Research Note

Risks Associated with “Bring Your Own Device” in a Government Agency

Beth Hutchens

November 2017

Keywords: BYOD; Bring Your Own Device; Workforce Security; Organizational Risks

Abstract: This research notes explores the practice of “bring your own device” (BYOD), specifically within the public sector. Permitting employees to use their personal technological devices (such as smartphones, laptop computers, and tablet PCs) has been an increasingly popular option within organizations as a means to cut costs, increase productivity, and provide better work-life flexibility. While BYOD is generally looked upon favorably, what is often overlooked or ignored, however, is the fact that there are significant risks associated with the practice, including legal liability, regulatory scrutiny, data exposure, increased costs and expenses, and potential brand and reputation damage.

Introduction

As the connectivity of society continues to trend upward, organizations and government agencies frequently look for new ways to increase productivity, give employees more flexibility, and cut costs. Permitting employees to use their personal devices for work purposes is one way to accomplish these goals. Commonly referred to “Bring Your Own Device” - or “BYOD” - it is a term that collectively refers to the related technologies, concepts, and policies in which employees are allowed to access internal corporate IT resources (such as databases and applications) while using their personal mobile devices like smartphones, laptop computers, and tablet PCs. Put simply, BYOD is a business practice in which employees of an organization are allowed to use their own electronic devices (as opposed to those supplied and controlled by the company) to access company information and applications.[1] It is not a practice that is well understood and many times BYOD is conducted under the radar without meaningful guidance or rules from managers, stakeholders, or even regulatory authorities.[2]

BYOD is generally looked upon favorably by CEOs and the overarching attitude is that the increased productivity and reduced operating costs that BYOD facilitates by far outweigh the added risks for many organizations. For example, Cisco’s 2016 annual report found that 66 percent of IT decision makers feel that BYOD is a good thing and

[1] “Bring Your Own Device: An overview of risk assessment”, R.I. Ogie Smart Infrastructure Facility, University of Wollongong, Northfields Ave, Wollongong NSW *citing* E. B. Koh, J. Oh, and C. Im, “A study on security threats and dynamic access control technology for BYOD, Smart-work environment,” in Proc. Int. MultiConf., vol. II, Hong Kong, Mar. 12–14, 2014.

[2] For a general definition of BYOD, *see* Whatis.com entry “BYOD (Bring Your Own Device*) available at:* http://whatis.techtarget.com/definition/BYOD-bring-your-own-device.

that workers save an average of 81 minutes per week when permitted to use their own devices.[3] What is often overlooked or ignored, however, is the fact that there are significant risks associated with BYOD, including legal liability, regulatory scrutiny, data exposure, increased costs and expenses, and potential brand and reputation damage.

Operational Risks accompanying BYOD

For the most part, the risks associated with BYOD in the public and private sectors are similar, if not identical. In addition, those risks are numerous, complex, continually changing, and occur in a regulatory environment that is still evolving. In fact, the practice is often jokingly referred to as "bring your own disaster" with good reason.[4] While the cadre of risk factors that accompany these practices fit into traditionally defined categories -people, processes, systems, and external events- there is a uniqueness to BYOD that causes the risks and control failures involved to become increasingly intertwined.

For example, a single event- such as ransomware[5]- involves an external force in the form of an individual or group of individuals hijacking a user's computer, a personnel failure at the hands of the person who unwittingly clicked a harmful link, a process failure in the form of a lack of education to help the employee identify suspicious emails, and a system failure in the form of an as yet unknown exploit. Broadly defined, the risk associated with BYOD leads back to leakage and / or exposure of sensitive data belonging to the public, the employee, or in some cases, both. Accordingly, while it is true that the "risk" associated with BYOD is nearly always the broad concept of data exposure, an analysis that only looks into technological ways to prevent or mitigate that (and only that) is incomplete and misses the big picture because it focuses too much on an IT solution as opposed to a companywide, systemic approach.

BYOD is also unique from a risk management standpoint because of the inherent insecurity of mobile devices. Not only are they easier to exploit, but also an important function of these devices is that they are always connected wirelessly. Thus, vulnerability to malicious attacks is increased because the communication channels are more numerous and varied as opposed to traditional desktop machines relying on a wired connection. Further, unlike other types of computing devices, BYOD means that personal and company data are permitted to exist on the same device, which creates at least two conflicting interests when it comes to risk management. Among other things, this puts personal autonomy and privacy of the employee at odds with the controls necessary to safeguard company data. In addition to this, the opportunity for inadvertent exposure of sensitive information by, for example, mistakenly sending sensitive information to personal contacts is extraordinary high. These problems are compounded by the fact that BYOD involves devices that require a very high level of IT support, regardless of the make, model, age, or type of the device.[6]

Moving beyond a purely technology-focused inquiry requires an assessment of a company or agency's internal

[3] *Available at* http://www.cisco.com/c/en/us/about/annual-reports.html.

[4] While this paper discusses risks in a negative context, the increased costs incident to creating and implementing a BYOD program and employing still-developing technologies such as mobile device management can also be thought of as positive risks in that they present tremendous opportunities for growth and efficiency.

[5] Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. More modern ransomware families, collectively categorized as crypto-ransomware, encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key.

[6] It is worth mentioning that the risks associated with BYOD are heightened with the instance of a disgruntled former employee or rogue current employee. In some cases, the control failures and risk mitigation associated with these types of events share some similarities with the actions of "innocent" personnel, but a thorough discussion of how to prevent these types of events is beyond the scope of this paper.

protocols, culture, and approach to conducting business. Many of the risks associated with BYOD can be directly tied to personnel, or more specifically, to the ignorance and/or indifference of personnel. For example, it is quite common to have stakeholders and members of the management team who cannot or will not make the commitment of company resources to create, implement, and/ or enforce BYOD protocols. Even if they could, personnel tend to push back on what they view as yet another set of hurdles that prevent them from being able to do their jobs efficiently and effectively. The result of this collective reluctance can be thought of as the cause of a level of ignorance that translates into an opportunity for an organization to virtually hemorrhage sensitive information, which can cause legal liability, federal scrutiny, reputational damage, and internal strife, or a combination of the four.

Current Controls Pertaining to BYOD in Government Agencies

Public records laws, data security and privacy regulations, accountability, and legal liability are more keenly felt in the public sector, and change is not easily accomplished for a variety of reasons. Thus, the state of BYOD remains inconsistent across state lines, differs between agencies depending on their function, and the practice is still in its infancy stages. This is not to suggest that BYOD does not exist at the state, federal, or even local level, but what has emerged is a practice that is largely unregulated, undeveloped, and more often than not, proper procedure and risk management are an afterthought (if ever). The result is an ad hoc business practice where the lines between professional and personal lives are blurred, employees have concerns that their privacy is at risk (either from a member of the public or a snooping employer), and serious issues associated with the public's personal information are created- all of which go unaddressed.

From a planning standpoint then, risk management with BYOD might not be feasible for agencies that are subject to higher information security standards such as state and federal law enforcement agencies. Those agencies might do well forbid BYOD and supply any and all mobile devices themselves, as the risks- no matter how remote in possibility- are simply too great to ignore.[7] Thus far, the overwhelming attitude from the public sector is to ignore the existence of, rather than embrace, the complex issues that come with BYOD. The reality is that BYOD occurs in government agencies whether management knows it or not, which results in a general attitude of denial or willful ignorance when it comes to personal devices in the public workplace.

In 2015, mobile security company Lookout analyzed 20 federal agencies and discovered 14,622 Lookout-enabled devices associated with government networks, despite the lack of permission or a BYOD policy in place for that agency. In another survey of a thousand federal employees, Lookout found that 37 percent said they are willing to sacrifice government security to use a personal device at work despite understanding security concerns, and 40 percent of those working at agencies with policies preventing the use of personal smartphones admitted the rules have little to no impact on their behavior. Lookout's State of Federal BYOD report also found that 24 percent of employees install apps from places other than official app stores, and that 18 percent reported encountering malware on their devices.[8]

Alarming as these numbers are, this is not to say that government agencies have no BYOD controls whatsoever. Though sporadic and imperfect, some state and local governments are beginning to address the growing BYOD issue and the federal government has identified some best practices.[9] Some agencies permit BYOD so long as the

[7] Some states and companies do not permit employees to use their personal devices at all and opt for agency supplied and controlled devices. This is certainly the easiest way to reduce risks associated with personnel, but is reportedly the least popular option among employees.

[8] "Feds: You Have a BYOD Program Whether You Like it or Not." 2015 Lookout State of Federal BYOD Report, *available at* https://media.scmagazine.com/documents/144/fed_byod_report_35977.pdf.

[9] *See for example* "Bring your own Device: A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs", Digital Services Advisory Group and Federal Chief Information Officers Council,

employee agrees to give the agency at least some control over the device. Known as mobile data management, or "MDM", this includes installing software that gives the agency the power to remote wipe the device in the event it is lost or stolen, limit access to certain kinds of apps and downloads, and sequester the device owner's personal data. Others have not embraced the practice yet, and are working on developing a program before allowing the use of personal devices. Still others have acknowledged that BYOD is happening regardless of a meaningful protocol and are using the "under the radar" approach as a way to shape and drive their program in a way that best meets their internal goals and needs.

It is an accepted truism that, when it comes to cyber incidents, it is not a question of *if* one will occur; it is a matter of *when*. With that in mind, external actors are a driving force that should be accepted as fact and while cyber security is always at the forefront, because a BYOD device necessarily and by definition involves people, the control factors that should have the greatest amount of attention are personnel and processes. [10]

The Private Sector's Approach to BYOD

Permitting employees to use their personal devices for work is well established in the private sector. Companies engaging in the practice typically have a robust policy in place that establishes rules, procedures, and polices relating to use of personal devices. Many times, employees must undergo extensive training and agree to company procedures before they are extended the privilege of using their personal device. A common theme in the private sector is to start with answering the general questions of who owns the device, who manages the device, and who secures the device. The answers to these questions help drive the company policy and establish the rights and responsibilities of both the employer and the employee.

In addition to employing innovative technology, the private sector has been implementing and adopting BYOD procedures for quite some time. This may be for any number of reasons, such as the fact that private industry has differing goals and concerns than public entities, is not hindered by public records laws, has more internal controls, and is in a better position to shoulder risks. For whatever reason, private companies have been honing and developing controls for BYOD that, at least in some cases, the public sector could learn from. For example, there is a litany of guidance from trade organizations and interest groups that routinely publish studies, guidance, templates, checklists, and all other manner of help a company wanting to develop a BYOD program might look to.[11]

A common approach is for a private sector company is to limit certain types of applications that may be installed on the device. For example, in 2012, IBM banned the Dropbox and Siri apps over concerns about data security.[12] In fact, some companies and agencies scrap BYOD altogether and do not permit commingled data on devices as a matter of course. Others use MDM or other types of software solutions that are still under development and still others create

August, 2012; Joanne E. Hale, "BYOD Policy Release", Acting Secretary of Information Technology, State of Alabama, June 2016.

[10] It is interesting to note that BYOD is not as prevalent in Europe and Canada. As cross border data transfers become more prevalent, and as the United States struggles to remain compliant with increasing security and privacy regulations, the question remains whether BYOD will decline in popularity for practical reasons. This is especially true when considering the European General Data Protection Regulation that goes into effect in 2018 and requires, among other things, Privacy by Design.

[11] *See*, *e.g.,* "3 Keys to Mastering BYOD", IAPP Privacy Academy 2013; Staff Mobile Phone Policy Pilot Program, Financial Policy Office, Harvard University, 2014; James Sherer and Melinda McLellan, "Privacy, Security, and Practical Considerations for Developing or Enhancing a BYOD Program", International Association of Privacy Professionals Resource Center, 2015; IT Peers Share Advice on Effective "Bring Your Own device"(BYOD) Strategies", Wisegate Community Viewpoints.

[12] "IBM: Sorry, Siri. You're Not Welcome Here," InformationWeek, *available at* www.informationweek.com/news/security/mobile/240000882.

protocols and practices that are company-specific and tailored to their business needs. When it comes to device security, a collaborative and effective relationship with the IT department is common in the private sector and many times, the IT department is involved early and often - as it should be.

Recommendations for Implementing a BYOD Program

As a threshold matter, a meaningful program must start with stakeholders and management and will require cooperation among departments, so the first step should be to obtain a commitment to dedicating the time, energy, and resources to such a large-scale endeavor. The next step in deciding whether to permit BYOD in an organization is to conduct a thorough privacy assessment and threat risk. This will determine if BYOD is feasible, possible, or desirable for the particular organization[13]. In some cases, it may not be.

Then, operating under the premise that developing a workable BYOD program is wanted, needed, and possible, there are a few considerations that an agency can address to mitigate the risks. Of the utmost importance is to develop, communicate, implement, and enforce a BYOD policy. The parameters of this policy will be specific to each organization, but at a minimum, the policy should: 1) identify the information collected, used, and disclosed; 2) clarify the user's rights and responsibilities; 3) discuss how the devices will be monitored and / or controlled by the company (including software application management); 4) identify what privacy rules, regulations, and practices come into play; 5) develop an incident response team and a clear chain of command in the event employee or public data becomes compromised; and 6) provide a clear set of protocols, tasks, and guidelines to help them manage the risk.

Naturally, before the program is implemented, there must be thorough employee training that includes a discussion of safety and security protocols, but also their rights and obligations when it comes to using their personal device for work purposes. There should be an employee handbook that details their rights, responsibilities, and obligations and a detailed incident response protocol that is routinely tested, analyzed, and perfected. Finally, regular audits of the incident response protocol, reviews of the program's regulatory compliance, and tests for the efficacy of the program should be conducted frequently to make sure the program remains viable in a rapidly evolving environment.

Conclusion

Permitting employees to use their personal devices for work purposes is not the right solution for every company or every government agency. The risks related to commingled data on such devices are high, nuanced, and will vary depending on the type of data the organization collects, hosts, and shares. They include legal liability, enhanced regulatory scrutiny, and reputational damage. The benefits include time and cost savings, happier employees, and increased efficiency in the work place.

There is some guidance from the federal government and a smattering of state and local governments are beginning to create policies when it comes to BYOD best practices. Government agencies can learn much from the private sector's approach to BYOD. From the outset, developing, implementing, enforcing, and monitoring an effective BYOD policy requires a commitment to early involvement from senior management and stakeholders. Moreover, agencies and private companies will do well to be cognizant of, and adhere to, applicable state and federal data security and privacy regulations in developing their programs. Then, using known risk assessment and privacy impact tools, the decision can be made whether or not to permit employees to use their personal devices according

[13] In some cases, depending on the type of data collected, used, disclosed, and retained BYOD is not an option. This is especially true where federal or state regulations that may be implicated such as for example, health information or information pertaining to persons under the age of 13. *See e.g.,* HIPAA, COPPA, and GLBA, state data breach notification laws, and the like.

to the agency's goals and the regulatory environment. By starting with asking the right questions and involving stakeholders and the IT department in the process, a collaborative approach can be fostered and a meaningful program can be developed that accommodates and mitigates those risks to the extent possible. Though the private sector perhaps has more flexibility to embrace BYOD as much or as little as they choose, the public sector need not eschew the practice entirely. By adopting established practices and protocols, and by engaging in Privacy by Design practices, state and local governments can establish themselves as thought leaders with respect to BYOD.