Mobile Device Management and Best Practices

Adam P Phelps

East Carolina University

Abstract

With the year 2014 slowly coming and quickly fading, the need to have the latest and greatest mobile device has become the new standard. Wireless speeds are increasing, Random Access Memory (RAM) is tripling, and processing time is becoming faster with half the size and power than in previous models. Moore's law has been proven yet again. But what does this mean for those who use these fast devices for work through a company loan? How do you limit what an employee's personal devices can access on the corporate network? What happens to the data when they leave? Who governs these rules and what is to become of them? In this paper, I plan to define what it takes to have good Mobile Device Management (MDM) policies and procedures in a corporate setting, and what a company should do to follow MDM best practices.

Keywords: Mobile Device Management, MDM, Mobile Devices

Intended Publication: InfoSec Writers

Mobile Device Management

A mobile device (also known as a handheld device or handheld computer) is a small computing device, typically having a display screen with touch input and/or a miniature keyboard and weighing less than 2 pounds (Wikipedia, 2014.) With the latest Google and Apple devices hitting the shelves monthly, it's hard to resist not getting the latest gadgets out of the stores and into your pockets. Social networking continues to rise each and every day, which is making the standard phone call a thing of the past. Doubling Wi-Fi speeds, tripling RAM, the amount of applications, or Apps, for these devices are growing at an exponential rate. Does this not sound like today's time of 2014? The technology is here, but the question is are CIO's and CEO's making the permanent switch to these powerful mobile devices? What security policies must be set in place to safeguard network services and company data if this is to be the new standard in the workplace? Is this something that "IT" organizations are willing to comply with and extend support for? The most obvious hazard so far is what happens when a wireless device is connected to the corporate network via WIFI. Company data is immediately at the fingertips of its user. If this goes unmanaged who knows what these insecure devices will do to a network. All these questions should raise concern, but the primary issues are still to be discovered. The following are primary reasons mobile devices should be used but cautiously implemented in a work place. Quality of Service - do too many mobile devices slow down the network? Spamming and Malware - is there a need for it on mobile devices? Will there need to be more support for these devices in an IT Help Desk type fashion? And finally, what happens if a device is automatically signed into a network and then the device is lost or stolen. How does the

company handle its potential security breach? These are the primary questions of concern that will be addressed throughout this paper followed by some best practices of Mobile Device Management.

Challenges

QoS and WLAN Access

When first asking the question, “How does a mobile device slow down, or inhibit a wireless network,” we need to look at some average devices capabilities. Let’s take a Smart Phone for example, such as an iPhone. This is possibly one of the most popular devices in the market, so we could assume they would be highly favorable in a corporate setting. They have WIFI capability, wireless N, G, and B signals (Apple, 2014.) It uses voice/video apps like Skype, and FaceTime; VPN connections can be established to a company network, again via WIFI (Apple. 2014.) Employees bring these devices into the workplace and expect to connect to the corporate network, but according to Christian Gilby, “These devices have not been tested by the enterprise, nor are they supported or endorsed by the company” (Gilby, C. 2008.) These devices often access the WLAN without the user's knowledge, as the radios are usually enabled by default (Gilby, C. 2008.) So essentially, if a device not as popular and well tested as an iPhone came into a corporate network, it potentially could disrupt the network severely enough to cause a network outage (Gilby, C. 2008.) A key consideration is to find ways to ensure these applications do not disrupt the mission-critical applications running on the network. One way this could be done is to maintain a database of authorized devices and have the WLAN system verify each device's hardware ID prior to letting it access the network. Many of today's WLAN systems provide a mechanism, called

Radius Mac filtering, which can be used to perform this validation process for any of the extended service set IDs (ESSID) on the system (Gilby, C. 2008.) If a company were to adopt this approach the MAC filtering would then be able to perform database lookups on the server and in return send a message to the device with either an accept or deny message, providing the device access to the WLAN, or rejecting it. To ensure Quality of Service, QoS, corporations should enable the WLAN features of the most important features such as voice, data, and video applications, and best effort services for guests or non-corporate devices (Gilby, C. 2008.)

Mobile Security

We now understand mobile devices are on the rise, with each passing year more and more devices flood into the market and become available for personal and corporate use. In fact, more companies have turned to using mobile devices. Among U.S. companies, 56 percent reported increased usage of smart mobile devices among managers, and 60 percent reported increases in staff usage (Next, 2007.) With this growth, improved mobile device management is a key priority to support mobilizing the workforce and to improve the productivity levels of mobile workers. This is such a phenomenal rate and one only can think of where these numbers will go in the near future.

So, what happens if an employee losses a corporate device or worse, what if they are robbed and the device is stolen? First, each organization should educate its workforce members on how to report loss or theft of a mobile device. Users should note and store the serial numbers for all electronic devices they may possess, and store them in a secure location. Such numbers increase the likelihood of finding a device if it's

stolen (Hughes, G. 2012.) Mobile devices can exploit vulnerabilities to corporate data; protecting this sensitive information on mobile devices is a complex task. You have to keep track of what files are being accessed, what company materials have been downloaded, and manage third parties who may have access to your corporate network. Should mobile devices be managed with administrators or audits? Yes, mobile devices should be able to be remotely wiped and/or lock by administrators. Audits should be conducted regularly to meet with various corporate regulations, and passwords should be as strong as possible. Let's face it; users do not want the extra expense and headache of managing the security on their corporate handset. The company/corporation needs to be vigilant when protecting itself from harmful threats and keeping sensitive information on its mobile devices safer. Incorporating VPN and authentication software for remote access is one way of addressing lost or stolen devices (Fitzgerald, J. 2009.) To manage mobile devices effectively and securely, policies must include security authentication through VPN, the use of WPA2 for wireless authentication, and remote termination and encryption/decryption using AES 256 cipher (Fitzgerald, J. 2009.) Using these methods will often keep mobile devices free from battery drinking security clients, mobile viruses/malware, and third party applications that cause phone crashes and user frustration. To add, some corporations have gone to the extent of blocking outside Service Set Identifier networks, (SSID's.) making their devices only able to access the local area network (LAN) and blocked all other incoming wireless signals (Fitzgerald, J. 2009.) Also, in the mobile environment, password protections should include automatic device shutdown after multiple unsuccessful login attempts. Such protections can wipe the device back to a factory state in the case of

loss or theft (Hughes, G. 2012). While on the topic of passwords, I have walked into many of offices and have seen passwords written on desks, sticky notes and other easy to spot locations around the office. This is not a safe practice and it can also apply to the mobile user. Organizational password policies for mobile users should be the same as workstation systems. Corporations must ensure that passwords are being used and are not written on the device. They should follow the best practical uses of passwords by using of strong passwords of at least seven to eight characters, including alphanumeric and special characters and having those reset every 90 days (Summers, N. 2009.) While mobile device management does seem to be this unbeatable Titan, following the above steps can help when facing lost or stolen devices, and securing classified data on an enterprise network.

Supporting the Multitudes

As mentioned earlier, the number of mobile devices is growing, and it will continue to grow at an exponential rate. What does a corporation do to provide support for this many devices? IT organizations are dealing with various types and product lines of mobile devices. These devices frequently run on different platforms, use different applications, different network access technologies, and so on. It can be very overwhelming as an IT person myself when someone walks in and has the new widget with the latest software. Personally, I don't keep up with every new operating system that comes out every two weeks so I can't troubleshoot the problem quickly and proficiently. This presents a problem when there are more important things to do in the office than configure someone's email, or open their last text message. Not to mention, many organizations have applications for general use that are not designed for mobile

devices, which again makes support that much more difficult.

What are the solutions for this endless cycle? Standardization. If a corporation is to provide for its employees, standardization should be the only option (Goth G, 1999.) A key to successfully integrating remote-access devices into the enterprise is developing simple and well-defined user requirements. Businesses and employees must determine which devices are best for which users, and which business functions need sustainable technical support (Goth G, 1999.) Looking at the business model and what important features a mobile device should have within the company should determine what devices are available that best suits each employee. This will limit selection and provide a steady ground on what applications and support can be provided for the device.

Mobile Web

Some companies now give remote workers access to their networks and applications through the Web; and because now so many websites are configured for many different web browsers, it's time for the whole company website to be specifically designed with mobile computing in mind. Through this mobile client interface, or mobile portal, companies can minimize bandwidth demand and be relieved that the main power users will not experience any latency.

Spam and Malware

We've all heard of Spam and Malware for our personal computers, but can this be a threat to a company's mobile workforce? Absolutely. Companies should consider adding on-device anti-malware, like firewalls to protect device interfaces (Galletto, N 2011.) Companies should also consider installing anti-spam software to use against

unfiltered voice and text media. This will allow the safest working environment and provide the best defense again cyber-crime (Galletto, N 2011.) Another easy way to limit what goes on an employee's device is to use software that limits what applications can be put on phones. For example, Apple has software called Configurator, for Macintosh computers. This allows an IT manager, or administrator, to seamlessly configure and deploy iPads and iPhones in a large setting (Weintraub, S 2012.) As stated in its description, Configurator passes through three simple workflows while preparing your new iOS devices for immediate distribution, supervise devices that need to maintain a standard configuration, and assign devices to users (Weintraub, S 2012.) With simple applications to use like this, companies should easily be able to manipulate and protect what goes on each devices located within the LAN, and more importantly, provide a safe and secure mobile device field.

Best Practices Recap

Many CIOs, Administrators, IT managers, and help desk technicians face overwhelming user demand to support personal mobile devices on the company WLAN. With the continuous increase of mobile devices, these new tools present new security risks, and potential network management and a helpdesk burdens, which are difficult to quantify but are clearly significant. Network vendors until now could not provide the features and tools necessary to accomplish the steep responsibility of aiding enterprise corporations with Mobile Device Management. This paper has touched heavily on managing mobile devices in a corporate setting, and will conclude with an overview of best practices corporations should follow.

Figure -1below, lists the concerns identified earlier, and shows how they can be addressed in corporate settings.

Corporate Challenges	Corporate Recommendations
Ensure mobile devices do not disrupt the mission-critical applications running on the network.	Maintain a database of authorized devices and have the WLAN system verify each device's hardware ID prior to letting it access the network. (Radius MAC Filtering)
Reassure QoS (Quality of Service) to corporate employees.	Enable vital LAN features voice, data, and video applications, and best effort services for guests or non-corporate devices.
What to do with lost or stolen devices.	Provide efficient training on what users should do in the event of a lost or stolen device. Secure serial numbers and ID numbers in a SAFE location.
Lost and stolen device security.	Devices that are lost or stolen should have the ability to be remotely wiped, or reset.
Wi-Fi access through LAN.	Policies must include security authentication through VPN, the use of WPA2 for wireless authentication, and remote termination and encryption/decryption using an AES 256 cipher.
Other WLAN's corrupting enterprise devices.	Block outside Service Set Identifier networks, (SSID.)
Hackers trying to Brute Force a password.	Password protections should include automatic device shutdown or wipe after multiple unsuccessful login attempts.
Password protection and security.	Corporations should follow best practical uses of passwords by using of strong passwords of at least seven to eight characters, including alphanumeric and special characters and having those reset every 90 days. Passwords should never be written on the device.
What to do for supporting multiple devices?	Standardization, a corporation should select one, maybe two overall devices to support and distribute to its user population.

Many website differences and compatibility standards.	Ensure all websites are mobile friendly for ease of use, and to maximize bandwidth.
Spam and malware creators are becoming cleverer in mobile platforms.	Upgrade your devices with spam and malware protection such as firewalls.
Users adding unsecure applications and third party software.	User administrator programs like Apples Configurator, to control what goes on a corporate device.

Figure - 1

Corporate issued devices such as iPhones, iPads, Androids, BlackBerrys, and Windows devices all are part of the general trend of technology which are flooding with popularity, and should be welcomed for its ensuing productivity gains. Like video collaboration, which has been a significant new trend in enterprise communications and will continue to see greater influxes of importance as Wi-Fi and cellular data networks progress. Large and small companies are buying mobile devices, providing mobile devices application access, and even developing new mobile device applications. CIOs, and IT departments must quickly recognize the growing value of mobile devices, and support these mission critical business tools with IT best practices for management, administration, and security that were mentioned above. Organizations that lay the groundwork with comprehensive management and control employee-owned mobile devices will be in strong position to capitalize on productivity-enhancing service emerging from technology; and anything else the future holds for these powerful handhelds.

References

Apple iPhone Tech Specs. (2014). Retrieved October. 8, 2014 from http://www.apple.com/iphone/specs.html

Fitzgerald, J. Managing mobile devices, Computer Fraud & Security, Volume 2009, Issue 4, April 2009, Pages 18-19, ISSN 1361-3723, 10.1016/S1361-3723(09)70049-1. (http://www.sciencedirect.com/science/article/pii/S1361372309700491)

Galletto, N., Rampado, S., & Proudian, K. (2011). Dangers lurking in mobile devices. *Canadian HR Reporter, 24*(19), 19-19, 25. Retrieved from http://search.proquest.com/docview/904654889?accountid=10639

Gilby, C. (2008). Mobile devices impact WLANs. Communications News, 45(1), 28-29. Retrieved from http://search.proquest.com/docview/202804209?accountid=10639

Goth, G., "Mobile devices present integration challenges," *IT Professional*, vol.1, no.3, pp.11-15, May/Jun 1999 doi: 10.1109/6294.774947 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=774947&isnumber=16824

Hughes, G. (2012). Mobile device security (updated). Journal of AHIMA, 83(4), 50-5. Retrieved from http://search.proquest.com/docview/947995487?accountid=10639

Next: Mobile device management. (2007). Communications News, 44(10), 6-6. Retrieved from http://search.proquest.com/docview/202803364?accountid=10639

Weintraub, Seth. (2012, March 07). Apple releases configurator app for mac [Web log message]. Retrieved from http://9to5mac.com/2012/03/07/apple-releases-configurator-app-for/

Summers, N. (2009, October 19). Building a Better Password. Newsweek, 154(16), E2. Retrieved from http://go.galegroup.com.jproxy.lib.ecu.edu/ps/i.do?id=GALE%7CA209693339&v=2.1&u=gree96177&it=r&p=HRCA&sw=w

Wikipedia. (2014, October 21). Retrieved from http://en.wikipedia.org/wiki/Mobile_device