4-1-2013

Managing and Securing Business Networks in the Smartphone Era

Sathiadev Mahesh
University of New Orleans, smahesh@uno.edu

Aaron Hooter
University of New Orleans

MANAGING AND SECURING BUSINESS NETWORKS IN THE SMARTPHONE ERA

Sathiadev Mahesh & Aaron Hooter, University of New Orleans

ABSTRACT

This paper discusses the impact of user owned mobile computing devices (smartphones, tablets, and future devices like Google Glass) on management and security of the corporate network. Personally owned portable computing devices are widely used at work and create a porous network perimeter for the enterprise network. The paper reviews corporate policies posted on websites along with research papers and corporate whitepapers to develop a comprehensive user owned mobile computing device policy. This is a rapidly evolving topic that has not been researched in the business academic literature. We survey trade journals and corporate websites for information regarding this policy and make recommendations that can be applied by business managers.

INTRODUCTION

The proliferation of portable, mobile computing devices has increased the number of user owned devices brought into corporate networks (Burt, 2011). Over 60% of companies allow user owned devices and there are believed to be over 150 million such devices connecting to organization networks (Schulze-Warnecke & Hartman, 2012). Most network managers in the past forbade users from bringing their own devices and connecting them to a corporate network, citing security concerns. However, that restriction is often lifted nowadays due to user demands. Even security conscious industries like banking have been forced to adapt to the "consumerization" trend in information technology, where users (consumers) are the first to introduce a new technology into the workplace, before corporate IT (LaBarre, 2012). Bring your own device (BYOD) policies for user owned mobile computing devices are part of this trend. In addition, the increasingly mobile employee works from multiple locations, and work is not restricted to the physical confines of the office.

The business gains from having access to the employee anytime, anyplace, blurring the work-leisure divide, and in addition may actually further save costs by having he employee purchase the preferred device rather than providing it out of the corporate budget. Employees are more comfortable using their own devices and especially the millennial generation is passionate about indulging in their passion for acquiring and using the latest mobile device (Accenture, 2010). The challenge facing the business network manager is the need to securely manage company data that on that device and in transit between the device and the corporate IT system. The device itself must be secured and needs to be tested to meet security standards. Finally, the task is further complicated by the need to understand security across many different devices and platforms.

A business should create a policy that will allow for the successful management of employee owned devices at work. Data encryption standards for corporate data loaded on these devices need to established and enforced. User education sessions explaining the important role they play in keeping their devices secure as well as the consequences of not complying to the company's policy for its network need to be conducted. The policy can be extremely strict and allow no user owned devices, can permit other devices but limit them to net access, allow user owned devices to access existing services, or permit many devices and create new services to support them effectively (CISCO, 2012).

The policy needs to consider the technological advances that have rapidly advanced the capabilities of portable devices and the increased integration of these devices into work processes. These changes have made portable computing an integral part of employee work processes. At the same time, the devices facilitate extensive data theft, malware intrusion in business networks and impose an ever-increasing burden on corporate network managers. The BYOD policy should balance network security and effectiveness with employee empowerment in the richly interconnected business environment. Organizational policies have not kept up with the rapid proliferation of this technology as clearly demonstrated in two surveys of 650 IT managers conducted in 2012 (Johnson & DeLaGrange, 2012). In the first survey nearly three fifths of the organizations allowed some form of user owned devices to access the corporate network, "while only 9% were fully aware of what those devices were and what they were accessing" (Johnson & DeLaGrange, 2012). Half of Dell's customers that allowed user owned devices have suffered a security breach (Masons, 2013). Over 70 percent of 768 IT professionals surveyed in 2012 stated that mobile devices were a contributing factor to the increase in security incidents faced by their firm (Checkpoint, 2012). A brief review of BYOD models and a few security issues are discussed by Scarfo (Scarfo, 2012).

In this paper we begin with the benefits of user owned mobile devices to the organization. We then proceed to discuss the security and management challenges of managing UOMCDs. Based on our research of a large number of policies, we develop and present an integrated UOMCD policy that will address the security of a business network.

BENEFITS OF UOMCDs

UOMCDs offer low cost ubiquitous connectivity between employees, the enterprise, and its customers/partners. In addition the interface for mobile devices is richer than that available with corporate IT systems and more tuned to highly interactive transactions.

Ubiquitous Connectivity

One key factor driving increased use of UOMCDs is the continued improvement in performance to price ratios which has made high capability devices affordable for individual acquisition. When coupled with ubiquitous mobile connectivity, users have a great incentive to acquire and use these devices for personal and employment use. Ubiquitous connectivity can support virtual co-presence with remote employees and business partners which has been shown

to improve productivity (Subramaniam, Nandhakumar, & Baptista, 2013). It must be noted that the reduction in cost also facilitates business purchase of devices for all employees. However, the mixed use of these devices for both personal and work use poses a challenge for businesses, since the separation of costs for business and personal use will rapidly become a cost accounting nightmare (Digital Services Advisory Group and Federal CIOs Council, 2012). If the business enforces a strict business-use only policy on a mobile device, the user needs to carry multiple devices for personal and business use, and use the appropriate device in each situation; a major impediment to user convenience. Hence, allowing the user to use their own mobile computing device for business use offers flexibility to the user and 24 by 7 connectivity for the business.

Interface Richness & Employee Learning

While MCDs have less screen real estate than desktop devices, the user interface is typically enhanced with touch and voice interactivity, and custom designed applications (apps) to facilitate user interactivity on the small device (Nilsson, 2009). Vendors have promoted proprietary interfaces to enrich user experience on the devices, focusing on aesthetic integrity, direct manipulation, feedback and metaphors (Apple, 2012). Even open source systems have evolved multiple interface versions, each with their own idiosyncrasies. Users acquire skills in the interfaces through repeated use rather than formal training sessions, and often develop a high loyalty to a preferred mobile UI (UserCentric, 2011). They develop numerous short-cuts to perform common tasks and this enhances their productivity on the device when performing business tasks. When the business allows users to bring UOMCDs into the organization and use them for business tasks, it benefits by allowing them to maintain a high level of productivity on the device. Note that private use of the same device allows a rapid transfer of skills acquired in private use to the work domain. This does pose a problem for the information systems managers within the organization since they have to deal with a plethora of devices connecting to corporate applications. This issue will be dealt with in the next section.

One other issue to be considered when allowing UOMCDs is the significant learning that occurs within the enterprise when many employees have similar devices. There is a strong ecosystem effect (Lala, 2011), where users share learning experiences about a particular device and its interface, leading to enhanced productivity in the business. When the UOMCD policy has no device restriction, the vast array of devices and interfaces in use limit learning from a large ecosystem.

Connected Enterprise

The scientific management approach to work design is based on a detailed analysis on highly repetitive tasks to determine an optimal sequence of steps to complete the task. Line employees are trained to perform this task in the designed manner to achieve high productivity and standardized output. Changes in technology have reduced employment in such jobs, especially in the developed economies with high labor costs. Jobs today are much more diverse and require a variety of skills, with the driving need to react to contingencies effectively and adapt work to meet new requirements. MCDs have rich communications capabilities allowing

employees to rapidly search for and obtain necessary data, analyze the data quickly to determine the optimal response, and respond to the emerging needs of customers.

MCDs must not be used as add-ons, but must be well integrated with work process to support effectiveness and efficiency at work in the education (Ktoridou, Gregoriou, & Eteokleous, 2007), healthcare (Prgomet, Georgiou, & Westbrook, 2009), and other environments (ATT, 2012). Consider a situation where a customer wants to cancel an order since a competing service has made a low-bid offer. Online opinion sites could contain numerous customer complaints about the competitor, and a mobile device could be used on a 24 by 7 basis to instantly gather the data, organize it into a useful information and electronically deliver it to the customer, calling into question the value of the lower cost bid from a competitor with a highly unsatisfied clientele.

The organization becomes truly effective in the highly connected global marketplace only when its employees can rapidly retrieve, analyze and deliver information to users. They need to embed MCDs in the work process on a 24 by 7 basis, and ensure employee effectiveness. A good UOMCD policy should understand the value of these devices and focus on supporting these devices in the enterprise (Walton, 2012).

SECURITY CHALLENGES FROM UOMCDs

Bring your own Device (BYOD) policies result in a wide diversity of devices accessing the corporate network. Many of these devices are not designed for security and pose security threats. Simple controls can stop most breaches in security (ISACA, 2010). A more advanced approach using software named BYODroid, which can guarantee that devices running Android comply with the security policy of the organization has been presented (Armando, Costa, Merlo, & Verderame, 2012). The two major security issues for UOMCDs are data theft and malware intrusion into the corporate network. The diversity of user owned devices poses a management challenge for IT.

Data Theft

Mobile devices have become the new target for data theft (Yeaton, 2012). Data theft has become a serious issue due to the vast storage capability of devices. While a corporate database over a gigabyte in size was considered a large system, a couple of decades ago, storage on any portable device is many gigabytes today. Hence, it is possible to store an entire corporate database on a portable device. While UOMCDs are by their very nature connected to the global network at any time, users tend to download and carry far more data than they need on their devices due to a fear of not being able to access the data in the event of a loss of connectivity to the corporate database. This means that even the accidental loss of a MCD will result in significant data loss for the business. The damage from a deliberate, planned theft will be much worse. The loss can result in an adverse impact on business reputation, legal costs from losses of private customer data, and regulatory charges due to the failure to protect data secure by law such as healthcare related data.

One solution could be to limit the data stored on the device by designing applications that download only the absolute minimum of data needed for the task, encrypting the data stored locally and periodically cleaning out un-necessary data stored on the device. Data protection and encryption is a critical process according to 57% of the respondents in a major industry survey of BYOD policies (Johnson & DeLaGrange, 2012). Note that all these approaches require corporate IT to manage the device, thereby requiring the user to submit their MCD for corporate IT certification and inspection. An organization that possesses data that needs to be highly secure would limit UOMCDs and prefer to provide users with business owned devices that can tightly controlled and monitored. Obviously, this will typically be based on an approved architecture for the business and this approach will limit some of the benefits discussed earlier with UOMCDs. It is possible to build this security into a custom designed application for the UOMCD that enforces data access, storage and encryption limitations. In fact, one benefit of building security into the application, rather than the device, is that the security is extended to all machines, including business desktops and the workload on the IT team is limited since the individual devices need not be repeatedly inspected.

In addition, since UOMCDs are by definition, mobile, they are transported to insecure locations frequently, and this increases the threat vector faced by UOMCDs. Strategies to address these risks include device tracking where the device can be tracked and remotely wiped if necessary, enhancing user awareness of device security, and regulatory compliance (Figure 2, (ISACA, 2010)). (Johnson & DeLaGrange, 2012)

Malware Intrusion

The net has a serious problem with malware that in introduced into devices from browsing to compromised sites or downloading infected applications. A UOMCD is subject to constant attack. While the walled garden approach taken by some vendors has controlled malware within MCDs compared to rampant malware in the more open desktop environment, the problem of infections is serious and needs to be considered by corporate network security. The corporate network should not be configured as a closed, multi-walled, highly protected system, due to the increasing need for openness. As discussed in the scenario where an employee may need to rapidly gather customer opinions expressed on public networks and blogs for a quick and effective response, the system must permit users to go outside the business network and bring in data, analyze it and integrate the results with internal information. While preventing malware intrusion is a laudable goal, it has to be balanced with the need for openness. The business can enforce policies that require UOMCDS to meet security standards, have an updated app and browser to access the network, and have traffic monitored for security.

MANAGEMENT OF UOMCDs

Workload

Traffic Management: While the previous section focused on threats from UOMCDs, this section looks at the increased workload faced by corporate IT when having to manage the rush of

user owned devices. UOMCDs typically have a large number of apps that encourage user "playfulness", using the device for play rather than work. Many of these devices can switch seamlessly between corporate wifi and direct access to cellular service. In addition to the distraction from work, these apps spawn traffic that can load the corporate network. Many businesses limit traffic on their network through firewalls. However, new apps often bypass firewalls, necessitating work on continually fine tuning firewall rules to support legitimate traffic and stop unapproved traffic (Constantin, 2012). The direct consequence of load on the network due to an employee streaming a movie on a UOMCD at work is accompanied by the indirect cost of employee time spent watching a movie at work. Many younger employees work online seamlessly switching between work and play, and often work at home or remote locations round the clock. When the US EEOC offered employees the option to drop the department issued Blackberry in favor or UOMCDs, many younger employees were willing to pay for the data costs on their own rather than have the employer pick up the tab for an "older" device (Digital Services Advisory Group and Federal CIOs Council, 2012). While a complete ban on use of UOMCDs at work is possible only in organizations with a very controlled work environment, many businesses do not allow UOMCDs wifi access at work.

App Integration: UOMCDs may have customized apps that make a particular task very convenient, such as note taking, maintaining contacts or generating charts. Users typically would like to interface the app with their office systems, continually updating notes on a desktop and mobile device or synchronizing contacts between systems. Corporate IT needs to build the necessary integration into business systems. Even though many apps use evolving standards such as XML that are supposed to seamlessly transfer data between systems, a significant amount of work needs to be done to set up and maintain synchronization and data transfer between each app and the corporate IT system. In the absence of a standard MCD OS and app selection, the workload rises rapidly for corporate IT. When the need for data security is also considered, it becomes clear why many corporate IT departments would prefer to limit UOMCDs in the enterprise.

Setup Configurations: Finally, new MCD apps may have set-up configurations that use policies conflicting with corporate systems. When the first iPads were connected to corporate wireless networks, the configurations for IP addresses allocated to the device conflicted with corporate IP address allocation policies leading to added work for network managers. This can create errors in corporate networks ranging from resource allocation problems to security holes.

UOMCD POLICY

In the previous sections, we have considered the benefits of allowing employees to bring their own mobile computing devices to work and the management problems that arise from the devices. In this section, we will discuss a suitable policy to manage the devices. The policy should include appropriate limits on allowed devices, data security policies, and user education to keep the corporate system safe and effective. The policies presented in this paper are based on a review of user owned device policies at many organizations posted on their corporate websites and trade journal reports of BYOD policies (Appendix I).

Device Registration Policy

Device registration helps set better access controls to the corporate network and data. For example, requiring the register the device MAC address helps set up MAC address restrictions on network activity. In addition, corporate IT can scan the device for viruses and necessary security updates during the registration process. In some cases device registration is coupled with software installation that can create a secure mobile execution environment (James & Griffiths, 2012). In the absence of registration, users may bring in other devices owned by family members or friends and connect to the corporate network. A formal registration process limits such access from insecure devices. Registration imposes a cost on the IT department, which has to certify and include the device in a list of approved devices, and manage the access list over time as old devices are retired from the list and new devices are added to the list. IT departments facing time constraints may delay the registration process leading to frustrated users who face a long wait before getting to use their newly acquired, leading edge, devices on the network.

Device Data Policy

Business data delivered to and stored on a user owned mobile computing device needs to encrypted, not just during transmission over the public network, but must also be maintained in a secure manner on the device. The storage capacity of mobile computing devices has grown faster than computing capability growth predicted by Moore's Law and users can download vast amounts of data to their device. It is difficult for CIO's to strictly enforce restrictive data download policies on savvy users. There are three ways to secure this data on mobile devices.

The first is to provide good encryption applications on these devices that keep the data secure when it is not being actively used. This approach forces the user to keep business data in a secure lock-box, with a transparent decryption process that quickly pulls up the data in a usable format for analysis. After it is used, the data is placed back in a secure lock-box and unencrypted data is deleted from the device. The entire security process should operate quickly and seamlessly. This reduces the opportunity for data theft from stolen user owned devices. The computational load of encryption/decryption is worthwhile when data security is paramount, for example in the case of medical data that needs to be protected for patient privacy. Regulations such as HIPAA mandate the use of good security for medical records.

The second option is to maintain corporate data in the cloud and provide cloud based analysis applications that only deliver results and not raw data to user owned devices. This requires corporate IT to acquire and/or develop the necessary cloud based mobile applications. If the business already has a dispersed workforce (multiple locations and home offices), corporate-managed secure cloud storage is a necessity, and this can be easily extended to UOMCDs. Corporate managed secure cloud storage also reduces the need for employees to place data in unencrypted flash drives that pose a serious security threat. Since even the output from these apps could contain valuable proprietary information, security is still necessary for any

information stored on the mobile device, due to the high propensity for device loss. Many businesses enforce a device cleaning process prior to corporate use to ensure system security followed by periodic updates to meet security requirements. In addition, most install a remote wipe application that supports quickly erasing all sensitive data from the device in event of a loss notification.

A third option is to make the access context sensitive; i.e. recognize the physical location of the device and environmental parameters and limit the data delivered to the device (Carter, 2012), (Feth & Jung, 2012). An example would where the geospatial location of the device is first determined before data delivery. The payroll file will be delivered to a home office but not to a bar.

Another issue that needs to be considered is the user's private data stored on the device. Security is often implemented on UOMCDs by corporate security apps that are installed on the device to limit access, encrypt data, and clean out risky applications. This often provides corporate IT with the ability to "clean wipe" device storage and to look into anything stored on the device. In turn, this can provide corporate IT the ability to look at personal information stored on UOMCDs. This is often overlooked, and data privacy legislation breaches may occur if the IT employees were to open private files (Ovum, 2012). The study (Ovum, 2012) reviews cases at organizations around the world including Volkswagen in Germany, Leeds City Council, UK., Unisys in the U.S., and SAP in Australia. A well-defined user data privacy policy on UOMCDs needs to be laid out and enforced to ethically protect corporate resources while preventing eavesdropping on user data stored on the device by IT and mid-level managers (Gotterbarn, 2012).

Network Security Policy

UOMCDs have the potential to weaken the security of the corporate network. Security is only as strong as the weakest link. A single UOMCD with an unpatched system, lacking anti-virus and malicious code protection, or having a compromised application can wreak havoc when permitted within a corporate network. The device registration policy discussed earlier should include requirements for up-to-date security patches, accepted anti-virus and malicious code protection applications, and be clean of applications that could compromise the IT system.

While verifying the device at registration is a good beginning, users typically fail to maintain the device to meet security standards. In the case of security updates, the IT department could monitor the systems on all allowed devices and force updates whenever a new path is released. This adds to the management burden, since UOMCDs that are not patched within a reasonable time need to be disapproved for system connections. In addition to updates for the OS, there are many other applications on the device that need to be updated for security. this includes popular apps like Adobe Reader, Flash, and Java. The problem of applications that can compromise security is far more challenging. Since these applications are installed by the user's deliberate actions, they typically bypass the security offered by anti-virus programs.

If the business restricts UOMCDs to a pre-approved list of devices, and applications, such as devices running an approved version of an operating system and using approved media drivers and browsers, it is possible to remotely update all connected devices whenever a patch is released. This is the reason some enterprises limited users to only laptops running the Windows OS, tablets to only iPads, or phones to Blackberry's. Administrative costs are reduced and the management process becomes more reliable since IT can be well trained on a limited number of systems. Note that some operating systems allow network security to active monitor the device and ensure security levels on the device and others are less amenable to control. Hardware restrictions are becoming more difficult due to the proliferation of UOMCDs in the marketplace and users may not be happy with such restrictions imposed on hardware. In addition, the highly dynamic environment means that the business may select a standard that rapidly becomes outdated, leading to significant frustration among employees.

Highly security conscious firms make the IT department the system administrator on the user's machine and prevent any application installation without IT approval. This defeats one of the main aims of users in acquiring UOMCDs, which is to install all their preferred apps, at their convenience. Hence, such a restrictive policy will not be acceptable to most users. A tradeoff is to screen the device initially, and follow up with a good user training policy discussed in the next section. In addition, corporate IT needs to monitor traffic from UOMCDs much more closely to identify suspicious traffic.

VPN use: Virtual private networks establish a secure, managed private tunnel between the UOMCD and corporate IT centers. VPN's are typically implemented on UOMCDs by installing a VPN client application on the device and having it connect over the public network with a VPN gateway, that in turn connects to the corporate network. VPNs offer a transparent security where the user does not need to run through hoops to establish a secure connection. VPNs support a secure cloud-computing environment where corporate data is placed in a well-managed cloud hosted data center, and is accessed from remote locations and even the business office. UOMCDs follow the same policies as machines in the business office since all devices connect to a hosting site over VPNs. Implementing VPNs has become easier with many providers offering turnkey solutions (Cisco, 2012).

Network DMZ :UOMCDs create a porous perimeter, opening up the firewalled, secure internal network to attack from compromised diverse devices. One solution is to UOMCDs is to put these mobile devices on a segment of the network that is separate from the main corporate LAN. This network could be located outside the firewall in a DMZ of sorts. This is not necessarily the best option however as employees may not be able to access the information they need, thus defeating the purpose of them bringing the device to work in the first place. One way around this is to use a device fingerprinting approach that authenticates the user (user ID/password) and the device (IT managed workstation or UOMCD) when a user logs into the corporate domain. Network security policy for example could permit a user on a corporate PC to download HR data but restrict it for the same user on an iPhone (Aruba Networks, 2011).

User Training Policy

A suitable user training policy needs to be developed and implemented when UOMCDs are permitted within the corporate system. This user training policy should include user understanding of threat scenarios, the need to separate work and personal data, and a well-designed file sharing policy. A study of 768 IT professionals showed that a lack of employee awareness has the greatest impact on the security of mobile data (Checkpoint, 2012). Another study of 1500 respondents fro 14 countries conducted by McAfee and Carnegie Mellon University found that less than one in three employees are very aware of their company's mobile security policy while 95% of the organizations had a policy in place (Power, 2012)

UOMCDs contain corporate data and access capability, and are carried into insecure environments by users. Thieves understand that UOMCDs possess far more than their intrinsic value, due to the valuable data stored and accessible through the device. While the theft of the device may be purely opportunistic, it may later morph into a targeted attack that holds the device and its data to ransom. In addition there are targeted attacks on the corporate network though the weak link in security presented by UOMCDs that traverse open, unsecure networks and the secure corporate system (Dhanjani, Rios, & Hardin, 2009). Users must be educated on threats to the physical device and to data on the device. In addition, they need to understand how virus and phishing attacks are carried out. Malicious software can be downloaded to the device from compromise websites and Trojan horse files that purport to contain a favorite video or music but contain an embedded, hidden, program that compromises security. The hidden program may be logging user keystrokes to capture passwords or sending copies of secure files to hacker controlled sites.

A second issue that needs to be dealt with in user training for UOMCDs is the need to separate personal and work spaces on these devices. Common problems encountered by users include sending personal email to work partners or releasing work data to their personal contact list. Earlier we discussed the need for corporate policy that restricts snooping on personal assets retained on the device by users. The training should extend to users to ensure that they also maintain the separation between work and play on their devices. Policies and training need to be coupled with tools like Software as a Service (SaaS) mobile applications management solutions that create a sandbox like virtual workspace can be used to separate work and play (F5, 2013).

The third issue is a file transfer policy. Many employees use services such as Dropbox, iCloud, SugarSync, and Boxnet that allow employees to easily lease space to store corporate and personal files that can be accessed by devices, especially tablets that often do not have a USB port for flash drives. This causes company data to be placed not just on an employee's BYOD device, but also on the public cloud. The BYOD policy must include user training to understand the security implications of storing corporate data on public clouds and on flash drives without encryption.

The fourth issue is a file sharing policy. Many users load popular torrent software to download media files and share them with friends. While this may be common practice on personal devices, it is definitely not acceptable on corporate devices. Users may feel this policy infringes on their rights to their own devices. However, the business can be liable for copyright

violations if traffic from sites such as BitTorrent and Limewire traverses the corporate network. User training should highlight the legal and ethical implications of using these programs to dissuade users, and this network security policy should limit access to such programs and related sites to actively stop use of these sites. The policy may include denial of network connectivity to users who run these applications on the corporate network.

SUMMARY

The trend labeled "consumerization", the infusion of technology in the work place driven by users rather than corporate IT has brought significant challenges to IT security. In particular, we look at the impact of user owned mobile computing devices (smartphones, tablets, and future devices like Google Glass) on security in the corporate network. While surveys have shown that most companies have a BYOD policy in place, only a small percentage of the employees are actually aware of these policies. This creates a security hole in corporate network security. In addition to policy features, a strong user training policy needs to be developed and implemented to ensure the continued security of the network.

REFERENCES

Accenture. (2010). *Jumping the boundaries of corporate IT Millennial Generation is rocking the foundation of IT.* Retrieved 4 27, 2013, from accenture.com: http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture_Millennials_Video_Transcript.pdf

Apple. (2012, 12 17). *ioS Human Interface Guidelines.* Retrieved 2 15, 2013, from developer.apple.com: http://developer.apple.com/library/ios/documentation/userexperience/conceptual/mobilehig/MobileHIG.pdf

Aruba Networks. (2011). *Bring Your Own iPad to Work.* Retrieved October 16, 2012, from http://www.arubanetworks.com/pdf/technology/whitepapers/WP_Bring-Your-Own-iPad-to-Work.pdf

Armando, A., Costa, G., Merlo, A., & Verderame, L. (2012). Securing the "Bring Your Own Device" Policy. *Journal of Internet Services and Information Security , 2* (3/4), 3-17.

ATT. (2012). *Mobile Applications: Develop Mobile Apps to Transform the Way You Work.* Retrieved 2 26, 2013, from business.att.com: http://www.business.att.com/enterprise/Family/mobility-services/mobile-applications/

Burt, J. (2011, 9 5). BYOD Trend Pressures Corporate Networks. *eWeek News , 4*(15).

Carter, J. (2012). *Context-Based Mobile Security Enclave.* Naval Post Graduate School.

CISCO. (2012). *CISCO BYOD Smart Solution.* Retrieved 2 15, 2013, from cisco.com: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5712/ps11640/at_a_glance_c45-692412.pdf

Cisco. (2012). *Cisco Mobile VPN - Increase Mobile Worker Productivity*. Retrieved 2 15, 2013, from cisco.com: http://www.cisco.com/en/US/products/ps6744/products_ios_protocol_group_home.html

Checkpoint. (2012, 1). *The Impact of Mobile Devices on Information Security: A Survey of IT Professionals.* Retrieved 2 15, 2013, from checkpoint.com: http://www.checkpoint.com/downloads/products/check-point-mobile-security-survey-report.pdf

Constantin, L. (2012, 7 25). *New tool gives 150 ways to bypass web app firewalls.* Retrieved 4 27, 2013, from computerworld.com: http://www.computerworld.com/s/article/9229659/New_tool_gives_150_ways_to_bypass_web_app_firewalls

Digital Services Advisory Group and Federal CIOs Council. (2012, 8 23). *Bring Your Own Device A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs*. Retrieved 2 15, 2013, from Digital Government: http://www.whitehouse.gov/digitalgov/bring-your-own-device

Dhanjani, N., Rios, B., & Hardin, B. (2009). *Hacking: The Next Generation.* Sebastopol, CA, USA: O'Reilly

F5. (2013, 2 15). *Mobile App Manager*. Retrieved 2 15, 2013, from f5.com: http://www.f5.com/products/mobile-app-manager/overview/

Feth, D., & Jung, C. (2012). Context-Aware, Data-Driven Policy Enforcement for Smart Mobile Devices in Business Environments. In A. U. Schmidt (Ed.), *MOBISEC 2012*, (pp. 69-80).

Gotterbarn, D. (2012). Corporate Social Media Use Policy: Meeting Business and Ethical Responsibilities. *HCC10* (pp. 387-398). IFIP.

ISACA. (2010). *Securing Mobile Devices.* Retrieved 02 15, 2013, from Isaca.org: http://www.isaca.org/Knowledge-Center/Research/Documents/SecureMobileDevices-Wht-Paper-20July2010-Research.pdf

James, P., & Griffiths, D. (2012). The Mobile Execution Environment: A Secure and Non-Intrusive Approach to Implement a Bring You Own Device Policy for Laptops. *Proceedings of the 10th Australian Information Security Management Conference.* Perth: SRI Security Research Institute.

Johnson, K., & DeLaGrange, T. (2012, 10). *SANS Survey on Mobility/BYOD Security Policies and Practices.* Retrieved 2 15, 2013, from sans.org: http://www.sans.org/reading_room/analysts_program/SANS-survey-mobility.pdf

Ktoridou, D., Gregoriou, G., & Eteokleous, N. (2007, Sept.). iability of Mobile Devices Integration in Higher Education: Faculty Perceptions and Perspective. *Next Generation Mobile Applications, Services and Technologies, 2007. NGMAST '07. The 2007 International Conference on* , 12-14.

LaBarre, O. (2012, 4 24). *Banks May Not Be Able to Resist 'Bring Your Own Device'*. Retrieved 2 26, 2013, from Bank Systems and Technology: http://www.banktech.com/management-strategies/banks-may-not-be-able-to-resist-bring-yo/232900559

Lala, W. (2011, 10 14). *Its all about the ecosystem. Not the device*. Retrieved 2 15, 2013, from onlineeconomy.org: http://www.onlineeconomy.org/its-all-about-the-ecosystem-not-the-device

Nilsson, E. (2009). Design Patterns for User Interface for Mobile Applications. In V. Jaquero, F. Simarro, J. Masso, & J. Vanderdonckt (Eds.), *Computer-Sided Design of User Interfaces* (pp. 307-312).

Masons, P. (2013, 3 20). *BYOD Policies*. Retrieved 3 27, 2013, from out-law.com: http://www.out-law.com/en/articles/2013/march/half-of-firms-with-byod-policies-have-suffered-a-security-breach-dell-claims/

Ovum. (2012, 5 17). *International Data Privacy Legislation Review: A Guide for BYOD Policies* . Retrieved 4 15, 2013, from ndm.net: http://www.ndm.net/mobile/pdf/resources/1209-International_Data_Privacy_Legislation_Review-A_Guide_for_BYOD_Policies.pdf

Power, R. (2012). *Mobility and Security.* Retrieved 2 15, 2013, from mcafee.com: http://www.mcafee.com/us/resources/reports/rp-cylab-mobile-security.pdf

Prgomet, M., Georgiou, A., & Westbrook, J. (2009). The Impact of Mobile Handheld Technology on Hospital Physicians' Work Practices and Patient Care: A Systematic Review. *J Am Med Inform Assoc , 16* (6), 792-801.

Scarfo, A. (2012). New Security Perspectives around BYOD. *Broadband, Wireless Computing, Communication and Applications (BWCCA), 2012 Seventh International Conference on*, (p. 446=451).

Schulze-Warnecke, M., & Hartman, L. (2012, 8 12). *Juniper Press Releases*. Retrieved 2 15, 2013, from juniper.net: http://www.juniper.net/au/en/company/press-center/press-releases/2012/pr_2012_08_17-11_00.html

UserCentric. (2011, 6 15). *Best Practices for Designing Mobile Touch Screen Applications*. Retrieved 2 15, 2013, from usercentric.com: http://www.usercentric.com/news/2011/06/15/best-practices-designing-mobile-touch-screen-applications

Walton, D. (2012, Septemer 6). *Bring Your Own Device' to Work Carries Data Security Risks*. Retrieved October 16, 2012, from Law.com: http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202570405609&Bring_Your_Own_Device_to_Work_Carries_Data_Security_Risks_&slreturn=20121010145525

Yeaton, M. (2012, 5 7). *Mobile devices:the new target for data theft*. Retrieved 2 15, 2013, from mit.edu: http://web.mit.edu/newsoffice/2012/mobile-devices-data-theft.html

APPENDIX I: WEBSITES WITH BYOD POLICIES AND CASE STUDIES

Mastercard, http://www.cio.com/article/706456/A_Secure_BYOD_Policy_at_MasterCard_Priceless.

User Access Agreements for many schools, Intel, http://engage.intel.com/thread/11545

Janco http://blog.e-janco.com/2013/02/14/byod-policy-template-release/

Federal Agencies http://fcw.com/articles/2012/04/04/fose-byod-mobile.aspx

County Governments http://www.statetechmagazine.com/article/2012/04/counties-forge-byod-policies

Eastman Chemical http://content.maas360.com/www/content/cs/cs_maas360_mdm_EastmanChem.pdf

Frederick Mutual http://content.maas360.com/www/content/cs/cs_maas360_mdm_FrederickMutual.pdf

Conan Foods http://content.maas360.com/www/content/cs/cs_maas360_mdm_conan.pdf

Judson School District http://www.judsonisd.org/district/technology/BYOD.cfm

Telesoft http://www.telesoft.com/sites/default/files/pdfs/whitepapers/Telesoft_whitepaper_mobilepolicy.pdf

PriceWaterhouseCoopers http://www.pwc.com/en_US/us/increasing-it-effectiveness/assets/byod-1-25-2012.pdf

IBM http://www.infoworld.com/d/consumerization-of-it/how-ibm-manages-80000-bring-your-own-devices-189504

Citrix http://www.citrix.com/site/resources/dynamic/additional/byod_best_practices.pdf

Villanova Certificate Program in BYOD http://www.villanovau.com/byod-bring-your-own-device/

Fujitsu http://globalsp.ts.fujitsu.com/dmsp/Publications/public/wp-byod.pdf

TrendMicro http://www.trendmicro.co.uk/media/ds/mobile-security-datasheet-en.pdf

IBM – Cases at other companies http://www-07.ibm.com/smb/in/services/industry_special/hd/images/CIW03077USEN.pdf

Blue Coat http://www.bitpipe.com/detail/RES/1363265570_71.html

Broadcom http://blog.broadcom.com/network-infrastructure/broadcom-takes-on-byod-it-starts-in-the-network/

Juniper http://www.juniper.net/us/en/local/pdf/whitepapers/2000363-en.pdf

BYOD.us http://byod.us/create-security-policy/

Symantec http://www.emea.symantec.com/web/BYODPolicy/

Clareity https://www.realtown.com/mattcohen/blog/info-security-policy-byod

Zenprise http://i.dell.com/sites/doccontent/business/smb/sb360/en/Documents/wp-mobility-zen-byod-policy.pdf

Ford http://www.computerworlduk.com/news/mobile-wireless/3364129/ford-deploys-byod-mobile-security/?intcmp=rel_articles;mbl-wrlss;link_2

NIST http://csrc.nist.gov/publications/drafts/800-124r1/draft_sp800-124-rev1.pdf

Microstrategy http://www.computerworlduk.com/in-depth/it-business/3375103/microstrategy-ceo-michael-saylor-and-implications-of-the-mobile-wave/?intcmp=in_article;related

Intel http://www.computerworlduk.com/news/it-business/3372818/intel-employees-prefer-to-choose-their-own-devices/?intcmp=in_article;related

Network Equipment http://networkequipment.net/2012/08/31/integrating-byod-into-the-workplace/

Apple http://searchconsumerization.techtarget.com/guides/Securing-data-in-the-mobile-era-An-Apple-and-Android-security-guide