Bring Your Own Devices in Business and Education

Theresa Meza

East Carolina University

ICTN 6823

July 23, 2015

Abstract

Companies have developed policies, procedures, and guidelines to manage the information security of the computers that are provided to employees but now they must go beyond that realm. Today's world has seen the abundant increase of mobile devices that are used on a regular basis by all people. Employees are now bringing these mobile devices to the workplace and are using them to perform work as well as access company networks and information. The management of these employees' own devices must not only include the risk of access to company networks and information but the management of risk related to the information that is stored on the devices. This is also seen within educational institutions and must be managed from a variety of aspects within these organizations. Information security has evolved to include bring your own devices and organizations must be diligent in remaining up to date and managing the potential risks associated with these devices so that they may perform an adequate cost benefit analysis when it comes to bring your own devices.

Introduction

Bring your own devices (BYOD) is a phenomenon that has seen a rapid increase in popularity but some research indicates that it has also reached its peak and has begun its decline. No matter where it stands in its lifecycle, it is something that information security professionals must take seriously. This phenomenon has the ability to cripple a company or educational institution if it is ignored. A stance must be taken, whether it is one of acceptance or prevention. Once a stance is taken, the organization must then follow that stance with proper policies and procedures to ensure that the stance that has been adopted is followed by the employees and students in the word of education.

When deciding upon the stance that they are going to take, the organization can chose to acceptance and allow employees, and students, to bring their own devices and access the organization's networks and data using these personal devices. If this stance is taken, the organization must institute a plan to protect the information assets of the organization as well as determine how they are going to manage the devices that are accessing the information. They must also determine how they are going to deal with the data being housed on these devices. Another consideration will be how they will handle the increase in activity over the networks.

Another option that an organization can choose is to ban employee personal devices in the workplace. Should a company take this stance, they will need to determine how they will enforce this position. Many employees have these devices and how will the employer police the use of the devices. Will they be banned from the premises, will they solely be banned from accessing the network and company data?

As with any decision made by an organization, a company must consider the benefits of allowing employees to bring their own devices and weigh them against the costs of such practices. This paper will introduce the trends for both industry and education as a starting point. It will then discuss the advantages or benefits of allowing employees and in the case of educational institutions, students, to bring their own devices. It will next

address the cost or issues that bring your own devices raise for these organizations, focusing on information security. In the end, it will be up to an individual organization to determine if the benefits that they will receive outweigh the risks/issues that they will face in allowing their employees/students to bring their own devices.

Business Trends in Bring Your Own Devices

A survey in 2013 revealed that thousands of employees were using their own mobile devices for work. The expectation was that this number would continue to increase. It was expected that up to 250 million employees world-wide would be using their personal mobile devices for work (**Bello Garba, Amarego, Murray, & and Kenworthy, 2015). They have attributed this growth to the current generation of employees who are technology savvy. These employees are demanding the ability to use the devices that they are comfortable with instead of having to use the devices that are provided by their employer. Another reason noted in the article for this trend is the fact that employees are determined that they are going to use their personal devices even though it may violate the policies that their employees have in place regarding the use of personal devices (**Bello Garba, Amarego, Murray, & and Kenworthy, 2015).

While the employee desire and actions may support a move toward the growth of bring your own device practices in the workplace, a recent article in Computerworld contradicts this practice. It conducted a survey which found that U.S. companies are moving away from the bring your own device trend (Hamblen, 2015). The survey included 375 U.S. IT professionals and was conducted in April and May. The results found that 53% allowed no bring your own devices which was a significant increase over the previous reporting of 34% from 2013 (Hamblen, 2015). The smallest portion of respondents (7%) allowed a full bring your own device policy but the company did not take any responsibility for the devices being used by the employees and remaining respondents had a hybrid of employer provided devices and employee provided devices (Hamblen, 2015).

Contradictory to this, another study reported that half of the companies that they surveyed intended to move exclusively to employee provided smartphones by 2017 (Weise, 2014). There is however agreement that there are differences between what employees and employers want that is creating tension (Weise, 2014). There is no doubt that the devices are out there and employees have them and are using them. The questions that comes in to play is whether they should be using them for company business and if they are what responsibilities does this create for the employer as well as what risks must be managed by the employer.

Business Benefits and Concerns

If all an organization had to consider when it came to employees bring their personal devices to use on company networks and access company data was the security concerns, it would be straightforward for companies to ban the use of employees' personal devices. A company can experience benefits when employees bring their own devices to the workplace or use them with work. One of the benefits seen by an

organization is the fact that the employee can be accessible anytime, anywhere because they will be carrying their personal mobile device with them when they are on the job as well as off the job. They will also be the ones purchasing the device so the company will not have the outlay in purchasing the device. A third benefit presented is that the employee can be more productive when they have the flexibility to purchase the device of their choice (Olalere, Taufik Abdullah, Mahmod, & and Abdullah, 2015).

Benefits of bring your own device can extend beyond the ones presented above. BYOD allows an employee to access organizational resources online and work with this material at their preferred time and pace (**Bello Garba, Amarego, Murray, & and Kenworthy, 2015). The convenience and flexibility offered to employees by being able to work in remote locations and at their convenience. Being able to choose the device that they are working with allows for an increase in employee satisfaction and prevents the employee from having to carry multiple devices to handle both their personal and business affairs. Since the employee has chosen the device that they are using, they are likely to quickly become experts on the devices which will increase their productivity. Organizations will also benefit from an employee's desire to always have the most up to date technology (**Bello Garba, Amarego, Murray, & and Kenworthy, 2015). The employee will bear the expense of updating their technology and the organization will benefit from the employee using that updated technology in the completion of their work.

Now that we have seen the advantages and understand why a company would be inclined to all employees to BYOD, we must consider the risks and concerns that arise when such practices occur. According to Bring-Your-Own-Device, "IT's best strategy to deal with the rise of BYOD is to address it with a combination of policy, software, infrastructure, controls, and education, in the near term, and with application management and appropriate cloud services in the longer term (Bring-Your-Own-Device, 2013)." This gives us an overview of what an organization must consider but it is important to take a closer look at exactly what needs to be considered.

As soon as an employee connects their personal device to an organization's network, malware could migrate onto the organizations machines and networks (Miller, Voas, & and Hurlburt, 2012). There is also concern about the information that goes from the network or employer devices onto the employee devices. This information should be kept private or confidential and this may not happen on an employee's personal device. A mobile device is smaller than a laptop and there is increased concern that it may be lost and private information may become available (Miller, Voas, & and Hurlburt, 2012).

Since employees are bringing their own devices, you will likely find a variety of devices with different operating systems and applications. For an organization to develop a secure infrastructure that can accommodate the number and variety of devices that will be found in this environment will be expensive and challenging (**Bello Garba, Amarego, Murray, & and Kenworthy, 2015). One of the biggest risks reported is that there is no guarantee that the security and privacy risks associated with BYOD programs can be eliminated (**Bello Garba, Amarego, Murray, & and Kenworthy, 2015). Organizations will need to maintain control over which devices are accessing their

networks, which networks, or which parts of their networks. Network access control technology controls how devices are able to connect to your network and which devices will be allowed to connect to your network (**Bello Garba, Amarego, Murray, & and Kenworthy, 2015). Two available products for network access control solutions are CISCO Networks BYOD Solution and Meru Networks BYOD Solution. An approach that monitors and securely manages the actual devices is the mobile device management approach. This approach includes a centralized distribution of applications, data, and configurations settings to all devices that are connected to the network. In this approach there will be a centralized distribution of the applications to devices, data that can be accessed by the devise, and configuration settings will be sent to all devices that are on the network at that time (**Bello Garba, Amarego, Murray, & and Kenworthy, 2015). A third approach uses password to secure to organization. Passwords provide access to desktops and apps through the employee's personal mobile device. If a mobile device is no longer in the employee's possession due to loss or theft then the remote access connection is broken and the organization's data is protected (**Bello Garba, Amarego, Murray, & and Kenworthy, 2015).

With virtualization, applications run on back-end servers and not on the mobile devise. This allows access on the mobile devices but keeps the data and corporate apps off the employee's device (**Bello Garba, Amarego, Murray, & and Kenworthy, 2015). This practice not only prevents data from being misplaced with a lost phone but also provides for full separation of organization and personal data. These virtualized apps offer increased functionality and are easy to update on the mobile devices. An additional benefit is that malware and viruses cannot be sent through these apps. Virtualized apps do have some shortfalls. Not all devices will meet the system requirements for all virtual apps and some virtual apps will not be easily used without additional hardware like a keyboard and mouse. Another downside is that virtualized apps may take longer to load and may not be optimized on smaller screens (**Bello Garba, Amarego, Murray, & and Kenworthy, 2015).

The phone-centric approach uses permanently installed systems on the device itself to secure the device. Controls are put in place on the device that will work based upon how the device will access the network and information. Technologies are used to separate personal and organizational space on the device. This highly effective approach is typically seen on company owned devices verses employee owned devices or in organizations where security is very high (**Bello Garba, Amarego, Murray, & and Kenworthy, 2015).

Educating the Next Generation for BYOD

As indicated above, if employees are allowed to bring their personal devices to work, organizations need to have well thought out policies, procedures, and education in place to deal with the possible security risks associated with the personal devices accessing company networks and information. According to a McAfee survey, 71% of organizations that are allowing employees to use their personal devices for work purposes do not have policies in place to ensure the protection or the company's data. A SAN's Institute survey also found that only 41% of the respondents felt strongly that it

was needed to have these types of policies (**Pattern & and Harris, 2013). Surveys also show that while IT professionals understand the threat these technologies impose, they do not know how to deal with this threat. It was also noted that the employees themselves do not truly understand the threats posed by the personal mobile devices that they are wanting to bring into the workplace. One key solution to both of these is education (**Pattern & and Harris, 2013). Providing the this education to student in information technology programs is a start to ensuring that the IT professionals of the future are prepared to handle these situations. This education needs to include basic personal mobile device security and how to protect an organization from the threats that these mobile devices pose (**Pattern & and Harris, 2013). While all college students should have the opportunities to learn about these topics it should be an absolute must for information security students. Information security students should be education on the different mobile operating systems, app markets, malware, jailbreaking, rooting, anti-virus, firewalls, passcodes, data privacy and security, and app permissions. IT students also need to know how to create mobile device security policies for devices that are provided by the company and for devices that are provided by the employee. It is also going to be essential for the IT student to be able to assess the mobile deice risk within an organization so they can develop a plan of action to manage that risk. Within this area, they will need to be able to identify the threats, assets, likelihood, consequences, and document the process (**Pattern & and Harris, 2013).

Education Trends in Bring Your Own Devices

The number of colleges that are asking students and faculty to bring their own devices into the classroom is increasing (**Violino, 2012). This movement is meant to give easier access to textbooks, educational services, as well as increase productivity, and enhance collaboration among faculty and staff (**Violino, 2012). It seems that the adoption of bringing your own device in the classroom is occurring at a slower pace in community colleges than in other education sectors. It is believed that this is due in part to a lower pressure than four-year institutions. Prince George's Community College and Lansing Community College have launched bring your own device programs at their colleges and since community colleges are less likely to issue standard technology to their students they would seem like a perfect place for this type of initiative (**Violino, 2012). Some colleges are taking an informal approach, in which students are encouraged to bring their mobile devices into the classroom instead of the college having a dedicated program (**Violino, 2012).

Bring your own devices raises unique challenges in the educational setting. To what extent will the school support the devices that are brought to the classroom? What will the school do to help provide devices to those students that cannot afford to purchase a device? Will they provide access to required software and digital resources across multiple platforms (**Newhouse, Cooper, & and Pagram, 2015)? Will there be access to the Internet in all classrooms? In all instructor offices to prepare for class on the device needed in class?

A study with American higher education students found that tablet devices were the most useable device for mobile learning (**Newhouse, Cooper, & and Pagram, 2015).

These devices surpassed smartphones and e-book readers. When looking for a mobile device for use in the classroom, the most critical characteristics that students considered were weight, battery life, robustness, and networking (**Newhouse, Cooper, & and Pagram, 2015). From the tablets researched, it was determined that the iPad 2 was the only tablet device that the student could use alone on campus but they would still need access to a laptop at home for printing purposes (**Newhouse, Cooper, & and Pagram, 2015). Since the research was done there have been some advancements in the technology but the needs of the students remains the same. They are looking for a device with a battery to get them through the day but is light enough to carry around without adding much weight to their already heavy backpack. They need wireless capabilities, office suite, and printing capabilities. As more apps have been developed for use in the classroom, access to a good app store to be able to access the apps being used in the classroom would also be necessary.

Education Benefits and Concerns

Students in today's world are not only familiar with technology but comfortable with technology. A benefit to allowing students to bring their devices to the classroom is that having the use the technology they are familiar with will encourage participation in the classroom (Bruder, 2014). A benefit to the schools would be that with the students bring their own devices, they could use those funds for other expenditures. When students have devices in the classroom, they can use them to conduct research, participate in polls, participate in interactive assignments, store assignments in the cloud, play background music (with earbuds) to block out distractions, and they can Skype with students in other schools/countries (Bruder, 2014).

As with most any case, in addition to the benefits there are some disadvantages or problems that can be created by students bringing their own devices. There are concerns that students will become easily distracted by the devices as well as find way around the restrictions that are in place regarding the devices. Another concern is the widening of the significant tech gap for lower income students (Bruder, 2014).

As with business organizations, there are also the security concerns and policies and procedures that must be considered within the school setting when bringing your own device. Once possibility is for the network administrator to setup separate zone for the network users to avoid drain by multiple devices on the network. Bandwidth limits could also be imposed at certain times of the day and students should be shown how to create cloud storage accounts and then use them to save their files. Student's devices must also be secured and rooms need to be locked when students will be away from their devices. The school must make sure that they create a policy for the bringing of personal devices and then must also make sure to enforce the policy (Bruder, 2014).

Faronics has provided four tips for deploying a successful classroom bring your own device program. The tips include making sure that you have reliable bandwidth available (Faronics Blog, 2015). IT administrators will need to be prepared for a spike in demand when students bring their own devices. The second tip is to create guidelines for appropriate use of devices (Faronics Blog, 2015). Making sure to explain what is

proper behavior before the program begins can help prevent problems. The third tip is to create lesson plans with BYOD in mind (Faronics Blog, 2015). Think about the device when creating your lesson to get the most out of the device and the lesson. You will probably end up reworking many of your prior lessons if you want to make the best use of the program. The last tip is that well balanced learning is essential (Faronics Blog, 2015). While you want to make use of the devices in the classroom, you still want to have activities and time that you are not using the device. Try to aim for a fifty-fifty split between the two.

Conclusions

While there was some discrepancy between some of the studies, bring your own device to work/school is not going away. Each organization will need to weigh the benefits and costs of having the employees/students bringing their devices and make the decision that is correct for their organization. In this process, an organization must understand the threats that they face when allowing employee devices to access their networks and data. They must also assess their position to defend against those threats and weigh that against the benefits that would be provided if the employee was able to bring their own device. No matter what the decision is, it is going to be vital to have a formal policy in place regarding bring your own device or the ban on brining your own device. Once the policy is creating, it is going to be just as essential to enforce the policy and have security measures in place to safeguard the organization networks and data.

References

**Bello Garba, A., Amarego, J., Murray, D., & and Kenworthy, W. (2015). Review of the Information sEcurity and Privacy Challenges in Bring Your Own Device (BYOD) Environments. *Journal of Information Privacy and Security*, 38-54.

**Newhouse, C. P., Cooper, M., & and Pagram, J. (2015). Bring Your Own Digital Device in Teacher Education. *Journal of Digital Learning in Teacher Education, 31*(2), 64-72.

**Pattern, K. A., & and Harris, M. A. (2013). The Need to Address Mobile DEvice SEcurity in the Higher Education IT Curriculum. *Journal of Information Systems Education*(Spring), 41-52.

**Violino, B. (2012). Education in Your Hand. *Community College Journal, Aug/Sep*, 38-41.

Bring-Your-Own-Device. (2013). *Communications Today*.

Bruder, P. (2014, Nov). Gadgets Go To School: The Beneftis and Risks of BYOD (Bring Your Own Device). *The Education Digest*, pp. 15-18.

Faronics Blog. (2015, June 26). *4 Ways To Wmploy BYOD Successfully in Schools.* Retrieved from http://www.faronics.com/news/blog/4-ways-to-employ-byod-successfully-in-schools/

Hamblen, M. (2015, July 15). The bring-your-own-device fad is fading. *COMPUTERWORLD*.

Miller, K. W., Voas, J., & and Hurlburt, G. F. (2012, Sep-Oct). BYOD: Security and Privacy Considerations. *IT Professional*, pp. 53-55.

Olalere, M., Taufik Abdullah, M., Mahmod, R., & and Abdullah, A. (2015). A Review of Bring Your Own Device on Security Issues. *SAGE Open*, 1-11.

Weise, E. (2014, August 26). USA Today. *Brind Your Own Dilemmas: Dealing with BYOD and Security*.