Bring Your Own Technology (BYOT) to Education

Joseph M. Woodside
Department of Decision and Information Sciences, Stetson University
DeLand, FL 32746, US

and

Shahram Amiri
Department of Decision and Information Sciences, Stetson University
DeLand, FL 32746, US

ABSTRACT

In an effort to reduce costs and increase worker satisfaction, many businesses have implemented a concept known as Bring Your Own Device (BYOD) or Bring Your Own Technology (BYOT). Similarly, many school districts are beginning to implement BYOT policies and programs to improve educational learning opportunities for students who have a wide variety of technology devices. BYOT allow districts with limited budgets enable usage of technology while improving student engagement. This paper explores the technology devices, and educational implications of policies, device management, security and included components.

Keywords: BYOT, Wearable Tech, Education, Learning Technology

1. BRING YOUR OWN TECHNOLOGY (BYOT)

Businesses are spending increasing amounts of resources on technology devices for employees such as laptops, tablets, phones, computers, printers, scanners and other devices. In an effort to reduce costs and increase worker satisfaction, many businesses have implemented a concept known as Bring Your Own Device (BYOD) or Bring Your Own Technology (BYOT). In one case study Cisco was able to increase productivity by $300 million, eliminate $1.3 million in device spending, and reduce end-user support costs by 25%. BYOD and BYOT is a disruptive force where employees are able to bring their personal devices into the organization and connect [1]. Where BYOD typically focuses on smartphone and mobile devices, BYOT expands to all technologies including recent trends in wearable tech. Similarly, many school districts are beginning to implement BYOT policies and programs to improve educational learning opportunities for students who have a wide variety of technology devices [2]. BYOT allow districts with limited budgets enable usage of technology while improving student engagement [3].

2. SMARTPHONES AND MOBILE DEVICES

The top smartphone operating systems by sales share include Android, BlackBerry, iOS, Windows. In the majority of regions, Apple was second to Android, with several companies challenging leaders within varying degrees of success depending on region [4].

Android is an open source operating system by Google and runs over a billion mobile devices globally. Due to its ownership by Google, works in conjunction with a number of Google products and applications. Android also runs on additional devices such as netbooks and cars [5]. The current version of Android 4.4 is also named KitKat, with the next version Android 5 expected during 2014. Anticipated new features include expanded chat services and wearable tech built-ins, such as fitness components to compete with Apple, along with API compatibility with Android-based smart watches and Google Glass [6].

Apple iOS is a proprietary operating system that was introduced in 2010, which started with the Unix core in Mac OS X. The iOS runs the iPhone, iPad, and iPod touch. The current version iOS 7 underwent a significant visual update consisting of layering. Besides new software support, improved multitasking, AirDrop, another key security feature was the introduction of biometric thumbprint detection to unlock the device. iCloud is another feature built-in to iOS, which allows users to wirelessly sync their content across all their devices and provides a secure backup of data [7,8].

The Windows Phone by Microsoft version 8.1 was also recently released with new features intended to compete with Android and iOS. One key feature is Cortana, a voice activated assistant. Other features include a notification center for emails, updates, and information. An updated app store has been released, along with an updated internet browser with HTML5 support [9].

BlackBerry, from Research in Motion (RIM) was an original leader in the mobile industry with the BlackBerry solution in 1999. In 2009 BlackBerry held approximately 50% market share, though has since declined to a few percentage points. Company officials blame absence of apps, and introduction of the iPhone win 2007 with touchscreen only and no physical keyboard, also the reliance solely on email instead of a total mobile experience. With the latest release of BlackBerry 10, additional features have been made include formally adopting the name BlackBerry from RIM. Some key features include a communication hub to link email, social media and other updates. An updated touchscreen keyboard, extended battery life, and improved HTML5 browsing [10, 11].

3. WEARABLE TECH

One of the latest trends in BYOT is wearable tech such as smart watches and glasses. Shipments of 100 million wearable

devices are estimated in 2014, with 485 million by 2018. To further educational learning opportunities these devices must also be incorporated into the classroom and a tremendous area of growth potential within an innovative classroom environment. With BYOT in education, instead of demanding students turn off or put away technology devices, BYOT captures the students use and interest of technology within an educational context [12].

The initial items released under wearable tech included watches and eye lenses, followed by fitness and health monitoring devices, then smart watches with an example being Samsung's Android powered Galaxy Gear smart watch. The smart watch allowed connections to a smartphone, health, and fitness patterns. The most recent notable entry was Google Glass, an eyewear with connection to a smartphone, GPS, voice activation, camera and video recording. These devices utilize demonstrated technology such as Wi-Fi, Bluetooth Smart, Near Field Communication and GPS [12].

Apple, Microsoft, Blackberry, Android, Google, and Samsung are all interested and reviewing possibilities for integration of their devices with wearable technologies. Future ideas include biological data trackers, physician use in operating rooms, vehicle integration, and medical sensors. Apple's CEO Tim Cook has indicated that the company is interested in wearable tech, but has to yet make any formal announcements on a new device in this area, though expected to release a device in 2014. Future versions of iOS are expected to contain health and fitness functions, driven by patents in areas of biometrics [12, 13].

4. EDUCATIONAL IMPLICATIONS

When implementing a BYOT strategy, a few of the best practices include development of a formal set of policies including governance, compliance, equitable access to technology, and acceptable usage. The second component includes device management and ensuring compatibility between all devices and development of the appropriate infrastructure to accommodate the increase in demand of traffic and user connectivity. The last area is security, and verifying all devices contain up to date anti-virus software and patches to prevent unauthorized access or loss of data [1, 3].

BYOT Policies

Below are a set of example policies for BYOT. These policies ensure that appropriate board and district components are taken into account. Some policies are more open and describe only rules rather than true polices, and there are many ways a BYOT program may be successfully implemented [14].

Acceptable Usage: Existing policies must be reviewed to ensure they are compatible with BYOT and modified as appropriate. Individuals are still bound by acceptable use guidelines whether on personal or provided devices. Also device usage time can be restricted and not permitted at all times. Acceptable personal computing devices may include laptops, netbook, tablet, cell phone, smart phone, e-reader, iPad, iPod. Gaining devices with Internet access are not permitted [14, 15]

Technical Support Levels: In most cases, BYOT support is the responsibility of the individual, and they are expected to be knowledgeable on the device's usage. The company or educational facility personnel to not provide direct support for devices. This is primarily due to the range of devices and resources necessary to provide complete support [14].

Network and Software Access: Individuals are provided with Internet access and wireless access which may be filtered, and also reduced for bandwidth. Individuals may download and install any additional applications, components, or storage as they see fit, granted any do not conflict with the ethics and acceptable use policies. This is viewed similar to public access in coffee shops, hotels, or other public access points permitted [14, 15]

Technology Ethics and Acceptable Usage: For acceptable use, this is using technology as a privilege to improve the skills, knowledge and abilities students will require in the 21st century. One important component of BYOT is acceptable online behavior and safety [14].

Lost or Stolen Devices: Personal devices are used at one's own risk, loss or damage would need to be covered by the individual. Due to lack of secure storage, theft is often cited as a top reason students did not bring personal devices [14].

Staff Training: While in some cases instructors were not provided with direct training, after implementation recommends providing professional development to learn best practices and have an interactive community to share insights and expertise. An entrepreneurial spirit is encouraged along with experimentation to achieve the best results of BYOT and share those results with others to continuously improve [14].

Device Management

In order to ensure compatibility and consistent user experience across devices, organizations should utilize open standards. One such open web standard HTML5 is intended to allow cross-platform usage with a promise of write once and run anywhere, for example a Windows, Apple, or Android user could all access the same application across devices and platforms. This allows the developers to focus on the features and functionality rather than the conversion between platforms. Along with operating systems, screen sizes, resolutions, aspect rations, orientations, cameras, GPS, accelerometers and other features may vary by user and device. HTML5 is designed to accommodate these items through dynamically adapting to platforms variables and delivering a consistent experience. Currently the major browsers Internet Explorer, Firefox, Opera, Safari, and Chrome support HTML5 and CSS3, with full readiness varying [16, 17, 18]

In a letter from Steve Jobs, Apple believe that all web standards should be open, creating a conflict with Adobe Flash Player a proprietary web software. Apple supported open standards such as HTML5 of which are controlled by a standards committee of which Apple is a member. Apple went on to cite the security, reliability, and mobility issues associated with Flash included items such as ease of use with touch-compatibility and power consumption [19, 20].

Security

In order to ensure adequate security is in place for user of mobile devices, security methods must be employed. In discussing security methods, or the tools and techniques used to prevent security issues, there are three main categories: 1.

authentication and authorization, 2. prevention and resistance, and 3. detection and response [21].

Authentication and authorization deals primary with people, which is often the greatest source of security breaches. This includes people both inside the organization who may misuse or distribute their access, and people outside the organization and may include social engineering to learn access information. Strong information security policies and security plans such as password and logon requirements can help prevent these types of issues. Authentication confirms the user's identity, whereas authorization provides a user with appropriate permissions to the environment. Smart cards, tokens, and biometrics are types of devices that improve authentication of the user and implemented in conjunction with passwords [21].

Prevention and resistance deals primarily with data and technologies including encryption, content filtering and firewalls. A firewall is a hardware or software device that analyzes information to detect unauthorized use. Content filtering prevents uses software to prevent emails and spam from being received or transmitted. Encryption requires a special key to decode the information and make the information readable, this is used for secure information such as financials or other protected information [21].

Detection and response deals primarily with attacks by analyzing suspicious activity such as password attempts or file access. Intrusion detection software will monitor and alert if patterns are detected and can even shut down part of the network as warranted (Baltzan, 2012). Organizational users need advanced tools similar to malicious users and the advanced tools being used to compromise the systems. Security Intelligence and event monitoring systems analyze network, user, application, and datasets to identify trends, behaviors, and incidents [22].

For dataset inputs these include firewall, network, system, application, rules and other event logs. These logs are then normalized to a standard format for review. Once standardized, the data is analyzed for patterns, and alerts are generated for user review. Examples of analysis methods include aggregation and categorization of logs and events, time of events and directions, statistical log, source and host information, and top items within various categories for further detailed drill-down and analysis. Examples of analysis output include the ability to detect unusual application behaviors, unusual network connections, user behavior, network baseline deviations, and compromised credentials. Other methods analyze historical data to recreate scenarios for auditing, and also generate detailed and summary reporting output for security professionals, compliance officials, or other end users to review. Organizations are beginning to establish a security center in which monitoring and investigations occur [22].

5. CONCLUSION

BYOT interest is increasing in business and educational industries. With the explosion of smart devices and wearable technologies, this trend will continue over the next several years and must be addressed and leveraged for success. The technology can support both learning and productivity in employees and students. Future directions include developing curriculum to support BYOT, learning outcomes, and evaluation of BYOT in an educational environment.

6. REFERENCES

[1] Gartner, **Bring Your Own Device**, Gartner, 2013.

[2] Digital Learning Day, **Bring Your Own Technology/Device (BYOT/D)**, Digital Learning Day, 2011.

[3] W. Wong, **BYOT Improves Learning Without Breaking the Bank**, EDTECH, 2011.

[4] L. Whitney, **iPhone Market Share Shinks as Android, Windows Phone Grow**, CNET, 2014.

[5] Google, **Android**, Google, 2014.

[6] G. Beavis, McCann, J., **Android 5 release date, news and rumors updated. Here's what we know about Android 5.0/Android 4.5 so far**, TechRadar, 2014.

[7] Verge, **iOS: A Visual History**, Verge, 2013.

[8] Apple, **Apple iOS**, Apple, 2014.

[9] B. Griffen, **Windows Phone 8.1 Review: The good, the bade and the ugly**, Digital Spy, 2014.

[10] Blackberry, **Blackberry Company**, Blackberry, 2014.

[11] J. Garside, **Blackberry: how business went sour**, The Guardian, 2013.

[12] R. Patel, **Where is wearable tech headed?**, Gigaom, 2013.

[13] A. Cover, **Apple's wearables will be for fitness**, CNN Money, 2014.

[14] M. Ray, **BYO What?**, Library Media Connection, 2013.

[15] TeachThought Staff, **11 Sample Education BYOT Policies to Help You Create Your Own**, TeachThought, 2013.

[16] W3C, **HTML5**, World Wide Web Consortium, 2014.

[17] Intel, **Building Cross-Platform Apps with HTML5**, Intel, 2013.

[18] J. Wolf, **Responsive HTML5 Apps: Write Once, Run Anywhere?**, Wired, 2013.

[19] S. Jobs, **Thoughts on Flash**, Apple, 2010.

[20] P. Irish, D. Manian, **HTML5 and CSS3 Readiness,** HTML5Readiness, 2013.

[21] P. Baltzan, A. Phillips, **Business Driven Technology,** McGraw-Hill Irwin, 2012.

[22] LogRhythm, **Security Intelligence: Can Big Data Analytics Overcome Our Blind Spots?**, 2012.