Skyler Booth

Legal and Social Informatics of Security

Sameer Patil

March 9th, 2017

Company X’s Bring Your Own Device Policy

**Introduction**

This policy has been put in place for the employees under Company X. This document explains the procedure, security, and policies for the use of personally-owned electronic devices, such as cell phones, tablets, and laptops of employees of Company X in order to access Company X’s files, databases, and other company resources. All employees are subject to this policy and are required to adhere to it. This policy is separate from Company X-owned devices which has its own policy.

**Objectives**

The objective of this policy is to establish the guidelines and terms of use for personally-owned electronic devices of employees of Company X. Its goal is to protect Company X from security breaches, privacy incidents, and protect sensitive data pertaining to the company’s clients.

**Requirements**

All personally-owned devices must be approved by Company X’s IT department before use. The IT department will be installing three pieces of software, a Mobile Device Management (MDM) system, an anti-malware software, and a remote-wipe software. The MDM will create a partition in your data in order to separate your business data from your personal data and will be used for all business-related tasks. The MDM application will always require a user login in, in order to protect business data. All devices must update any software when new versions are available, this includes operating systems. If a major issue/bug is announced by a device manufacturing company and it applies to your device, immediately take it to the IT Department to resolve the issue.

*Acceptable Behavior*

* Working on Company X business
* Completing tasks that pertain to your job requirements
* Turning the device into the IT Department if there is suspicion the device is compromised or has malware on it
* Turning on vibrate or silent mode during company meetings where the device is not required

\*This list is not exhaustive and other work-related behavior is acceptable.

*Non-Acceptable Behavior*

* Transferring data to unapproved devices or non-business networks
* Doing non-work related activities (i.e. checking social media, texting, ETC.)
* Removing any company installed software
* Violating other Company X policies
* Storing company information outside the MDM
* Backing up data on cloud services

\*This list is not exhaustive and other non-work related behavior is not permitted

*Acceptable Devices*

* iPhones (iPhone 5 or newer with iOS 8 or newer)
* iPads (iPad 2 or newer with iOS 8 or newer)
* Mac-OS laptops (Mac OS X Snow Leopard Version 10.6 or newer)
* Windows laptops (Windows 7 or newer)

*Unacceptable Devices*

* Jailbroken or modified devices are not permitted
* Any device that isn’t listed under the acceptable devices section

*Security*

* All BOYD devices must have a secure password on their device that isn’t the same as their password on their MDM account
  + Company X defines a strong password as a minimum of 12 characters, with at least one of each of the following: an uppercase letter, a lowercase letter, a special character, and a number. The password may not contain dictionary words or names.
* The device must be set to automatically lock after being idle for no longer than 5 minutes.
* The devices auto-wipe after 10 failed login attempts must be enabled
* The device must be remote-wiped if the device is lost, stolen, hacked, or damaged
* Only approved devices may connect to the Company X network
* Many applications are not allowed, consult with the IT Department to get the most recent list of approved apps and software.
* All devices must have privacy screen protectors installed
* Employees must attend two security awareness training events a year pertaining to personally-owned devices in the workplace

\*If you are questioning if your device or a certain action is acceptable, refer to management or the IT Department

**Privacy and Inspection**

Company X will respect employees’ rights to privacy and only request access of the personal device to install/maintain Company X’s MDM and anti-virus software or to investigate violations of this policy or any other policies Company X has. Any proof of violations on personally-owned devices can and will be used for disciplinary action, and in extreme cases, a court of law. Company X will only monitor activities on the device that are within the MDM sector of the device. Shall your employment with Company X cease, you are required to give the IT Department all of your approved devices in order to wipe all company data and remove company software.

**Off-Site Behavior**

Employees are expected to follow all these guidelines whether they’re working in the office, at home, or while visiting a client. However, the information an employee is allowed to access is different when it comes to working outside of Company X’s network. Only the following information will be available for access on the MDM:

* Contacts
* Email
* Calendars
* Non-critical documents

**Adherence/Violations**

This policy applies to all employees of Company X. All employees are not only expected to follow this policy, but also required. If this policy is violated in any way, the violator will have be written up. If the same employee violates the policy for a second time, all privileges of using a personal device revoked. The third violation will result in the employee’s employment being terminated. In extreme cases, such as transferring Company X data to a non-approved device or network, can result in legal actions in addition to termination of employment. Violations will be reduced by one level for every year without a violation, i.e. if an employee has two violations but doesn’t get a third for an entire year, the employees violation status will go back down to one and they will be given privileges back.

**Disclaimer**

By virtue of employment within Company X, you hereby acknowledge this policy and agree to follow it. If you violate this policy in any way, you will be subject to disciplinary action as guided by the adherence/violation section. Company X is not responsible for reimbursement if an employee’s phone bill increases due to an increase of data use or phone calls resulting from work-related tasks. If you do not want to adhere to this policy, do not bring in your own devices to the workplace and only use company-issued equipment for all business matters. If you have any questions about this policy or the reasoning behind any aspect of it, contact your supervisor or the IT Department to get clarification

Justification

**Requirements**

First of all, the Mobile Device Management software would be installed for a few reasons: First, it would allow the employees to have all their work data saved in one location. Second, it would allow for the company’s secure, HIPAA compliant, encrypted email system to be installed, as well as a secure browser and an application catalog to allow the company to update and maintain the applications used for business applications. This software doesn’t only help the company manage its employees, but it adds an extra layer of security by adding a second password-protected layer as well as keeping the data encrypted. The software also leads to more usability by partitioning business data and personal data which allows an employee to securely work on business matters or easily switch to personal activities. The software MDM system allows the disabling of applications during certain times or locations, which enables to company to disable unapproved applications during work hours or at work locations. Finally, the MDM systems complies with HIPAA guidelines, “ensuring the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit” by allowing authorized employees to access e-PHI’s anywhere they need as well as keeping confidentiality and integrity by requiring a sign-in to access the files, which means unauthorized user cannot see or edit the files (HIPAA Journal). It also fulfills HIPAA requirements because it implements access control as well as a mechanism for authentication.

The next requirement of the policy is that all users need to have an anti-malware software installed by the IT Department. This is solely to increase security. All companies experience some sort of attack through viruses, worms, or other malware in order to disrupt company activities, steal data, use resources, ETC. The anti-malware software is a safety precaution against these attacks as well as a compliance action for HIPAA. HIPAA guidelines state, “Identify and protect against reasonably anticipated threats to the security or integrity of the information”, which this anti-malware is doing, the threat of malware attacks is anticipated and the software is protecting against that threat (U.S. Department of Health and Human Services).

Another requirement of the policy is that a remote-wipe system must be installed. This a precaution if the employee were ever to have their device stolen, lost, hacked, or damaged, the company can erase all the company’s files from the device. This complies with HIPPA by taking all patient data, as well as all company data, off of a device which allows the data to remain confidential and maintain its integrity. HIPAA also requires that there are “procedures for removal of ePHI from electronic media before the media are made available for re-use”, which this software accomplishes by giving the company the ability to wipe all data on a given device at any given time (HIPPA Journal).

Updating and maintaining software and operating systems is the next requirement of the policy. This requirement aims to increasing the protection of data stored on the devices. The increased protection is a result of updating software because software companies are always testing their products and searching for security holes/bugs and patching the issues, if a user is constantly updating their software, they keep all their software as secure as possible.

The next requirement is reporting your device to the IT Department if a device manufacturing company announces a known bug or issue with a device. This was added for two reasons: the first is to investigate if the device has been compromised and the second is to quarantine the device until the known bug or issue is fixed. This is a security precaution that follows HIPAA guidelines by maintaining data confidentiality and data integrity. It also follows the HIPAA requirement to “identify and protect against reasonably anticipated threats to the security or integrity of the information (U.S. Department of Health and Human Services)”.

Acceptable behavior and non-acceptable behavior are the next two sections of the policy. These sections are for usability and policy understanding. These sections lay out basic do’s/do not’s that the policy has laid out in other sections. This allows employees to understand what is acceptable and what isn’t. These sections also make note that they aren’t exhaustive, so there are other behaviors that may or may not be acceptable, which allows the company to manage situations as they see fit.

Another section of the policy is the guidelines for approved and non-approved devices. The reasons the list of approved devices is short, is for compatibility with the MDM software as well as the anti-malware software. This allows the company to use one program for each and the IT Department only has to manage those 2 programs instead of having multiple MDM’s and anti-malware programs that have different methods of operation and different programs. The purpose of this is to allow uniform operations throughout the company, in other words an employee may have a device go down but they can pick up any other device and they will know exactly how to get their work done since they all use the same programs. There is a trade-off here with security though, that trade-off is that if a hacker gets into the MDM or past the anti-malware software, that bug is present in all the devices that the company uses. However, I believe a hacker can accomplish the same damage if there were multiple MDMs in place, if the hacker got into one system, he can still access all the devices that run on the one system and can access all the resources in the system. I also think that having all the resources for the company in many different programs allows hackers to find the weakest one and attack it, instead of being forced to choose the only one that would be available to hack. So there is a trade-off for security with usability, but I believe the security trade-off is minimal and the usability gained is better for the company.

The next section of the policy is the security protocols for the devices. This section is full of good security practices that we have discussed in class this semester, such as strong passwords, auto-locking, device lockout/wiping contents, ETC. Most of the security practices laid out in this section have a trade-off with usability. For example, the password policy is very strict by having to use a variety of characters from four distinct character sets as well as the password not containing names or words from the dictionary. This policy restricts usability because it requires a lot more effort by an employee to remember as well as enter a complex 12+ character password versus a 4 digit pin. However, the sensitivity of electronic Protected Health Information (ePHI) not only calls for this level of security but HIPAA requires it in its frameworks. That is why the security principles in the security section are very strict and can be viewed as not the most user friendly principles.

**Privacy and Inspection**

This section of the policy addresses how the employee’s privacy will be affected by the BYOD policy. One big trade-off with BYOD policies is employee’s privacy concerns. This section of the policy aims to mitigate the intrusion of employee’s privacy by only being able to monitor activates within the MDM. The gives employees the privacy they have the right too on the personal sectors of the device, however this does limit the company’s ability to determine if an employee is using his or her device for a non-work related manner during business hours. I believe the privacy of the employee outweighs this concern and employees should be given the benefit of the doubt. I also think that the violations section of the policy will mitigate the non-work related uses of the device since the punishments give zero leeway.

**Off-Site Behavior**

This section applies to how employees are expected to act when they’re operating outside of the company network. The reason employees are only allowed to access non-sensitive documents, calendars, contacts, and their email is strictly for security. The company cannot verify how protected other networks are that an employee connects their device too, so the best thing to do is to not have any critical data on the device if it is connected to a potentially unsecure network. The other reason they can only access these things is because there isn’t a need to access anything else. The requirements document says non-sales employees only use telecommunications during the weekends or evenings. The document also says that the sales personnel are working on the go, but to do their job, sales personnel don’t need to access any of the sensitive data. This means that there is no reason that sensitive data should be on employees devices when they aren’t in the office, if it was on the devices, it only leads to more vulnerabilities with no benefits.

**Adherence/Violations**

In order to address violations of the policy, this section was implemented. The punishments may be seen as unfair or unjust, but I feel that bringing your own device is a privilege, not a right. That’s why there is a three strike policy, the first is a write up, the second is the loss of privileges, and the third is termination. However, I do believe in second chances, so this policy allows an employee to gain privileges back if they have one full year without a violation.

**Disclaimer**

The disclaimer section addresses that all employees are expected to adhere to the policy and that being a member of the company requires them too. This section is in place in order to stop employees from claiming that they didn’t know about the policy or they didn’t sign a consent form for it by stating that being a member of the company requires your adherence. This section is also important because it gives employees a way to opt-out of the policy by never bringing in their own devices and only using company-issued devices.

While there are trade-offs between security, usability, and privacy, I believe my BYOD policy is effect. I believe my policy not only achieves the needs for the company, but according to the HIPPA Journal’s HIPAA compliance checklist for technology, the policy meets all of the HIPAA requirements. This policy isn’t only effective but it meets all laws and guidelines and that’s why I believe this policy is just.

Connection to Class

The first connection to the class is with one of the first activities we did in class, the threat modeling and stakeholder analysis. When I was creating the rules for the security principles of the policy, I though back to this activity and even went through the guidelines for it.  I found the stakeholders, such as employees, upper management, patients, insurance companies, ETC. as well as took their incentives, motives, and influences into consideration (profits, privacy, and security). I also analyzed threats of security and privacy, such as hacking, data leakage, and data integrity. All of these factors help me tailor the security principles to cover all of the interests and threats. An example of the stakeholder influence was implementing only one MDM software system, this allows the company to only maintain one system which is cheaper than having multiple systems as well as not needing as many IT members dedicated to supporting the system. An example of the security analysis is requiring the auto-wipe software on all platforms. This protects against data leakage and keeps data secure because any device that is lost, stole, hacked, or damaged can be remotely-wiped before a potential leakage ever happens.

The next connection to the class had to do with Massey et al.’s work, *Evaluating existing security and privacy requirements for legal compliance*. This paper helped me understand how to evaluate legal compliance with regards to security and privacy. Even though this is a policy and not a software system, the same rules applied. I was able to evaluate the policy according to the legal components of HIPAA to make sure that the policy complied with all of them. I found that the policy I laid out reached all of the requirements of HIPAA which is necessary since the company is subject to HIPPA because it deals with patient information from hospitals.

Another connection to the class that influenced my policy was *Usable Security Why Do We Need It? How Do We Get It?* by M. Angela Sasse and Ivan Flechais. After reading this article, I realized that it is easier to start thinking of security in the very beginning when creating a system, or in this case a BYOD policy. So I based my entire policy off of effective security, from doing threat analysis to implementing security principles, I made sure I thought of security throughout my implementation of the policy. This was a super effective strategy, I was able to easily add my security policies in the beginning instead of trying to add them at the end and tailor my policy to have some security in it, which is exactly what the authors found in their research.

The YouTube video “Security Fatigue” produced by the National Institute of Standards and Technology was another inspiration for different aspects of my BYOD policy. The video explains the finds of their research, users do not like making security decisions and the more they make, the harder the decisions become and they rely on habits to make them. This usually leads to bad decisions and/or bad security practices (NIST). That’s why I had many of the security decisions be implemented into the MDM. For example, the MDM does not allow access to any sensitive files by devices if the device is not on Company X’s network. Another example is the MDM auto-encrypts all of the data saved on the device as well as encrypts all emails sent by the device. These are just some of the instances that are in the policy that I have to take the burden of security off of the user.

A combinations of two papers also helped me when writing the policy, *An overview of social engineering malware: Trends, tactics, and implications* by Sherly Abrahamand *Understanding and transforming organizational security culture* by David Lacey. The first reading is about an emerging tactic used by hackers called social engineering, it is a psychological attack the entices a user by greed, curiosity, fear, or empathy. The second article is about understanding security culture, or how an organization feels about or understands security, and how to improve or change that culture. Abraham’s article helped me understand what social engineering is and how successful attackers have had with it. It also showed what consequences it can have on a company. The biggest threat for security is employee awareness and that is another reason why social engineering attacks are so successful. When writing my policy, I took these threats into consideration, which is why I stated that employees must attend two training events a year. This was a solution in Lacey’s work to increase security awareness in a company and to help employees be more security conscious. That’s why I implemented awareness training into my policy, there are many threats that can be solved just by increasing awareness and training employees to become more familiar with security risks.

The next connection to class that I used in my Bring Your Own Device policy, was the in-class activity we did regarding understanding privacy policies.  The activity helped me in a few ways: the first was general knowledge of how policies are laid out and what kind of wording they used. This was very beneficial to me since I’ve never really read a privacy policy in its entirety, let alone write one. The other benefit was, the discussion of the policies help us find weaknesses in them. The biggest one was transparency, very little explanation was given in the policies as to why something was a certain way or a way to find out why it was written a given way. The experience helped me in creating my policy because I realized I didn’t like policies that had no explanation, so for things I deemed non-obvious, I added in the reasoning or the why to something that was in the policy. I also knew that I didn’t want to add reasoning for everything, it would take up too much text and employees would be less likely to read the document. For this reason I added a note in the disclaimer giving employees who were curious about the policy a method of contacting management in order to get answers to their questions.

The last connection to class that was used when creating my BYOD policy, was the video we watched in class about the lost iPhone. This was a story covered by ABC News where an Apple employee left a prototype iPhone in a bar where it was later discover and shown to the world (ABC News). Company X may only be a financial company that specifies in patient matters at various healthcare facilities throughout the US, but a very similar thing can happen to them. Just like in the story, an employee can take their personally-owned device that they have work-related data on to a bar and up losing it because they’ve had a few to many drinks. That’s why the policy requires employees to have a remote-wipe system installed by the IT Department. If the employee was ever to loss their device or have it stolen, the company can easily have all the data on the device removed. This allows for the data to remain confidential and keeps its integrity. So this video helped me realize some of the insider threats that can happen and how to implement solutions to solve the threats, such as misplacing a device with company data on it.

Works Cited

ABCNews. "IPhone's Next Generation Found in a Bar." *YouTube*. YouTube, 20 Apr. 2010. Web. 09 Mar. 2017.

Abraham, Sherly. "An Overview of Social Engineering Malware: Trends, Tactics, and Implications." *An Overview of Social Engineering Malware: Trends, Tactics, and Implications*. Technology in Society, Aug. 2010. Web. 09 Mar. 2017.

Berry, Megan. "BYOD Policy." *IT Manager Daily*. IT Manager Daily, 30 Oct. 2013. Web. 08 Mar. 2017.

HIPAA Journal. "HIPAA Compliance Checklist." *HIPAA Journal*. N.p., n.d. Web. 08 Mar. 2017.

Kelley, P. G., Bresee, J., Cranor, L. F., & Reeder, R. W. (2010). A “Nutrition Label” for Privacy. In Proceedings of SOUPS 2009, Mountain View, CA, USA.

Lacey, David. "Understanding and Transforming Organizational Security Culture." *Emeraldinsight*. Information Management & Computer Security, 2010. Web. 09 Mar. 2017.

Massey, Aaron K., Paul N. Otto, Lauren J. Hayward, and Annie I. Antón. "Evaluating Existing Security and Privacy Requirements for Legal Compliance." *SpringerLink*. Springer-Verlag, 13 Nov. 2009. Web. 09 Mar. 2017.

National Institute of Standards and Technology. "Security Fatigue." *YouTube*. YouTube, 09 June 2016. Web. 09 Mar. 2017.

Sasse, M. Angela, and Ivan Flechias. "Usable Security Why Do We Need It? How Do We Get It?" *Usable Security Why Do We Need It? How Do We Get It?* (2005): 13-30. 5 Aug. 2005. Web. 9 Mar. 2017.

U.S. Department of Health and Human Services. "Summary of the HIPAA Security Rule." *HHS.gov*. U.S. Department of Health and Human Services, 26 July 2013. Web. 08 Mar. 2017.

SHRM. "Electronic Devices: Bring Your Own Device (BYOD) Policy." *SHRM.org*. Society for Human Resource Management, 17 June 2014. Web. 8 Mar. 2017.

Wang, Jason. "How Do I Become HIPAA Compliant? (a Checklist)." *How Do I Become HIPAA Compliant? (a Checklist) - TrueVault*. TrueVault, 30 Oct. 2013. Web. 08 Mar. 2017.

Wikipedia. "Mobile Device Management." *Wikipedia*. Wikimedia Foundation, 04 Mar. 2017. Web. 08 Mar. 2017.