https://doi.org/10.48009/4_iis_2016_254-259

Issues in Information Systems
Volume 17, Issue IV, pp. 254-259, 2016

LEGAL ETHICS AND CONCERNS WITH SECURITY IN A BRING YOUR OWN DEVICE PROGRAM

Misty D. Kiernan, Middle Georgia State University, misty.kiernan@mga.edu

ABSTRACT

When considering a Bring Your Own Device (BYOD) program there are many components to take into consideration. A Higher Education Institution may wish to conduct a risk assessment of their current security issues and how data is stored and accessed. In order to remain compliant an institution is required to know and understand the Federal and State laws, acts, and compliances (FERPA, HIPAA, HITECH, and FISMA) that apply to their data and business. This knowledge will assist with developing a BYOD program in order to protect the employer's and the employee's rights. Once a policy or program is established, it needs to be monitored, tested, and revised as needed in order to remain not only secure, but also compliant. Security risks are ever present and evolving while laws are continuously changing; therefore, a good program must be able to flex, grow, and adapt to maintain the necessary protection.

Keywords: BYOD, Security, Risk, FERPA, HIPAA, HITECH, FISMA

INTRODUCTION

When considering a Bring Your Own Device (BYOD) Program for any enterprise, there are many Information Security (IS) risks, as well as Federal and State laws, acts, and compliance issues that must be addressed. These are important to protect both the employer and the employee while allowing the employee to use their own mobile device to conduct company business. One must also understand the needs of the organization, type of employees that will access the system, data that must be protected, and type of methods or ways the data will be accessed. By detailing this information up front and setting clear expectations as to how to prevent, report, and handle any violations from the start, both parties could be protected. For most Higher Education institutes, the thought of BYOD usually revolves around support, bandwidth, and cloud storage. There was not much to be found in relation to the federal and state laws that could affect the use of a BYOD Plan on campus.

RQI: Does the current security literature fully address BYOD issues in Higher Education?

LITERATURE REVIEW

In DeFronzo's (2016) Information Security Guardrails, he details the steps that his organization, a Mortgage company, used in order to develop their security policy. The first step was a risk assessment. During this risk assessment they discovered nine initiatives to bolster the IS program: complete data and risk inventory, test and train for employee awareness, utilize a two-factor authentication, identify and monitor hardware devices on the network, establish security incident and event management policies and protocols, review and document outside vendors and partners security, segregate data, establish patch management policies and procedures, and develop a business continuity plan in case of a breach. The next step they detailed was employee training. Finally, they created their security incident response plan. This plan also took into consideration that federal and state regulators require different responses to breaches. The federal regulations are more concerned with Personally Identifiable Information (PII), while state regulations vary by state and primarily deal with notification requirements to consumers. Also, DeFronzo pointed out that state incident response requirements are based on where the consumer lives, not where the company branch is located; so all 50 states' requirements may need to be addressed in an incident response plan (DeFronzo, 2016).

One of the issues DeFronzo (2016) saw during his company's risk assessment was with their BYOD program. The BYOD users were not being smart while utilizing their mobile devices to connect to WiFi. They were connecting anywhere with no protection while conducting business. This led to better established procedures to protect their

data and more stringent processes for accessing this same data. He then went onto state that "The first line of defense to cyberthreats is employee training." (DeFronzo, 2016, p. 4)

In Rose's 2013 article, they address the fact that it is important for every organization to establish a privacy and security program with a committee to manage the policies, procedures, and training that must come out of this program. It also addresses the importance for members of this committee to have an understanding of the various laws that will affect this program, such as the Federal Rules of Civil Procedures (FRCP), Freedom of Information Act (FIA), Federal Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), Genetic Information Nondiscrimination Act (GINA), USA Patriot Act of 2001, Privacy Act of 1974, State laws, and United States Code Title 42 (Rose, 2013). Staying in alignment with these laws and reflecting how the organization plans on protecting their data in accordance to these laws are critical. A BYOD program will need to also look at these same laws, no matter the industry, in order to ensure that all bases are covered.

This same article by Rose (2013) also addresses the importance of education and training. A program is only as good as the training provided and if the employees are not aware of the policies and program and its importance, they will not follow them which will develop issues and problem areas (Rose, 2013). Education and training must not only provide manuals, tutorials, and other resources, it also needs to include regularly scheduled face-to-face training, year round online training, a help desk, recognition weeks, newsletters, and mock audits (Rose, 2013).

While simply having an information security policy; as Chen, Ramamurthy, and Wen point out in their 2012 paper "human beings are still the weakest link in the information security chain" (p. 2). This also reflects back to Rose's (2013) article that education and training are keys to a viable security policy. It is one thing to have a policy, but the employee must also be aware of and understand the importance of the policy and how their actions can help prevent violation of this policy. Back to Chen, Ramamurthy, and Wen's research, the most frequent security-related incidents were caused by virus and malicious software infection. Employee education could help prevent or at least lessen these kinds of incidents and if an employee is made aware of the policy and punishments for not following the policies and procedures this could also cut down on the second-most frequent incident of insider security-related abuse (Chen, Ramamurthy, & Wen, 2012).

Now granted having a security policy is not going to make employees behave so there must also be a balance in assuring security doesn't limit an employee so much that they simply bypass it in order to perform their job (Chen, et al., 2012). Chen, et al. goes on to look into how employees will react if provided a punishment or a reward for breaking or following policies. After much research and data collection they discovered that the severity and certainty of punishment seemed to work the best with significance of reward following closely behind. Although many of the participants felt that punishment was unmotivating and believed that a reward would be more motivating (Chen, et al., 2012). Rose (2013) offers up "Recognition weeks" as part of the education and training portion of a privacy and security program. It goes on to list examples for this as fairs, prizes, and organizational activities as part of the recognition. Not only is this a good way to reward good security policy procedures, but this could also be a great way to encourage employees to show up for important education and training activities.

Risk assessment can be analyzed deeper depending on the organization and the type of business they conduct. Typically, there are three levels of risk: operational, functional, and strategic (Raggad, 2010). All three of these risk levels must be evaluated and considered when developing a security policy. By building policies to diminish or avoid risk in these areas, an organization can protect its assets, enhance potential growth, and create distinction in a competitive market (Raggad, 2010). Raggad also goes on to point out that organizations must develop proactive plans instead of reactive, in order to be truly successful in a competitive market.

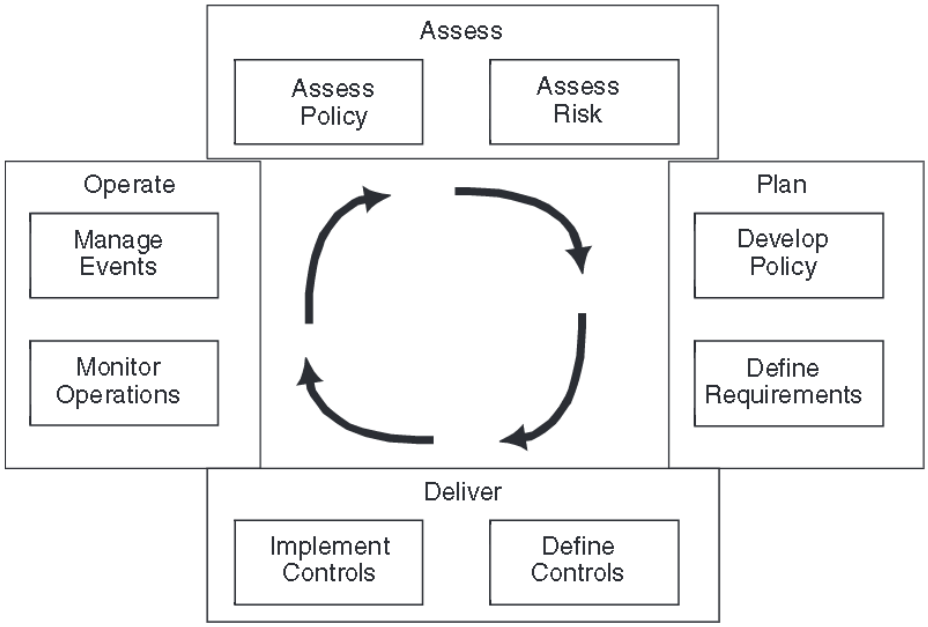
Now Rose (2013) feels security policies must also be implemented at the top of the organization and utilized throughout the entire culture in order to be the most effective:

> Two keywords in the definition of information governance are "trustworthy" and "control." These two words are vital when implementing and instilling sound privacy and security practices throughout an

> organization. Like information governance, privacy and security practices must come from the top down and be woven into the culture of an organization (p. 54).

She also goes on to state that continuous monitoring and testing are critical to ensure that a security plan is working and still viable (Rose, 2013). This is reflected well in the below image from Baskerville, Straub, & Goodman's 2008 book. It details a cycle that helps to drive home the idea that a security plan should be reviewed and continuously evolve based on the ever changing technology and organizational needs. This image shows the four phases as Assess, Plan, Deliver, and Operate. Within these phases they are further broken down into these major activities: assess policy and risk, develop policy, define requirements, define and implement controls, manage events, and monitor operations (Baskerville, 2008).

Figure 2.8 **PFIRES: Policy Framework for Information Security**



Source: Adapted from Rees, Bandyopadhyay, and Spafford, 2003, p. 102.

Using the same model detailed in the image above, one could apply this to the organizations' BYOD plan in relation to the FERPA, HIPAA, and other privacy laws. This will assist with maintaining a current policy which reflects the evolution and changes of these regulations. While following this framework and keeping the specific regulations that apply to the institution as the center of this model, an effective, current BYOD Plan would be possible.

Looking at DeFronzo's organization's steps, employee training is also critical to an information security plan. According to D'Arcy, Herath, and Shoss's 2014 research, employees are seen as a major threat to most organizations' information security plans. D'Arcy, et al. devoted their entire research to studying stress caused by IS policies. They referred to this particular type of employee stress as security-related stress (SRS). SRS overload is due to more work being created for an employee in order for them to meet security requirements (D'Arcy, 2014). Due to this potential SRS overload, employees often choose to bypass the security processes in order to get their work done (Chen, 2012). It takes a balancing act for an organization to find the proper amount of security without causing SRS overload on their employees and offering plenty of training and rewards could help employees cope better with SRS (Chen, 2012, D'Arcy, 2014).

Meyer (2016) addresses the risks to an enterprise that allows BYOD in regards to security, mobile management, access, and usage. She does not however, spend any significant amount of time on which acts and laws to address in a BYOD program in order to protect their employees' rights. She simply lists a few at the end of her article as

potential compliance requirements, such as HIPAA, FISMA, PCI, NERC/CIP and these are primarily related to protecting the enterprise in case of noncompliance and not so much their employee (Meyers, 2016). FERPA is another compliance requirement a BYOD plan or policy should take into consideration. An employee that has a child in school, or they are in school themselves, could potentially use an app on their mobile device to check grades or teachers' notes. This data is now possibly accessible to the enterprise. If a company receives a warrant for information that has been accessed on their servers through mobile devices, this student data would fall under FERPA. FERPA states that only a student or their family should have access to this information.

FERPA protects personally identifiable information (PII) of students to prevent their educational information from being shared without their consent (US Department of Education, 2014). According to a 2013 PBS survey, almost half of the teachers in the United States use technology in the classroom. Over a third of these same surveyed teachers use a mobile device in the classroom and 65% claim this technology assists with classroom demonstrations (PBS, 2013). With a greater number of teachers, parents, and students using mobile technology to access online education information, educational apps, and student records protecting PII under FERPA is becoming even more challenging for schools. These same challenges can bleed over into an enterprise situation with the utilization of a BYOD program for employees.

Or on the flip side, a school that allows students and teachers to use their mobile devices to access the school network is at risk of FERPA violations. Besides the obvious concern of a device being lost or stolen, information that is gleaned through the downloading of free apps, storing information in the Cloud, cookies, search engines, and many other methods used by advertisers to collect data could lead to a potential risk of violating FERPA (Tudor, 2015). There are stiff fines for FERPA violations (U.S. Dept. of Ed., 2014). Schools have to be extra diligent in assuring student records are kept secure, but with the ever increasing use of applications to monitor and offer services to students what is considered protected under FERPA is constantly being questioned. (Tudor, 2015).

In Mooney's (2014) article on Mobile Risks Demand C-Suite Action!, he also does not address FERPA within the context of his article, but it is mentioned in an Exhibit listing questions to ask a CFO. This Exhibit, titled CFO Cyber Security Checklist has the very first question as:

> Do you conduct a periodic review of regulations related to data protection (e.g., encryption) and retention policies (e.g., HIPAA/HITECH regulations related to health plan information and employee medical records and Family Educational Rights and Privacy Act [FERPA] regulations application to student educational records, etc.)? (p. 17)

This demonstrates that addressing FERPA in a BYOD program is important, even though it seems to have been overlooked in some of the other articles that addressed BYOD in the private industry. Mooney (2014) also describes how not only is it important to address legal compliance, the financial risk of not being compliant and having to pay fines can hurt a business, as well as doing harm to the corporate reputation.

HIPAA and the HITECH Act were created to protect personal health information (PHI) of individuals (Ealey, 2015). These acts primarily relate to hospitals and medical facilities, but could be cause of concern for many other organizations too. This is when knowing the type of data that an organization stores and allows access to is crucial. If any of this data contains PHI, such as a Human Resources files for injured employees, HIPAA and HITECH compliance would need to be addressed (McLaughlin, 2014).

The Federal Information Security Management Act (FISMA) seems like a very important law in regards to security and BYOD and was recently updated in December 2014 to become the Federal Information Security Modernization Act (2014) (Congress.gov). Unfortunately, at this time, FISMA only pertains to the government. FISMA details precise security features and how to report issues within a chain of command and policy. Khallaf & Majdalawieh (2012) summarize it perfectly:

> FISMA mandates that the federal and state agencies strengthen information security controls over resources that support federal operations and assets, including annual audits. In addition, FISMA requires that the agency head delegate to the agency CIO the authority to ensure compliance with the law (FISMA, 2004). It is important to note that FISMA standards apply only to federal and state agencies and do not apply to the

> private sector. The objective of the current federal government policy is to engage and collaborate with the private sector to disseminate best practices and to raise awareness of security issues (p. 56)

Although FISMA is specifically for government, it could be a good framework for a CIO to follow while organizing their own IT Security departments and features of security policies.

CONCLUSION

The literature leaves out some of these key model components. One major issue to assess is a revolving check of FERPA, FRCP, FIA, HIPAA, and other laws that may pertain to organizations' use of a BYOD Plan. Further case study should be conducted to determine how many Higher Education institutes have a BYOD plan and how many of those utilize a revolving cycle to ensure the plan is current and consistent with the current laws. This could also lead into a further study of how many Higher Education institutes have legal counsel available to assist with addressing these laws and how well the IT department and this legal counsel coordinate the BYOD plan and policies to stay within compliance. This paper consists of just a sampling of the few Acts, which hold important compliance requirements that any enterprise should address in a BYOD program. Not only is it the legal thing to do, it is also an ethical issue. Much is at risk for violating these Acts financially and reputation-wise. A well written BYOD program will protect a company and its employees when allowing them to bring or use their personal mobile devices in order to do their job. So, when considering securing devices in a BYOD Plan many components must be included; such as a risk assessment, the laws that must be addressed, employee education and training processes and procedures, the methods of reward for following the policy or punishment for breaking these security measures, and an incident response plan. Even after developing a secure BYOD program, these components must be revisited regularly to maintain a proactive stance in diminishing security risks. Technology and hackers are ever changing and therefore continuously developing and revising secure policies is wise practice.

REFERENCES

Baskerville, R., Straub, D. W., & Goodman, S. E. (2008). *Information Security : Policy, Processes, and Practices*. Armonk, NY: ME Sharpe, Inc.

Chen, Y., Ramamurthy, K., & Wen, K. (2012). Organizations' Information Security Policy Compliance: Stick or Carrot Approach?. Journal Of Management Information Systems, 29(3), 157-188.

Congress.gov. S.2521 - Federal Information Security Modernization Act of 2014. Retrieved from https://www.congress.gov/bill/113th-congress/senate-bill/2521

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. Journal Of Management Information Systems, 31(2), 285-318. doi:10.2753/MIS0742-1222310210

DeFRONZO, P. (2016). INFORMATION SECURITY GUARDRAILS. Mortgage Banking, 76(6), 86-91.
EALEY, T. (2015). HIPAA privacy meets BYOD...bring your own device. Long-Term Living: For The Continuing Care Professional, 64(4), 32-35 4p.

Khallaf, A., & Majdalawieh, M. (2012). Investigating the Impact of CIO Competencies on IT Security Performance of the U.S. Federal Government Agencies. Information Systems Management, 29(1), 55-78.

McLaughlin, P. F. (2014). BYOD: cool but dangerous -- 3 HIPAA Security Rule challenges, 7 key precautions. Venulex Legal Summaries, 1-6.

Meyer, C. (2016). Bring Your Own Risk in BYOD. *Security: Solutions For Enterprise Security Leaders*, *53*(4), 52-58.

Mooney, J. L., Parham, A. G., & Cairney, T. D. (2014). Mobile Risks Demand C-Suite Action!. *Journal Of Corporate Accounting & Finance (Wiley)*, *25*(5), 13-24. doi:10.1002/jcaf.21967.

Raggad, B. G. (2010). Information security management: Concepts and practice. Boca Raton, FL: CRC Press/Taylor & Francis. (p. 295-320)

Rose, A. D. (2013). Information Governance's Privacy and Security Component. Journal Of AHIMA, 84(11), 54-56 3p.

TUDOR, J. (2015). Legal Implications of Using Digital Technology in Public Schools: Effects on Privacy. *Journal Of Law & Education*, *44*287.

PBS. (2013). PBS Survey finds Teachers are Embracing Digital Resources to Propel Student Learning. Retrieved from http://www.pbs.org/about/blogs/news/pbs-survey-finds-teachers-are-embracing-digital-resources-to-propel-student-learning/

U.S. Department of Education. (2014). Protecting Student Privacy While Using Online Educational Services. Retrieved from https://tech.ed.gov/wp-content/uploads/2014/09/Student-Privacy-and-Online-Educational-Services-February-2014.pdf