BYOD Security Considerations in a College Environment

Gregory Boykin

East Carolina University

Target Publication: https://www.infosecwriters.com

Abstract

Increasing numbers of organizations are rapidly implementing bring your own device (BYOD) policies to allow users the freedom of utilizing their personal smart phones, tablets, and laptops on the organization's network. With this shift comes many challenges relating to the security of such BOYD practices. Notably in a college environment where students, faculty, and staff often use personal devices across campus, Information Technology and Security administrators are faced with numerous factors which must be considered in balancing the need for convenience against the security of information and technology assets. This paper reviews the literature in order to highlight some of the aspects college administrators are faced with when implementing a secure BYOD policy. College campus environments differ from corporate settings in ways which affect policy and technical requirements; consequently, both technical and policy considerations should be addressed in a manner which reflects these unique characteristics. Several of these challenges unique to the college environment will be evaluated and weighed on the importance and potential impact. After a review of significant hurdles, possible best practices and recommendations for implementing BYOD in the college environment will be outlined.

Keywords: information security, infosec, BYOD, college

Introduction

On today's college campuses, the technological landscape has shifted dramatically from what was seen in previous years. In the past, information technology and security professionals primarily dealt with college-owned assets which were connected directly to campus network resources and were managed with far less complexity than seen today. However, in recent years, the growth of laptops and mobile devices on the average college campus has exploded. Just this year, the latest Ericsson Mobility Report states there are 5.5 billion mobile broadband subscriptions, and this is growing at 20 percent year-on-year (Ericsson, 2018). In 2012, the SANS Institute reported that 61 percent of surveyed organizations were already allowing "bring your own device" (BYOD) access to resources, indicating that the BYOD movement has been developing for more than half a decade (Johnson). Educational institutions are no exception and should expect increased demand for support for BYOD on campus. Furthermore, most educational institutions have been experiencing the challenges of BYOD much longer than traditional business environments (Donston-Miller, 2013). Students, faculty and staff bring many personal devices to campus, using those devices as an alternative method to access resources and enhance the learning environment. Academic institutions who have adopted policies to allow for BYOD on campus have seen numerous positive benefits. With this shift towards the BYOD mentality, information technology professionals face a rapidly changing and expanding landscape which poses many security management challenges. Despite these challenges, most institutions agree that the benefits BYOD brings to the college space are worth the investment.

Why BYOD

Despite the challenges brought about through bring your own device policies, numerous advantages for the modern educational institution clearly present themselves. At the forefront of those benefits is improved educational results; such improvements have been observed when students have access to BYOD service (Kao, Chang, & Chang, 2015). Today's students are highly connected, and with the proliferation of affordable personal computing devices, most now come to campus with several devices dependent upon the campus network infrastructure. Colleges can utilize the availability of these devices to enrich the learning environment inside and outside of the classroom through e-learning resources. Such mobile device usage encourages students to collaborate and interact with faculty to a greater degree, even when not in a formal classroom setting. Through the growth of online education and distance learning opportunities, students and faculty can interact anywhere on campus by the use of mobile devices.

In the classroom, BYOD policies have allowed student-owned devices to be used to facilitate learning. Many faculty today look to utilize BYOD as they want to leverage the portability and ease of use to simplify the classroom and enhance the learning experience (DiFilipo, 2013). Many vendors have recognized this growing trend in the classroom and are developing platforms with a BYOD classroom in mind (Sangani, 2013). These various hardware and software technologies offer increasing levels of functionality for the classroom. Due to these developments, many faculty are now able to further engage students and encourage collaboration by including the use of mobile devices in their lessons. Interactive classrooms now extend faculty-driven content directly to students as well as allowing students to capture lecture notes, participate in polls, and even present using their own personal devices.

In addition to collaborative benefits, mobile devices within the classroom also bring the possibility of introducing many resources not previously available. Instant access for internet or cloud-based content expands what can be presented within the classroom. With the large movement of educational institutions adopting BYOD, cloud computing is being used more as it possesses a great ability to improve efficiency, cost and convivence in the classroom (Jayapandian, Pavithra, & Revathi, 2017). Many companies offer content and services specifically tailored for the technology-oriented classroom, particularly those utilizing mobile devices as the platform. BYOD allows students to be able to engage and interact with lectures and other streaming content, opening many options to enrich the lessons presented by faculty.

Educational institutions also see distinct benefits through BYOD outside of the classroom. Most educational institutions implement wired and wireless networks across the campus so that students, faculty and staff members can connect anywhere within the boundaries of their institute in a seamless manner (Patel, Ghaghda, & Nagecha, 2014). Modern students in the ever-connected landscape expect a high level of access from the library to the residence hall. With the increased internet-based delivery of entertainment--whether music, videos, gaming, or other content--educational institutions now must implement robust network infrastructure, paying close attention to the availability of wireless networks to support these growing trends that depend upon BYOD policy. Technology services directly affect retention on college campuses as students look for institutions which maintain a high level of access for their mobile devices. Campus leadership must look to offer increased services to the campus community and continually strive to improve access to those resources needed by the campus BYOD users.

Beyond the many positive classroom and campus benefits, academic institutions have also seen several direct benefits when implementing BYOD policies. One such benefit is a

reduction in cost of technology required in the classroom. By allowing students and faculty to use their own smartphones, laptops, tablets and other devices, colleges reduce the amount spent on mobile devices needed to support modern classroom instruction. In addition to the cost savings seen through not having to purchases hardware, colleges also save on software licensing (Johnson, 2012). Since most classroom participants seem to be more comfortable with, and prefer to use, their own devices to collaborate in the classroom, campuses can take advantage of this to redirect fiscal resources. Educational institutions now worry less about mobile devices for the classroom and focus on infrastructure and collaborative technology improvements. These cost savings can be redirected to improve the campus network infrastructure, upgrade classroom teaching technology or provide additional cloud-based content in order to deliver a better experience for BYOD users.

Challenges of BYOD

Despite the many benefits adopting BYOD brings to educational institutions, several challenges also need to be considered by campus information technology and security professionals. Initially, academic institutions must realize that, despite the similar BYOD concerns shared between corporate and educational networks, there are unique challenges. BYOD policies in educational institutions are more liberal as compared to businesses (Kao, Chang, & Chang, 2015). In higher education today, a large amount of connectivity is required by students, often at locations outside the classroom. BYOD may be utilized in areas across campus such as cafeterias, fitness centers, social events and sports venues, and the use of the technology is allowing students the capability to “live where they learn” in the truest sense (Cisco, 2015). With BYOD, supporting network infrastructure, whether wired or wireless, will need to be robust and widespread throughout the campus to support a large number of connected devices.

Consideration must also be given to ensure appropriate security measures have been implemented across the campus network to protect both end user devices and the college's data and systems. These challenges should encourage best efforts to be made in provisioning adequate infrastructure and security to deliver a high level of service to the many devices that arrive throughout the educational institution.

College campuses must also deal with the volume of new devices which arrive on campus each semester. Unlike corporate environments, where devices are added at a slower pace, educational institutions will see large quantities of new devices introduced to campus as incoming freshman arrive. Faculty, staff and public visitors also bring in new devices to campus throughout the year. Devices ranging from smart phones, tablets, printers, gaming consoles and TVs produced by various vendors, all at varying software levels should be expected and appropriately onboarded to the campus infrastructure. With this device diversity, many may not be running the most secure versions of software or operating systems. Due to the expansion of the mobile device market, there has been a related growth in malicious software specifically targeting these devices (Drew, 2012). With the suboptimal security state, these unmanaged and unsecure devices could potentially introduce malware and viruses which could expose the campus to potential security issues.

In the campus BYOD environment, consideration must be given to how mobile devices are utilized on the network. Mobile devices, particularly those owned by students, cannot be managed though the typical methods used by Information Technology. Corporate organizations typically have strict policies enforcing BYOD and set restrictions on how the devices can be used. However, notably in campus residence halls where students browse the internet, download applications and access content, college information technology and security departments have

little control over the devices. Students usually install random mobile applications from play stores without truly understanding the permissions these applications request (Ali, Qureshi, & Abbasi, 2015). These practices can sometimes create security issues with the device. In addition, student devices also are at times connected to other networks beyond the campus, thus potentially exposing the devices to other threats. While most staff and faculty members align closer to the BYOD policies seen in corporate organizations, students often expect and are allowed more freedom and privacy when considering restrictions put into place on devices. With these allowances, the potential impacts on college systems and data should be considered.

Colleges also face a more complex network and security infrastructure that what is seen in most corporate environments. Due to the varying locations in which personal devices will be used such as residence halls, classrooms and public meeting spaces, careful consideration must be given to the design of the network as well as its security. The campus environment often necessitates a more complex design, adding costs for the hardware and software required to ensure security for college systems and data. Consequently, additional support many be necessary to maintain the complex network designs and mobile devices BYOD brings to campus. Additional training and staff may be needed to the support the introduction of BYOD policies.

Recommendations for BYOD

As BYOD continues to grow in the college environment, some of the benefits and challenges associated with this process have been reviewed. In considering the challenges, there are several best practices seen in the literature which can help to promote a secure and robust environment, allowing for continued growth in BYOD at educational institutions. The first of these recommendations is the implementation of policy. There are still organizations that either do not have BYOD policies in place or have policies but often allow exceptions, which results in

increased vulnerability (Bello, Murray, & Armarego, 2017). The numerous groups, such as students, faculty, and staff, have very unique demands, and policy must address these needs accordingly. For example, students typically access very different systems and content than faculty and staff members. Also, students, particularly at on-campus social locations, such residence halls and student unions, tend to spend significant time accessing resources outside of college systems or educational content. With this in mind, policies will tend to allow for more freedom and privacy when considering a college student versus faculty and staff members. Policy should enforce a finely-balanced mix of security and convenience, allowing the different campus groups to access what is required while simultaneously keeping the campus systems and data secure.

Along with policy implementation, user education must be a focus. Even with policy in place, if in the end users are not aware of BYOD policy and educated on best practices, security can be compromised. All students, faculty, and staff need to understand the importance of security in the BYOD environment and should have the opportunity to learn about mobile device security (Patten & Harris, 2013). The campus community must be made aware of several important practices which will lead to a more safe and secure BYOD environment. Initially, BYOD users must be mindful of the critical nature of keeping personal devices updated with the latest operating systems and patches available from device manufacturers. Since end users are typically the device administrators and support staff have little control of the connected devices, users must be responsible for security updates. Regular awareness programs can assist to educate the campus community on their part in maintaining a secure BYOD environment (Shumate & Ketel, 2014). Additionally, it is important to be aware of the various threats presented by malware, viruses and phishing attacks, how to avoid them, and what to do if a

device is compromised. By communicating these best practices through training and awareness programs, campus BYOD users will be able to mitigate the impact of many potential threats.

Policy and training are an important first step in maintaining a secure BYOD environment; however, information technology and security team members must make best efforts to secure the physical network. In developing the campus network, careful thought must be given to its design. One strategy in the network design is to isolate different groups of devices and users by the content and usage those groups will require. For example, student access should be isolated via a separate network or virtual network. The Virtual LAN (VLAN) concept allows network segmentation, performance enhancements and efficiency, ease of administration and troubleshooting, workgroups and increased information security (Patel, Ghaghda, & Nagecha, 2014). This method could provide separate networks for student wired and wireless access, thus minimizing potential risk by restricting what resources can be accessed. Additional segmentation could be leveraged for faculty and staff, who need a higher level of access to internal campus systems and resources.

In addition to the physical network design and security, network access control functionality should be considered. In recent years, many educational institutes have adopted BYOD onto their campus--most via network access control (Musarurwa, Gamundani, & Shava, 2017). Network access control allows for devices to automatically be assigned to the correct network with the appropriate access based on the attributes of the device or user profile (Ali, Qureshi, & Abbasi, 2015). For example, students would be able to register their personal devices, and each would automatically be assigned to the correct network, enforcing the access and policies required for student-owned devices. Likewise, campus-owned equipment or

faculty/staff devices could be assigned to networks with access to additional resources based upon the needs specific to their position.

Network access control systems also can set standards and minimum requirements to access the network. Prior to being allowed upon the college network, scanning can be used to ensure a device has a secure state from onset and to set a baseline (Shumate & Ketel, 2014). When devices initially enroll in the network access control system, certain requirements can be defined before access is granted. Examples of these requirements could be minimum operating system versions, security patches, and even the presence of antivirus programs. This feature automates the management of the many devices attempting to access the network, lowering the burden placed upon support staff. Network access control systems allow support staff to ascertain which devices are utilizing campus network resources. Additionally, enforcing a security posture check increases user awareness and limits the number of insecure connections to the campus network.

Another best practice for BYOD implementation centers around the network perimeter defense. Network devices such as firewalls and intrusion detection systems create a more secure network for BYOD users and are a critical part of the security of the campus network. The first step recommended for perimeter defense is the implementation of a firewall. The firewall defends the perimeter of the campus network by inspecting traffic and preventing access to unauthorized resources while simultaneously logging actions for audit purposes (Patel, Ghaghda, & Nagecha, 2014). Most modern “next generation” firewalls allow higher levels of access control beyond the simple allowing or denying of traffic. Firewalls with advanced threat protections allow malware, virus, and spam to be stopped at the perimeter before reaching end user devices. Many firewalls can control traffic at the application layer, enabling certain

applications to be limited or blocked if determined to be a threat to the campus network or systems (Kao, Chang, & Chang, 2015).

A second step in perimeter defense is to implement an intrusion detection and prevention systems (IDPS). IDPSs combine the detection methods of intrusion detection systems (IDS) with the capability to react to changes seen in intrusion prevention systems (IPS) (Whitman & Mattord, 2016). IDPSs are effective tools for determining whether unauthorized users are attempting to access, have already accessed, or have compromised the network (Patel, Ghaghda, & Nagecha, 2014). IDPSs attempt to detect threats based on signatures or behavior seen in traffic passing through the device. If traffic is deemed as a threat, it can be blocked at the perimeter and information security support staff can be notified. As an option to a dedicated IDPS, many vendors offer intrusion detection and prevention functionality as a part of their firewall product. However, both a properly configured firewall and IDPS should be implemented, either separately or together, as a part of a holistic security solution for BYOD on academic campuses.

Conclusion

BYOD environments are complex, and the special requirements of college communities add further layers to the complexity. College BYOD environments present unique challenges related to the wide array of access scenarios which must be provided to faculty, staff, students, and visitors, both in and out of academic settings. Networks must be administered in ways which provide security and maintain the privacy of sensitive information, while also addressing the ever-growing demand associated with the proliferation of devices. This can be accomplished through the mindful development and implementation of sound policies which carefully balance the need for security against the freedom of thought, expression, and action held sacred in academic settings. A proactive approach to user training at all levels invites the entire college

community to be active participants in maintaining the security and integrity of the organization's network. The use of access controls and best security practices, including network segmentation, virtual LANs, and firewall and IDPS technologies, enable colleges to successfully navigate BYOD considerations. This results in the realization of both cost savings for the organization and enhanced educational experiences for its entire community.

References

*Ali, S., Qureshi, M. N., & Abbasi, A. G. (2015). Analysis of BYOD security frameworks. *Conference on Information Assurance and Cyber Security (CIACS)*, (pp. 51-61).

*Bello, A. G., Murray, D., & Armarego, J. (2017). A systematic approach to investigating how information security and privacy can be achieved in BYOD environments. *Information and Computer Security, 25*(4), 475-492.

Cisco. (2015). *Enabling Bring Your Own Device.* San Jose: Cisco.

DiFilipo, S. (2013, March-April). The Policy of BYOD: Considerations for Higher Education. *Educause Review, 48*(2).

Donston-Miller, D. (2013, August 1). 10 BYOD Lessons For Business From Higher Ed. *Informationweek - Online*.

*Drew, J. (2012). Managing cybersecurity risks. *Journal of Accountancy, 214*(2), 44-48.

Ericsson. (2018). *Ericsson Mobility Report.* Ericsson.

*Jayapandian, N., Pavithra, S., & Revathi, B. (2017). Effective usage of online cloud computing in different scenario of education sector. *2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS).* Coimbatore: IEEE. doi:10.1109/ICIIECS.2017.8275970

Johnson, K. (2012). *SANS Mobility/BYOD Security Survey.* SANS. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/mobility-byod-security-survey-35210

*Kao, Y.-C., Chang, Y.-C., & Chang, R.-S. (2015). Managing bring your own device services in campus wireless networks. *2015 International Computer Science and Engineering Conference (ICSEC).* Chiang Mai: IEEE. doi:10.1109/ICSEC.2015.7401456

*Musarurwa, S., Gamundani, A. M., & Shava, F. B. (2017). A review of security challenges for control of access to Wi-Fi networks in tertiary institutions. *IST-Africa Week Conference*. doi:10.23919/ISTAFRICA.2017.8102371

*Patel, A., Ghaghda, S., & Nagecha, P. (2014, March 5-7). Model for security in wired and wireless network for education. *2014 International Conference on Computing for Sustainable Global Development (INDIACom)*. doi:10.1109/IndiaCom.2014.6828051

*Patten, K. P., & Harris, M. A. (2013). The Need to Address Mobile Device Security in the Higher Education IT Curriculum. *Journal of Information Systems Education, 24*(1), 41-52.

Sangani, K. (2013). BYOD to the classroom. *Engineering & Technology, 8*(3), 42-45. doi:10.1049/et.2013.0304

*Shumate, T., & Ketel, M. (2014, March). Bring Your Own Device: Benefits, risks and control techniques. *IEEE SOUTHEASTCON*. doi:10.1109/SECON.2014.6950718

Whitman, M. E., & Mattord, H. J. (2016). *Management of Information Security* (4 ed.). Boston: Cengage Learning.