BYOD What You Need to Know

By: Vicki Holzknecht

East Carolina University

Contact: holzknechtvi07@students.ecu.edu

Abstract

International Data Corporation (IDC) analyst predicts in 2014 on a worldwide scale one hundred and seventy-five million workers will be using their own devices in the workplace and by 2017 that number will be estimated to three hundred and twenty-eight million (Hamblen, 2014). Gartner survey reported 50% of corporate users would rely on a mobile browser instead of a desktop client by the year of 2016 (Sophos Labs, 2012). Many information technology departments and security experts are not keen on the Bring Your Own Device (BYOD) concept because of all the loaded guns. Who owns the data (apps, pictures) on the device? If a mobile device management system is installed on the device how can the company discern what is considered invading user privacy and what is not? What requirements must be addressed to create a comprehensive policy that will not backfire on the company if brought into legal action? All of these questions are addressed within the following document. The primary goal of this research is to use this document as a tool to those who need to tackle the BYOD head, because BYOD is here to stay!

BYOD Trending

Bring Your Own Device (BYOD) has steadily been gaining traction since the late 2000s. Intel was one of the first major companies in 2009 grabbing the bull by the horns embracing the BYOD trend instead of rejecting it (Harkins, 2014). Accepting BYOD in an enterprise or in a higher-education environment comes with a main course of benefits for employees but also a side dish of annoyances for departments responsible for gatekeeping critical information from cyber criminals. The original notion of implementing BYOD into the workforce was to encourage employees to be more productive letting them use their own device(s) (Violino, 2012), whether it was a smartphone, tablet or laptop, providing a sense of familiarity for the employee.

BYOD is no longer a trend, it's almost a business essential; employees check email, take notes, manage calendars, practically anything that they could do sitting at their desk (Pavón, 2013). Jim Rhodes of AppRiver Mobile Solutions believes in todays business when you hire a new employee, companies are basically hiring their mobile device (2013). In 2013 an estimated figure of 50% of employees will be using smartphones within mid-large size North American organization, 25% will be using tablets such as an iPad and by 2013 at least 90% of all enterprises will embrace BYOD (Violino, 2012).

BYOD Blunders

A survey by CompTIA contradicts the statement of "*90% of enterprises will accept BYOD*, *practices*" reviewing responses from four hundred IT and business executives 39% to 51% are not permitting the use of BYOD (Kaneshige, 2014). Early adopters of BYOD struggled due to the lack of encryption on mobile devices (Jaramillo et al., 2013) straining existing networks (Karpinski, 2012), multiple platform support (Dysart, 2012) and liability issues (Wisegate, 2012). After analyzing their survey CompTIA made a list of blunders originally considered benefits in adopting the BYOD schema:

i. *Get IT out of mobile device purchasing and deployment arena*

   According to Aberdeen Group BYOD is punctured with buried cost: Mobile Device Management (MDM) software, zombie phones attacking budget, gaming expenses, etc. places a hole in the mobile budget.

ii. *Make a happier workforce*

   Lawyer involvements in preparing user policies full of jargon in approval of the companies right to access, monitor and review data on a personal device.

iii. *Make a more productive workforce*

   Less than half of the companies surveyed felt that BYOD contributed to employee's productivity. Many of the users do not want to work from home on the weekends, afterhours unless it's a necessity.

iv. *Make life easier for IT*

   Risk of data loss blindsided CIOs and other security experts because of third party apps installed on the devices. Centrify surveying five hundred employees in mid-large companies admitted that 15% had their personal account or password compromised.

(Kaneshige, 2014)

Lost or Stolen Devices

Today's security has improved on the two top mobile platforms Android and iOS. As an owner of iOS devices and a previous Android owner, first handedly users have the capability on an iOS using a fingerprint system, voice activation, a simple pin number that can be longer than four if toggled the correct switch. Android device are equipped with face recognition, pin code, pattern code to name a few. A survey by Consumer Reports discovered that 34% of Americans do not use the mobile devices built-in security features (Weisbaum, 2014). This presents a problem when personal devices are used in a business environment inside and out.

Users tend to leave or lose their devices due to their smaller form factor (Phneah, 2013). A mobile device in the United States in 2011 was lost every 3.5 seconds (Romer, 2014) equivalent to 9 million lost devices a year. In a 2012 December report Asurion reported after thirty days of activating a mobile device 60 million were lost, stolen, or damaged each year (2012). Annually two million laptops are stolen, misplaced or lost in the United States alone (Karpinski, 2012). Why is this information significant? One of the biggest challenges that companies struggle with is gaining control of protecting data from being leaked into the wrong hands becoming a treasure trove for those who target data (Gruman, 2007) possibly resulting in an embarrassing information spillage to a competitor.

Many users cache their app credentials so when connecting to a Wi-Fi spot their email or work related apps are automatically logged in (Romer, 2014). Now understand, if the device is loss or stolen a hacker can use password cracks to gain access inside the phone, potentially leaking any data that is personal or corporate. Security breaches have compromised more than five hundred million United States records alone since 2005 (Sophos Labs, 2012). Four out of ten organizations admit to having breaches in security that were BYOD related according to a 2012 Trend Micro survey report (BYOD Brings Security Challenges, 2014).

Platform Selection

With the variety of platforms available in the mobile market it is difficult to decide what devices to support and reject on the business network. According to Wisegate Online IT

Members Figure 1 is the result of the poll of what operating systems (OS) to allow and access company email resources:

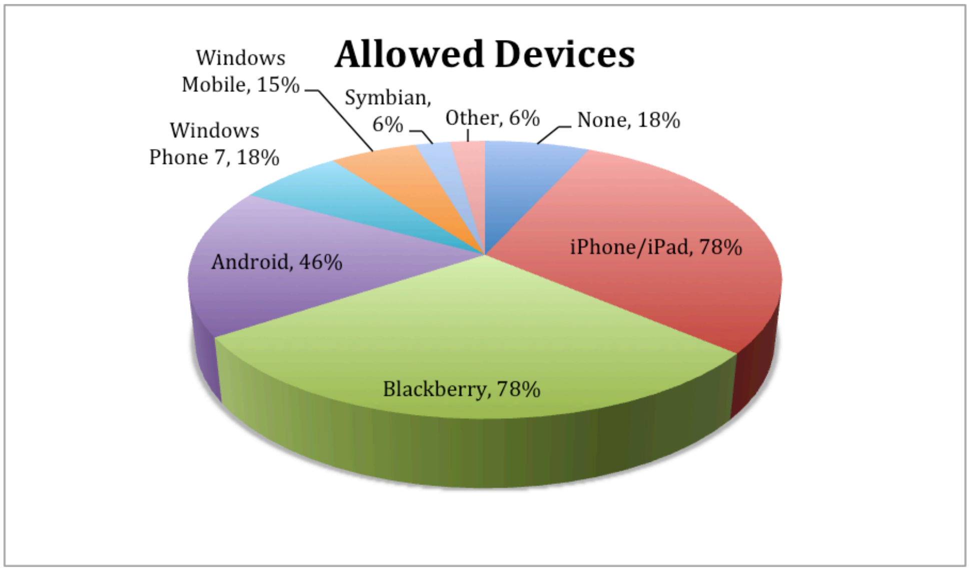

Figure 1 (Wisegate, 2012)

Notice that the pie chart does not equal to one hundred percent, reason being is the members of Wisegate were able to select more than one OS. Majority of Wisegate participants approximately 71% said “NO” they would not allow an Android device to be supported on their network because of viruses and the (uncontrolled) chaotic marketplace (2012). Android platform has been labeled “Typhoid Mary” (Stephenson, 2013), because of the trojanized apps that can spread rapidly through a corporate network. In 2011 Google removed more than one hundred malicious apps off the Google Play Market (Sophos Labs, 2012). McAfee Digital Assets Survey determined that 32% of the mobile users polled did not believe their devices needed to have any anti-malware software on their devices (2012).

The most preferred platform was iOS 5; Apple (controls) reviews the apps created by the developers, sandboxing and policies that are allowed via a mobile device management system (Wisegate, 2012). Blackberry is still in the running because of Enterprise Server allowing

Blackberries to be easily controlled: management of security, applications, and data in a secure manner (Jaramillo et al., 2013).

Mobile Device Management

Mobile Device Management (MDM) is software used for security, policy, inventory management (Gartner, 2013), encryption, enforcing pins, tracking user activity / location in real-time, remotely locking / wiping the device (Pavón, 2012). In 2019 the MDM market is expected to hit the $4 billion mark (Kaneshige, 2014) because of the popularity of the BYOD. The top three Mobile Device Management / Security Tools are Fixmo SafeZone v5.0, Good Technology, and Sophos Mobile Control based on a group testing presented by SC Magazine (Stephenson, 2013). Table 1 is a brief overview as to what each of the MDM products are capable of doing.

Product	**Maintain Security Policy through app / ActiveSync**	**Allows White/Black Listing**	**Remote Wiping**	**Browser Content Filtering**	**Supports iDevices**	**Supports Android Devices**	**Supports Windows Mobile Devices**	**Supports Blackberry Devices**
FixMo SafeZone v5	◉	◉	◉	◉	◉	◉		◉
Good Technology	◉	◉	◉	◉	◉	◉	◉	
Sophos Mobile Control v3.5	◉	◉	◉	◉	◉	◉	◉	◉

Table 1 (Stephenson, 2013)

Virtualization: Mobile Separation

Mobile virtualization techniques have advanced over the past couple of year's one in particular hypervisor virtualization separation (Jaramillo et al., 2013). Companies should consider virtualization options when moving towards supporting BYOD. Hypervisor technology or virtual machine manager (VMM) allows, "guest" OS(s)to run on the mobile device (host)

(TechoPedia). Hypervisor technology gives the ability to run more than one occurrence on the same device segregating business data from personal data (Jaramillo et al., 2013).

◊ **Hyper Visor Virtualization:**

- Type 1: Bare Metal Virtualization

  Allows for multiple OSs to run off the mobile device in its own unique environment shell sharing the hardware (memory, storage, processor, etc.) of the device. Having the OSs isolated from one another or in their own environment shell creates a level of security.

  Example: Corporate X creates a virtualized environment running a separate OS on the mobile device so the user can gain access to corporate data when not on the corporate network. The user decided to install Angry Birds not knowing that it was a cloned copy of the popular app loaded with malware (Sophos Labs, 2012). Now, the mobile device has been infected stealing credentials, sending information to the developer's remote server. However, the OS that Corporate X created is unharmed because it is living in a separate environment "isolated" from the mobile devices environment.

- Type 2: Hosted Virtualization

  Allows for one OS to be installed and layers on top of the host mobile device OS. Looking back at the previous example if something malfunctions or affects the mobile device, Corporate X's environment could be rendered inoperable, depending on the damage of the mobile device OS.

(Jaramillo et al., 2013)

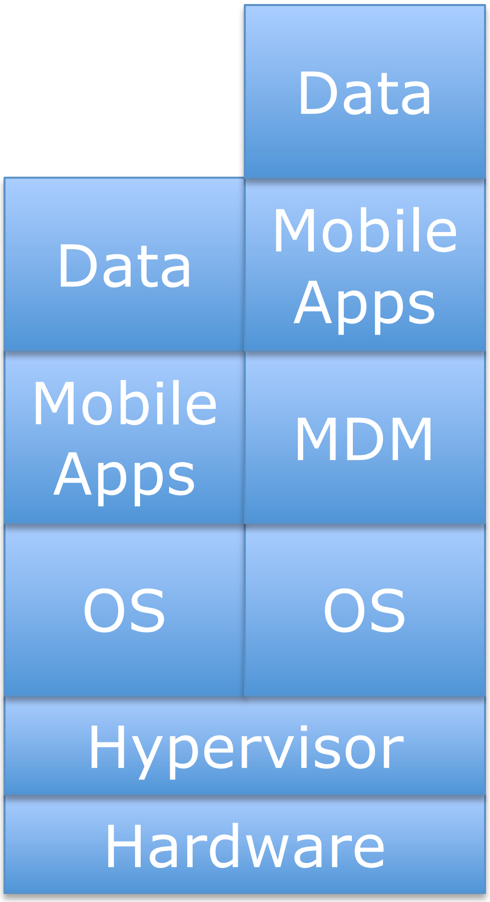

Figure 2 Type 1 (Jaramillo et al., 2013)

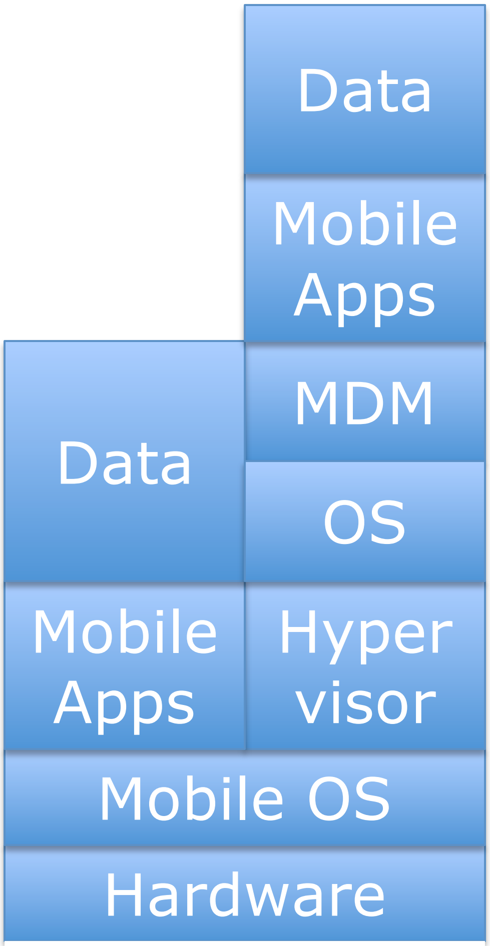

Figure 3 Type 2 (Jaramillo et al., 2013)

Figure 2 and Figure 3 demonstrates a rough visual representation of Type 1 and Type 2 virtualization separation techniques. Each figure is divided into two sides the left side being Personal and the right side being Enterprise.

Polices and Legalities

Companies are at risk when consenting to the use of personal mobile devices, without an effective policy and BYOD programs can create problems with the owner of the mobile device (Pavón, 2012). Who should be part of the writing of the policy process? Involve Human Resources, legal team, internal constituents, along with someone from the information security departments (security managers, CIO), etc. (Wisegate, 2012). There is a fine line of privacy monitoring, company’s can cross when users own the device. Balancing a policy that will not violate the users privacy but permits the company to monitor the company data is one of the biggest encounters companies will face when drafting and implementing a successfully policy (Pavón, 2012). There are five key topics to consider but not limited to when creating a policy / user agreements: data wipes, permitted photos, data breach policy, also web filtering requirements and a definition of what sensitive data is (Wisegate, 2012). To cover all bases other topics to consider are timely notification of when the device was lost/stolen; force password strength of a minimum of twelve characters or more (combining symbols and alphanumeric) (Dysart, 2012); the use of social networks (FaceBook, Twitter, Instagram, etc.) and third party cloud storage apps (Dropbox, Box, Google Drive, etc.). Sophos labs discovered that there were forty five million users of Dropbox and researchers were able to hack into the cloud storage three different ways gaining access to data without having to authenticate (2012). The sole purpose of using cloud storage is so data does NOT exist on the mobile device, just in case something happens to the mobile device. Employees who use third party cloud storage place the enterprise data at risk for "cross-pollination," once this occurs the data must be considered compromised (Pavón, 2013).

Before any MDM software is installed on a users personal device, the user needs to consent and fully understand exactly the software's maximums. If the user agrees to the policy of the MDM software install, the company will not look as if they are being misleading when monitoring the users device. Also, the user needs to be made aware of what happens in the event of the device being lost or stolen, termination of employment / leaving the company and exactly what is the company's contingency plan. Michael Irvin a full-time healthcare consultant for AlphaCare in NYC, was at a restaurant one evening when his iPhone blacked out, rebooted, when the phone came back on it looked as if it just came from the factory (Weber, 2014). All of his personal and corporate information was erase (contacts, calendars, text messages, family photos, apps, music) was erased (Ouellette, 2014). The BYOD policy that Mr. Irvin agreed to included the remote wiping, though he claimed he never knew about it. AlphaCare sent an email on the same day to Mr. Irvin warning that the remote wipe was going to occur (Weber, 2014). Was Mr. Irvin telling the truth that when he agreed to the BYOD policy remote wipe was not in the agreement? Did AlphaCare update the policy injecting the remote wipe without informing Mr Irvin? Or was the remote wipe policy in the original policy he agreed to and Mr. Irvin overlooked it? All of these questions could be avoided if a sound BYOD policy had been in place and was reviewed regularly just in case there were any alterations made after the first policy acceptance.

A 2013 survey by Symantec revealed that after twelve months of either being fired or leaving the company half of the employees keep the corporate data and around 40% intended on using that confidential data as an advantage in their next employment (Kaneshige, 2013). This may seem ethically and immorally wrong, however 62% believe that it was ok to transfer corporate files to a personal device and saw no offense (Kaneshige, 2013).

Pavón, believes in "smart-lawyering," when preparing a BYOD policy make sure the policy process is explained in full-detail (2012) any loopholes within the policy can be used against the company in legal lawsuit by the employee. For example, if any changes in the policy are made, make aware to the user of the changes and make them sign the policy change agreement. Jeff Schmidt at BT Global Services suggests periodically reviewing policies making sure the company stays ahead of the consumerization curve (2012). He is also a firm believer of companies testing out their policy to try and break them; "*testing for success is good, testing to try and break them is better*" (Schmidt, 2012).

What Users Can Do?

Before adhering to any policy put forth by the company, the company should provide the users with a prerequisite checklist of items ensuring their mobile device is safe to use on and off the corporate network. Here are the DOs of mobile security. Make the device password difficult to crack (Tittel, 2014) but something to remember. If going to use a pattern pin, make sure to wipe the display off due to fingerprints grease and the pattern to get into the device is still visible. Require the device to automatically lock after phone is idle for a short period of time. Use the encryption feature on the mobile device to add an extra layer of security. When connecting to a Wi-Fi access point try using security-enabled networks instead of open Wi-Fi networks to avoid drive by attacks. Run the latest operating system version and double check to make sure apps installed are up-to-date. Install an anti-virus or malware app protection (Tittel, 2014) to prevent viruses, Trojans, malware, from infiltrating the mobile device.

The Do Not's of mobile device security is using open Wi-Fi networks at the local Starbucks or McDonalds, to conduct business; drive-by's and shoulder surfers are always close. Never store critical data on the device in case of loss or theft, use a secure cloud app to back up data. Disable auto fill so user information is not stored / remembered; remove any apps that are no longer being used. Do not install an app without a thorough review, glancing at permissions, reviews by other mobile app users and making sure the anti-virus / malware protection scans the newly installed app for any rogue Trojans that are hidden inside the app just waiting to snatch user data. User's should NOT walk away from mobile device even if its just for a minute or two, keep mobile device around at all times

If an owner of the mobile device cannot abide by the stipulations devised by the company for protecting mobile devices to help mitigating data seepage into the wrong hands then at this moment of time it would be best to decline the mobile user from being apart of the BYOD network; allowing them to only check email and calendar with no access to critical information or an encrypted Wi-FI network; until the user complies with the mobile security checklist.

Conclusion

After extensive research on Bring Your Own Devices there are positives and negatives when implementing such an arduous and cumbersome model. The positives are the flexibility BYOD provides the users when away from their desk allowing them to access corporate data when off the network and the ability to check email and perform calendar task. Users perform better when they can use technology already having prior knowledge about, a sense of familiarity; most users are not susceptible to change. Previous BYOD adopters would tell you that the negatives outweigh the positives. Purchasing security tools such as mobile device management along side of virtualization software isolating the OSs from one another providing an extra layer of security can be costly depending on what the company needs. Upgrading older networks to support the growing demand for BYOD is not cheap, again dependent on what is needed to meet the demand of BYOD. Users can take a proactive approach and install anti-malware apps to discover malicious apps being installed; create long password, having device lock itself after being idle for so long and not having their user credentials cached just to name a view. Trying to discern what is considered monitoring a users device and invading the privacy of the user on their device needs to be addressed with a comprehensive policy drafted by several key players: security specialist, human resources and legal counsel.

Having a flawless BYOD model is realistically impossible; there is not one right way to apply it. Companies need to research BYOD solutions early adopters had some success with. BYOD is growing, as time goes on technology will advance to address the present day gaping holes of BYOD.

References

Asurion. (2012). 60 million reasons to protect that cellphone you received as A holiday gift. Retrieved, 2014, Retrieved from https://www.asurion.com/about/press-releases/156-60-million-reasons-to-protect-that-cell-phone-you-received-as-a-holiday-gift/

BYOD brings security challenges. (2014). *Information Management, 48*(1), 18. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/1503672206?accountid=10639

Dysart, J. (2012). Mobile security. *Electrical Wholesaling, 93*(5), 28-n/a. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/1014209476?accountid=10639

Gartner. (2013). Mobile device management (MDM). Retrieved, 2014, Retrieved from http://www.gartner.com/it-glossary/mobile-device-management-mdm/

Gruman, G. (2007). Mobile security definition and solutions. Retrieved, 2014, Retrieved from http://www.cio.com/article/2439278/mobile/mobile-security-definition-and-solutions.html

Hamblen, M. (2014). With BYOD smartphones on the rise, IT headaches will become migranes. Retrieved, 2014, Retrieved from http://www.cio.com/article/2379233/byod/with-byod-smartphones-on-the-rise--it-headaches-will-become-migraines.html

Harkins, M.MOBILE: Learn from intel's CISO on securing employee-owned devices. Retrieved, 2014, Retrieved from http://www.govinfosecurity.com/webinars/mobile-learn-from-intels-ciso-on-securing-employee-owned-devices-w-264

Jaramillo, D., Katz, N., Bodin, B., Tworek, W., Smart, R., & Cook, T. (2013). Cooperative solutions for bring your own device (BYOD). *IBM Journal of Research and Development, 57*(6), 5:1-5:11. doi:10.1147/JRD.2013.2279600

Kaneshige, T. (2013). IT learns to COPE with mobile devices. Retrieved, 2014, Retrieved from http://www.cio.com/article/2380806/byod/it-learns-to-cope-with-mobile-devices.html

Kaneshige, T. (2014). What is going wrong with BYOD? Retrieved, 2014, Retrieved from http://www.cio.com/article/2375498/byod/what-is-going-wrong-with-byod-.html

Karpinski, K. Retrieved, 2014, Retrieved from http://resources.idgenterprise.com/original/AST-0122594_Transforming_Higher_Education_with_Mobility_Solutions.pdf

McAfee. (2012). 10 quick tips to mobile security. Retrieved, 2014, Retrieved from http://www.intel.com/content/dam/www/public/us/en/documents/guides/10-quick-tips-to-mobile-security-guide.pdf

Ouellette, P. (2014). Looking at both sides of the BYOD remote wipe policy debate. Retrieved, 2014, Retrieved from http://healthitsecurity.com/2014/01/22/looking-at-both-sides-of-the-byod-remote-wipe-policy-debate/

Pavón, P. (2013). Risky business: "bring-your-own-device" and your company. Retrieved, 2014, Retrieved from http://www.americanbar.org/publications/blt/2013/09/01_pavon.html

Phneah, E. (2013). Five security risks of moving data in BYOD era. Retrieved, 2014, Retrieved from http://www.zdnet.com/five-security-risks-of-moving-data-in-byod-era-7000010665/

Rhodes, J. (2013). Building security around byod. *Rough Notes, 156*(10), 104-104,114. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/1471050949?accountid=10639

Romer, H. (2014). Best practices for BYOD security. *Computer Fraud & Security, 2014*(1), 13-15. doi:http://dx.doi.org.jproxy.lib.ecu.edu/10.1016/S1361-3723(14)70007-7

Schmidt, J. (2012). Not your parents' workplace anymore - managing the new security realities of BYOD. *Security, 49*(9), 25. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/1223497701?accountid=10639

Sophos Labs. (2012). Security threat report 2012. Retrieved, 2014, Retrieved from http://www.sophos.com/medialibrary/PDFs/other/SophosSecurityThreatReport2012.pdf

Stephenson, P. (2013). Mobile device security. *SC Magazine, 24*(7), 36-37. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/1420256250?accountid=10639

Techopedia.What is A hypervisor? Retrieved, 2014, Retrieved from http://www.techopedia.com/definition/4790/hypervisor

Tittel, E. (2014). 7 enterprise mobile security best practices. Retrieved, 2014, Retrieved from http://www.cio.com/article/2378779/mobile-security/7-enterprise-mobile-security-best-practices.html

Violino, B. (2012). The BYOD security challenge. *Insurance Networking News, 15*(8), 29. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/1038086218?accountid=10639

Weber, L. (2014). BYOD? leaving A job can mean losing pictures of grandma. Retrieved, 2014, Retrieved from http://online.wsj.com/news/articles/SB10001424052702304027204579335033824665964

Weisbaum, H. (2014). Most american's don't secure their smartphones. Retrieved, 2014, Retrieved from http://www.cnbc.com/id/101611330#.

Wisegate. (2012). IT peers share advice on effective "bring your own device" (BYOD) strategies. Retrieved, 2014, Retrieved from http://www.wisegateit.com/resources/downloads/wisegate-effective-byod-policy-report.pdf