD as possible business solution to reduce cost and improve performance. "Gartner Inc. predicts that by 2017 half of all employers will require their employees to supply their own devices for work purposes." [11] How and to what extent BYOD can be used is wholly based on the target environment. There are consulting firms that have the expertise, knowledge base, insight and resources to assist. By conducting a comprehensive audit of the organization's business goals, IT infrastructure, policies and procedures, a custom plan can be developed to implement a BYOD program that optimizes resources and minimizes cost on a long term basis. Best practice for implementing a BYOD solution in a business environment; contract with an organization that specializes in providing the best solution for your requirements.

Works Cited

1. Ssekibuule, Richard. “MOBILE AGENT SECURITY AGAINST MALICIOUS PLATFORMS.” *Cybernetics and Systems* 41.7 (2010): 522–534. Web. 5 Nov. 2016.
2. Betarte, Gustavo, and Carlos Luna. “Formal Analysis of Security Models for Mobile Devices, Virtualization Platforms, and Domain Name Systems.” *CLEI Electronic Journal* 18.3 (2015): 3:1 – 3:30. Web. 5 Nov. 2016.
3. Harvey, Melissa J., and Michael G. Harvey. “Privacy and Security Issues for Mobile Health Platforms.” *Journal of the Association for Information Science and Technology* 65.7 (2014): 1305–1318. Web. 5 Nov. 2016.
4. Romer, Hormazd. “Best Practices for BYOD Security.” *Computer Fraud & Security* 2014.1 (2014): 13–15. Web. 5 Nov. 2016.
5. Bürkle, Axel, et al. “Evaluating Mobile Agent Platform Security.” *Lecture Notes in Computer Science*. N.p.: Springer Science + Business Media, 2006. 159–171. Web. 10 Nov. 2016.
6. Product of the Digital Services Advisory Group and Federal Chief Information Officers Council. “Bring your own device.” *Whitehouse.gov*. The White House, 16 July 2012. Web. 10 Nov. 2016.
7. IBM Security. “The Ten Commandments of bring your own device (BYOD).” *IBM.com*. 12 Aug. 2016. Web. 21 Nov. 2016. In-line Citation:
8. Rubin, Ilan. "9 Best Practices for BYOD in the Industrial Environment." Pace, 10, 2013.
9. Stevens, Katie. “Strategic Bring Your Own Device.” *Protiviti.com*. n.d. Web. 10 Nov. 2016.
10. McCrea, Britget. “9 IT Best Practices For BYOD Districts.” THE Journal 42.1 (2015): 26-28. Education Research Complete. Web 19 NOV 2016
11. "10 Smart Strategies for BYOD Success." Information Management, vol. 49, no. 6, 2015., pp. 19