Journal of Forensic & Investigative Accounting
Volume 8: Issue 1, January–June, 2016

Countering Mobile Device Threats:
A Mobile Device Security Model

Grover S. Kearns[*]

Introduction

The use of mobile devices in business is increasing as employees use them for communications, creating and editing documents, storage and retrieval of data files, and browsing the Internet. In 2013, mobile device purchases exceeded personal computers (Murtagh, 2014). While mobile increases worker agility and allows them to work remotely the pervasiveness and evolution of these devices creates a special threat because policies and controls for computers are not sufficiently broad to cover the new threats these devices pose.

While mobile devices have made it easier for hackers to exploit systems and increased the possibility of compromising sensitive files, most organizations have failed to address these security issues through formal policies or create specific controls to reduce their likelihood.

A single data breach can cost an organization extensive loss in profits and reputation. The Target Corporation data breach is a current and notable example, not only because of the dollar loss and adverse publicity, but the amount of time before analysts could determine the nature of the attack (LA Times, 2014). As hackers engineer increasingly sophisticated attacks organizations must increase their vigilance. Because mobile devices present new vulnerabilities and wireless is eclipsing the traditional wired environment, it is necessary to formulate policies and controls to address these threats.

Failure to protect personally identifiable information (PII) may subject the organization to fines and other penalties. Federal regulations such as the Gramm-Leach-Bliley Act and the Health Insurance Portability Act stipulate that financial and health organizations are accountable for the safe guarding of PII (Pearson, 2008) and global firms may be subject to the European Union Data Protection Directive which places stringent rules on the protection of private information (Tran and Atkinson, 2002).

The importance of IT security is recognized by professional organizations like the AICPA that has listed Securing the IT Environment, Managing IT Risks, and Leveraging Emerging Technologies in the Top 10 Technology Initiatives for 2013 (AICPA, 2013). Today, securing organizational data and protecting PII is not possible unless mobile devices are secured.

The purpose of this article is to argue the importance of enhanced mobile device policies and controls, suggest specific policies and controls, and present a mobile device security model.

Mobile Devices in Organizations

Mobile devices are becoming ubiquitous within the organization and can deliver tremendous business value by creating efficiencies, reducing cycle times, and improving communication channels. Companies reporting on mobile device benefits cite increased employee responsiveness, improved worker productivity, improved customer relations, and satisfaction, and reduced inventory and maintenance costs. These same companies express concerns about network security and data breaches resulting from mobile

[*] The author is Professor of Accounting at the University of South Florida.

device vulnerability (Forrester, 2012B). Table 1 lists some of the most popular uses of mobile devices (Murtagh, 2014).

Security concerns about the expanding use of mobile devices are warranted. While physical or wired networks can rely upon multiple lines of defense that have been proven over time, attacks on wireless networks and mobile devices can compromise an organization's system in ways that bypass traditional network security. Existing controls such as firewalls, intrusion detection systems, and proxy servers are also effective for mobile security but are not sufficient and may not address employee misuse, new malware, theft, and compromise resulting from lax security.

The Stuxnet virus, for example, was transmitted by a simple USB and infected a large number of highly secured computer systems. Although loaded onto numerous computers, the virus was written to attack a single target—an Iranian nuclear enrichment facility—and was successful.

Table 1: Popular Uses of Mobile Devices in the Workplace

▪ Phone calls	▪ File storage	▪ Productivity apps
▪ Texting	▪ File transfer	▪ Collaboration tools
▪ Calendars	▪ Audio / music	▪ Cloud access
▪ Email	▪ Video	▪ Social media
▪ Meeting notes	▪ Photos	▪ Access content
▪ File editing	▪ Presentations	▪ Games

Another threat posed by mobile devices is the emerging practice of "bring your own device" (BYOD) that reflects an increased reliance on devices other than desktop computers for e-mail and productivity software. Phones and tablets are chief among these and Forrester (2012A) reports eighty-two percent of workers use smart phones and thirty-six percent use tablets to view documents, spreadsheets, and presentations. Certain applications are more specific to a device. For example, tablets are more likely to be used in video conferencing, data analytics, and the editing of documents. Employees frequently bring multiple mobile devices into the workplace and the majority of organizations lack any formal policies to insure data protection against threats created by this practice (McAfee, 2012). Other devices continue to evolve that could present new threats (for example, the Apple watch). Furthermore, the number and types of applications have exploded. A survey by Forrester Research (2012A) shows that the BYOD trend will continue and employees will bring multi-functional smart phones, tablets and other devices into the workplace plus a plethora of applications that may or not be necessary for work-related activities.

Removable devices such as USBs currently have capacities well exceeding ten gigabytes: more than enough to store copies of sensitive and proprietary information. It is common practice for employees to carry corporate data files between home and work. These files may end up on home computers in an unprotected environment creating a potential compromise of sensitive data.

Security Threats from Mobile Devices

A 2012 survey by the SANS Institute reported that sixty-one percent of respondent organizations allow employees to use personal mobile devices to access organizational resources (SANS, 2012). In the same year, a Tenable Network Survey revealed mobile device vulnerability to be the top concern for security professionals. Moreover, the majority of organizations in the survey could not identify mobile device based network vulnerabilities and either lack specific mobile device policies or employees simply ignore them. Many (forty-two percent) identified data leakage as the chief concern when a mobile device was hacked, lost, or stolen (Tenable-Security, 2012).

If policies and controls are lacking then the growing use of mobile device creates new opportunities for hackers to exploit a range of vulnerabilities including infection of corporate servers. Table 2 lists common mobile device threats and vulnerabilities. Some parallel those for corporate computers but mobile device security requires specific controls that frequently differ from those for servers and desktop computers. These threats can be categorized as emanating from the mobile device, the applications, the platforms, and the users.

Table 2: Threats to Mobile Device

▪ Theft of device	▪ Phone hijacking
▪ Virus infection	▪ Impersonation
▪ Data leakage	▪ Message contamination
▪ Modification or destruction of data files	▪ Jail unlocking
▪ Continuously send SMS or MMS messages	▪ Denial of service

Mobile Device Theft

The mobile device environment is vulnerable to passive and active attacks due to features such as an open medium, dynamic network topology, and lack of centralized management (Zhang, Lee, and Yuang, 2003). In one survey of computer security professionals, forty-two percent cited theft of laptops and other mobile devices as a top IT threat (Richardson, 2008). The loss of the mobile device itself, however, is small compared to the value of its contents.

Malware and Viruses

Mobile device viruses create a range of threats. These viruses take many shapes and may be fairly benign or highly malicious. Some malwares cause the device to send out large numbers of unsolicited text messages and run down the mobile device battery rendering the device unusable. The more dangerous malwares can modify, copy, or delete valuable files and potentially infect corporate servers. Malicious programs such as Cabir, Duts, Skulls, and DroidKungFu were specifically written to attack mobile phones and computers and can propagate to other devices and allow files to be stolen.

Application Risk

Applications on mobile devices can add value to the organization. Many organizations use special applications on phones that provide tremendous organizational benefits. For example, universities use scheduling software on an Android platform so that bus drivers are informed in real-time of any scheduling changes, bottlenecks, accidents, or special needs requests. This provides a great value to the students and faculty at a nominal cost. However, untested applications have been found to contain malware. In the absence of policy restrictions, employees might add games and other personal applications to corporate mobile devices. Free apps that could contain malware can harbor code that allows hackers access to address books, calendars, photos and even corporate servers (Hoffman, 2013).

Platform Risk

Threats associated with mobile devices may depend upon the operating system or platform. A good example is the Android platform versus the iPhone or Blackberry platforms. While Blackberry is recognized as having the safest operating system, it is losing market share to both iPhone and Android platforms. However, Android malware attacks exceed those for iPhone and represent the highest vulnerability (Patten and Harris, 2013). Because Android is an open source platform the programming code, with some restrictions, is made public which allows for faster creation of applications. The vetting process for Android applications is not nearly as extensive or restrictive as those Apple imposes

(Greenberg, 2012) leading experts to estimate that ninety-nine percent of mobile malware attacks are targeted at Android platforms (Apple Insider, 2014; Swamy, 2014). Compounding this problem is the fact that many employee-owned mobile devices run on outdated operating systems that are highly vulnerable to attacks and, while the organization can control the updates to its own devices, employees might bring in personal devices that are not secure (Mansfield-Devine, 2012).

Various platforms are available for mobile devices the most popular being iOS and Android. HTML 5, Tizen, Blackberry, and Firefox are also used and others are gaining popularity. Different platforms pose different risks. However, some applications may only run on a specific platform. Certain business applications that are highly productive may demand a specific device and platform. IT specialists should determine what platforms are allowable and assess the risk of each.

User Risk

In a lax corporate atmosphere, employees might install organizational data on personal mobile devices in order to work on the files remotely even when this violates policy. Employees who take their mobile devices home may risk introducing viruses or compromising organizational data integrity through the negligence of other family members. In addition, many companies allow important vendors and customers to remotely access corporate files to support supply-chain management. Vendors who do not enforce acceptable security rules may allow hackers entry into the corporate system. This was how hackers were able to access the Target Corporation files (LA Times, 2014).

When users dispose of mobile devices, they may not erase sensitive corporate information (Glisson, Storer, Mayal, Moug, and Grispos, 2011). Employees may assume that deleted files are no longer accessible when in fact recovery of deleted files is usually easy to accomplish. It is essential that policy require corporate data be erased (or wiped) before devices are retired.

It is also essential that employees do not use mobile devices in a manner that could introduce errors or viruses. Mobile devices are subject to viruses that can infect corporate computers as well as other mobile devices. Mobile phones and PDAs, for example, are targeted by over 350 different viruses and malwares and the number is growing rapidly (Shih, Lin, Chiang, and Shih, 2007). Updating these devices with current anti-virus software is more difficult than updating wired corporate computers that can be updated daily via the network.

Employees may increase vulnerability by altering personal mobile devices. Jailbreaking a mobile phone will allow the installation of any application or modified operating system. This poses a significant threat from personal smart phones that enter the workplace. Organizations should consider a ban on all smart phones that have been jailbroken and insure this does not happen to any corporate smart phones.

Because they operate in a wireless environment, mobile devices are more vulnerable to eavesdropping if security features are not enabled. Wireless also makes updating employee's personal mobile devices more difficult because of lack of availability and a multitude of operating platforms. An efficient approach to managing software installations on mobile devices is the use of mobile device management (discussed below).

Addressing Mobile Device Threats

Identification of Threats and Vulnerabilities

Tantamount to the creation of policies is the identification of business and technical threats to mobile devices or threats that are posed by mobile devices. This includes theft of devices, which not only represents loss of the device but the unauthorized access to information resources. Seemingly benign devices can be dangerous. Data on most USBs, for example, is not encrypted. Sensitive data on a lost USB could represent a costly exposure. A survey by Sandisk (Sandisk, 2008) revealed that corporate employees most frequently copy customer data, financial information, business plans, employee data, marketing plans, intellectual property, and source code. This data may be necessary for job

responsibilities but this includes PII, intellectual property and other sensitive information. Data breaches are costly resulting in loss of market share, reputation and possible lawsuits and regulatory sanctions.

Vulnerabilities can also be specific to operating systems (such as Android), to security settings that employees do not enable on their personal devices, to specific applications (such as personal games and applications), and to usage as when employees download data from untrusted sites. An effective security plan must address all of these possibilities.

Assessment of Threats and Vulnerabilities

A risk management approach assesses the likelihood and potential loss for each type of threat in order that policies and controls are appropriate for the perceived level of exposure. Security analysts may wish to categorize mobile device risks by devices, applications, and platforms. This assists in determining appropriate implementation of policies and controls and assures that higher risks will be identified and addressed. Threat assessments are based upon available information from surveys, the experience of similar companies, risk-management reports, and management decisions as to how usage of mobile devices will develop within the organization. Both internal auditors and IT specialists should play a role in the identification and assessment of threats.

Education

To be effective, employees must be educated to understand the policies and controls and the consequences of ignoring or overriding the controls. Employees who understand the reason and importance of policies and controls are more likely to respect and adhere to them. User awareness training should be pervasive as most employees can be expected to bring personal mobile devices onto the corporate premises. As organizations become more dependent on mobile devices and employ a BYOD policy the imperative to secure these devices increases.

Employee awareness of mobile device security policies and related controls is essential to a successful security program. Controls are not effective unless employees appreciate and understand the importance of controls and the consequences of ignoring or overriding the controls. It may be necessary for employees to sign an agreement to allow security officers to randomly search personal mobile devices that are brought on site. Training should also extend to the transport of information outside of the organization. Sensitive files that may not be copied or removed from the workplace should be identified.

Even supposedly computer-savvy employees can harbor erroneous assumptions about mobile device security. Many workers believe, for example, that viruses do not infect mobile phones or that they must open and run an executable file for it to be dangerous. However, smart phones are vulnerable to hundreds of viruses and some operating systems possess an autorun feature that automatically executes a file (Shih et al., 2007). Users who install games on their mobile devices, especially freeware, run the risk of embedding malicious code that executes whenever the game is played. Bluetooth also represents an avenue for hackers to exploit applications and access data on mobile devices. BlueSnarfing and BlueBugging are examples of attacks to obtain personal data, address books, calendars, applications, and data files (Koong, Liu, Bai, and Lin, 2008). Hardening requires that employees disable the Bluetooth feature when not in use and turn off the autorun feature.

Employees should be trained to recognize attacks and notify security personnel immediately when they suspect that a mobile device has been infected or compromised. Education and correcting misunderstandings will help to insure employees adopt secure practices.

Mobile Device Security Audits

Periodically, a mobile device security audit should be undertaken either by the internal audit department or by an external firm. If the internal audit function lacks IT capability then an outside firm can be selected. Although the internal IT department may assist in the audit tasks, the audit function cannot be relegated to the IT function. The mobile device security audit may be performed as a part of a larger IT

audit. However, the tasks may be different and it is essential that the audit carefully consider the controls specific to mobile device security and that the mobile device security audit not be subjugated to a larger process.

Audit findings should be carefully reviewed, summarized, and presented to management with recommendations for addressing perceived weaknesses in controls and instances of users ignoring the controls (Davis et al., 2011).

Addressing Mobile Device Security Threats

Auditors and IT managers are usually familiar with governance frameworks such as COSO (Committee of Sponsoring Organizations) and COBIT that serve to address both physical and logical threats. Most organizations have already implemented controls proposed by one or both of these models. Controls for mobile devices can be created by extending the controls in those frameworks. Identification of endpoints on the network, for example, can be accomplished by using network access control software. Virtual private network (VPN) tunnels can prevent eavesdropping and man-in-the-middle attacks.

Table 3: Recommended Mobile Device Security Controls

- Inventory organizational mobile devices and applications
- Identify personal and rogue mobile devices and applications
- Keep software and operating systems up-to-date
- Disable autorun features
- Disable Bluetooth when not in use
- Restrict copying of corporate data to USB and other mobile devices
- Implement access control management
- Insure all users are authenticated
- Install firewalls at important perimeters
- Maintain anti-virus software on all mobile devices
- Practice sound patch management
- Use mobile device management on all corporate mobile devices
- Remote access to corporate data uses virtual private network (VPN)
- Remote access to corporate data uses network access control (NAC)
- All smart phones should be enabled for remote wiping of data
  Security identifies mobile devices not qualified to be used with corporate data (these would include jailbroken devices, devices with outdated operating systems, or devices harboring unknown apps)

Some existing IT controls are applicable to mobile devices. However, mobile devices create a different set of threats that require additional or special controls. Many organizations, however, have not taken measures to identify or respond to those threats (Tenable-Security, 2012). Table 3 is a representative list of recommended mobile device access security controls.

Policies for Mobile Device Security

Organizational control begins at the policy level. Although many organizations report adoption of separate security policies for mobile devices, recent surveys show that most firms have not implemented specific policies or controls for mobile devices (Tenable-Security, 2012). Security controls are necessary to control levels of access to systems and establish proper authentication and authorizations. They should control what devices and applications can be used. Without specific policies IT administrators may not be able to configure security settings properly.

Mobile device security policies should be founded upon identified threats and assessed risks. This allows management to implement policies that address the specific threats in a cost-beneficial manner.

Information security controls derive from a formal risk management process that identifies the nature and magnitude of all threats to and responds with policies and controls to protect information assets and resources. The cost of security is weighed against the potential loss in order to derive a balanced security plan that is both effective and efficient.

Policies are specific statements that allow management to address the mobile device threats and provide a guide in which to create controls and train employees. The controls should address all of the mobile device security policies. Existing research and governance frameworks can assist in the selection of controls that support the policies. COBIT (Control Objectives for Information Technology), for example, is an IS governance framework available from ISACA (www.isaca.org) which can also be applied to mobile devices. The National Institute of Standards and Technology has published guidelines for mobile device security management that addresses both company-owned and employee devices (Souppaya and Scarfone, 2013). These guidelines recommend creating and maintaining mobile security policies and securing all mobile devices before allowing remote access to company files.

Mobile device security policies should reflect the recommendations of several standards for Information Security Management Systems. The most important are the ISO 27001-27006 standards. ISO 27001 was created to "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System" (Davis et al., 2011). ISO 27003 provides guidance through eleven control clauses that includes a security policy, physical security, and access control and incident management.

Table 4: Recommended Mobile Device Security Policies

- Access to corporate data must be secured
- Sensitive data and applications are restricted to employees using the principle of least privilege
- Whitelists and blacklists of mobile applications are maintained
- All applications on employee mobile devices are securely installed
- Employees must sign an accepted use agreement
- Employees must agree to allow personal mobile devices on corporate property to be seized and searched when violations are suspected
- Employees must agree to restrict the use of any mobile device storing corporate data to the employee and no other person
- Employees must register all personal mobile devices brought into the organization
- Employees are not allowed to access corporate information on unregistered devices
- Employees are prevented from installing personal apps on corporate mobile devices
- Employees must acquire permission to install corporate data onto personal mobile devices
- Employees cannot bring jailbroken mobile devices into the workplace or install corporate data on such devices
- All corporate data on mobile devices must be encrypted using the organization's key system

Table 4 lists recommended mobile device security policies. It is important that policies cover the use of employee's personal devices as well as corporate devices and those employees be aware of the policies. Because many of the recommended policies require employee acquiescence in matters that could affect privacy it is essential that a Human Resources representative be involved in policy-making. Stanford University provides a good example of a mobile device security policy and can be viewed online (Stanford, 2104).

Least Privilege Principle

Organizations do not wish to hinder employees from the legitimate use of tools to leverage their abilities. However, information security demands that organizations practice the principle of least privilege. This means that employees are restricted to the minimum level of information resources necessary to perform

their job functions. Workers frequently want to gain administrative rights to devices for greater flexibility but this creates additional vulnerabilities and should be avoided.

Mobile Device Management

Mobile device management (MDM) is a software tool that can be installed on corporate mobile devices to allow centralized control of installation and updates to email, calendar, address books, passcodes, VPN access, and privacy controls. It controls wireless distribution of both data and applications and configurations for phones, tablets, and ruggedized computers (those built to withstand harsh conditions). This includes both corporate and personal devices, which supports the BYOD practice rapidly becoming popular. MDM allows the organization to control the content of mobile devices and insure proper updates are installed throughout the system. Most organizations will choose to implement MDM as an essential and effective security control.

Physical Access Controls

Physical access controls are generally the easiest to execute and to observe. Organizations should identify those mobile devices that pose threats and to limit or prevent their presence in secure areas. The organization may choose to disallow outsiders to bring cell phones, tablets, cameras, and USBs into restricted areas. Safe rooms can be established by blocking transmissions through walls and windows with special paint and electronic jammers. Signs reminding employees and visitors of restrictions and acceptable use policy for mobile devices can be used to heighten awareness.

Logical Access Controls

Logical access controls are used extensively for computer systems and allow the organization to extend the least privilege principle to each employee based upon information needs according to job responsibility. User access controls can be implemented to insure each employee can only access information remotely that is consistent with limited privilege. Strong password policies should extend to all mobile devices and enforced under the same policy as used for all corporate computers.

Data recovery from smart phones and tablets is easily accomplished. Data on SIM and SID cards, for example, can be read on card readers available online for a nominal price. Most mobile phone operating systems allow phones to be wiped remotely. The loss of laptops, phones and tablets represents a serious threat and organizations should insure that any phone containing corporate data be enabled to remotely wipe data in the event the phone has been lost or stolen.

Authentication

Authentication tests are crucial to access control and basic to data security. They verify that the individual, program or message attempting to access a system is legitimate. Strong password policies should be enforced. Device recognition using fingerprinting of each approved device will insure that rogue mobile devices cannot gain unauthorized access.

Encryption

Sensitive data at rest and in transmission should always be encrypted. Strong encryption is easy to accomplish and provides highly effective protection of data. Mobile devices that are approved to contain sensitive information should possess partial or whole device encryption methodology. The decision to employ partial or full device encryption should be based upon the primary use of the device and if it is a corporate or personal device. At minimum, all confidential and personal data should be encrypted.

Monitoring Mobile Device Security

No matter how well a process is conceived it will likely perform below optimum and be vulnerable to well-articulated attacks. Employees may ignore or override controls or the controls may prove to be weak and inadequate. On a regular basis, the effectiveness of the mobile device policies and controls must be

audited. At the same time, management should continually emphasize the importance of the controls and compliance with regulations and standards. Defective or weak policies or controls should be modified to reduce future risks. At minimum, the audit plan for mobile device security should confirm the following:

- existence of security policies for corporate mobile devices and personal mobile devices that are brought into the organization or contain organizational data
- identification of specific mobile device threats
- existence of controls for mitigating or eliminating mobile device threats
- evidence that employees are knowledgeable of mobile device policies and controls
- evidence that employees are in compliance with mobile device policies and controls
- evidence that the controls for mobile device threats are effective and identification of weak or non-existent controls
- signed releases by employees for inspection of personal mobile devices
- verification that mobile clients are running protective software
- evaluation of authentication methods for access control
- verification that rogue access points are not used on the network

Finally, the audit should include written recommendations for corrective action where appropriate. A fuller discussion of IT auditing for wireless devices is presented by Davis et al., (2011).

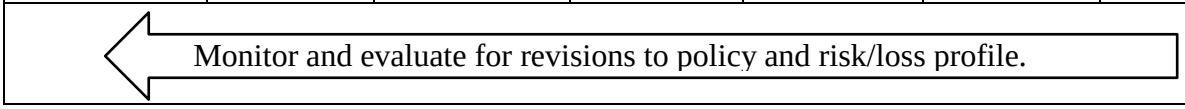
The audit of mobile device security can be integrated with a more extensive IT audit. However, for most firms, mobile devices represent a large and growing component of information resources that require separate and special attention. Many threats to network security are dissimilar to mobile device threats and require different controls and audit tests. At the same time, mobile devices use organizational networks to communicate so, to this extent, the audit of network security is highly important to mobile device security.

A Mobile Device Security Model

The goal in the development of a security model is to create a model that is effective, efficient, comprehensive, and transparent. Transparency promotes understandability and ease of communication to all levels of management, IT specialists, and auditors. Figure 1 presents a seven-stage mobile device security model.

Figure 1: Stages in Developing a Mobile Security Framework

1	2	3	4	5	6	7
Develop Mobile Security Policy	Inventory Devices & Platforms	Inventory Applications	Assess Risk & Loss	Classify According to Risk/Loss Matrix	Actions to Limit Risk & Loss	Educate Employees



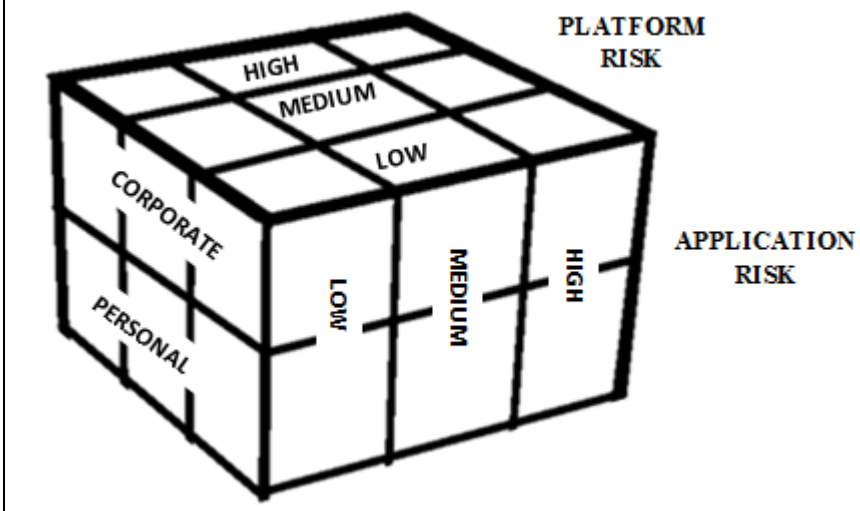
Stage 1: Develop a mobile device security policy by asking users what mobile devices and applications they need to perform their jobs. Explicitly state that the company reserves the right to manage all mobile devices used and brought into the workplace. Insure that data can be remotely wiped from lost or stolen devices and create an acceptable use policy (Netstandard, 2013).

Stage 2: Inventory devices and platforms to determine what mobile devices and operating systems or platforms are currently being used. These should be categorized by corporate-owned devices and personal devices as policies for personal devices may be more restrictive.

Stage 3: Inventory applications that are currently being used on both corporate-owned and personal mobile devices and the business use to ascertain whether the application is necessary to support a valid business function. Determine the source of the application as policy may not allow the use of untested applications, freeware, or shareware.

Stage 4: Assess risk and loss of each device, platform, and application. A high-degree of granularity is not necessary. Categorizing the risks as High, Medium, or Low will provide sufficient information to create an effective security framework.

Figure 2: Identification of Mobile Device Risk Level



Stage 5: Classify the devices, platforms, and applications according to the risk matrix shown in Figure 2. There are eighteen possible risk classifications that reflect whether the device is corporate-owned or personal and the level of risk for platforms and applications. For example, Android operating systems should be classified as high-risk (Greenberg, 2012). Corporate applications are usually low-risk. However, corporate applications on an employee's Android phone may be medium or high risk. Personal applications that do not access the corporate database do not have to be considered but policy may not allow employees to place personal and business applications on the same device to avoid the potential for introducing viruses and other malware into the business applications. Companies must determine their own risk profiles but a suggested one is shown in Table 5.

Stage 6: Take actions to limit risk and loss by ranking the overall risk factor from the risk matrix with the potential loss. Again, a high level of granularity is not needed for assessing the loss. Ranking the possible loss as High, Medium, or Low will be sufficient for security decisions. Using the Risk/Loss Decision Matrix in Figure 3, the intersection of risk and loss will provide a score of one, two, or three. The highest levels of mobile device security should be directed towards those risk/loss combinations ranked a three, while the lowest levels of security should be directed towards combinations ranked a one. This allows for the efficient application of security resources to protecting corporate data from mobile device based attacks.

Table 5: Possible Risk Evaluation of Devices, Platforms and Applications

Corporate Device			Employee Device		
Application Risk	Platform Risk	Overall Risk Level	Application Risk	Platform Risk	Overall Risk Level
High	High	High	High	High	High
High	Med	High	High	Med	High
High	Low	Med	High	Low	High
Med	High	Med	Med	High	High
Med	Med	Med	Med	Med	Med
Med	Low	Med	Med	Low	Med
Low	High	Med	Low	High	High
Low	Med	Low	Low	Med	Med
Low	Low	Low	Low	Low	Low

Figure 3: Risk/Loss Decision Matrix for Use of Mobile Devices

	LOSS		
RISK	Low	Medium	High
High	2	3	3
Medium	1	2	3
Low	1	1	2

Stage 7: Educate and train employees to mobile device security policies and practices noting consequences for violations. Employee education cannot be overemphasized. A survey by CheckPoint Technologies (2014) found that IS security professionals believe careless employees are a greater threat to security than cybercriminals and have the highest impact on mobile device vulnerability and associated data breaches.

Contributions for Researchers, Educators, and Practitioners

This paper presents several opportunities for researchers. Surveys show that organizations have been slow to adopt separate policies and controls for mobile devices. It would be interesting to inquire about the reasons and inhibitors to adoption and ascertain the intentions of organizations with respect to future adoption. It might also be interesting to know the security experiences for companies that have not adopted specific policies and controls versus those who have. Researchers might also use the model of mobile device security to determine if internal audit departments are using a similar approach and, if not, how and why their own approaches deviate from the model.

Accounting educators can benefit from the model and suggestions for policies and controls by incorporating the information into class discussions and projects for courses such as accounting information systems, IT auditing, and forensic accounting.

Practitioners, auditors and IS security officers in particular, should benefit from the suggested model, policies and controls by elevating their understanding of how to approach mobile device security. Executives, risk-management, IT managers, internal auditors, and members of the audit committee should all be interested in adopting practices that reduce corporate risk. At minimum, these suggestions provide a good basis for beginning discussions about mobile device security.

Conclusions

Destructive malware constitutes a serious threat to an organization's operations and reputation. Business continuity can be disrupted through a lack of vigilance in protecting information assets and customers may curtail business with firms that have suffered data breaches especially where personally identifiable information was compromised.

Organizations are becoming increasingly dependent on mobile devices for leveraging workplace performance. Surveys indicate that this trend will continue with increased reliance on mobile devices for a variety of tasks. The modalities of mobile devices are varied and expected to grow. Currently, surveys indicate that mobile device security is lax in most organizations. Theft, infection, and negligent use of mobile devices can result in data breaches that can be expensive to the organization, disrupt operations, and tarnish reputations. Therefore, it is in the best interests of organizations to develop and follow secure mobile device practices with particular attention to policies and controls.

This article presents a useful approach to mobile device security and recommends specific policies and controls for mobile devices. The model is transparent which assists in its understanding and should improve the speed and success of implementation. It also supports the future monitoring and auditing of mobile device security. Researchers can expand on these recommendations while practitioners can employ these recommendations as a basis for creation of a mobile device security framework within their own organization.

References

AICPA. (2013). North America Top Technology Initiatives for CPA's Survey—2013. Retrieved (1/16/2014) from http://www.aicpa.org/INTERESTAREAS/INFORMATIONTECHNOLOGY/RESOURCES/TOPTECHNOLOGYINITIATIVES/Pages/2013TTI.aspx

Apple Insider. (2014). Apple's Phil Schiller plugs security report showing 99% of mobile malware targets Android. Retrieved 1/22/14 from http://appleinsider.com/articles/14/01/21/apples-phil-schiller-plugs-device-security-report-showing-99-of-malware-targets-android

CheckPoint Software LTD (2014). The impact of mobile devices on information security: a survey of IT and security professionals. Retrieved from: http://www.checkpoint.com/press/2014/check-points-third-annual-mobile-security-survey-highlights-careless-employees-greatest-mobile-security-threat.html

Davis, C., Wheeler, K. And Schiller, M. (2011) *IT Auditing: Using Controls to Protect Information Assets, 2nd ed.* McGraw-Hill Publishing.

Forrester Research, Inc. (2012A). Mobile Application Adoption Trends and Strategies to Engage the Workforce. Retrieved (12/15/13) from http://bulldogsolutions.net/Humana/knowledgebase/Mobile_Application_Adoption_Trends.pdf

Forrester Research, Inc. (2012B). The Expanding Role of Mobility in the Workplace. White Paper, Forrester Research. Retrieved (12/28/13) from http://resources.idgenterprise.com/original/AST-0079727_Expanding_Role_of_Mobility_in_the_Workplace.pdf

Glisson, W.B., Storer, T., Mayall, G., Moug, I. and Grispos, G. (2011). Electronic Retention: What Does Your Mobile Phone Reveal About You? International Journal of Information Security, 10, 337-349.

Greenburg, A. (2012). Google Gets Serious About Android Security, Now Auto-Scans App Market for Malware. *Forbes* (2/2/2012)

Hoffman, D. (2013). Exposing Your Personal Information—There's an App. J-Net Community. Retrieved 1/05/14 from http://www.crnbuzz.com/rt_story/security_v1/-exposing-your-personal-information--the/6f6568677830567154535948 4e4a556852684d6633673d3d

Koong, K., Liu, L.C., Bai, S. and Lin, B. (2008). Identify Theft in the USA: Evidence from 2002 to 2006, *International Journal of Mobile Communications*, 6(1), 199-216.

LA Times (2014). "Target Traces Data Breach to Credentials Stolen from Vendor." Retrieved 1/28/14 from: http://www.latimes.com/business/money/la-fi-mo-target-data-breach-vendor-20140129,0,8026.story#axzz2rzEFEbhQ

McAfee. (2012). Mobile Devices Increasingly Vulnerable to Malware. Retrieved 12/15/13 from http://www.techweekeurope.co.uk/news/android-increasingly-vulnerable-malware-133094

Mansfield-Devine, S. (2012). Android Architecture: Attacking the Weak Points. *Network Security*, 2012 (10), 5-12.

Murtagh, R. (2014). Mobile now exceeds PC: the biggest shift since the internet began. Retrieved from: http://searchenginewatch.com/sew/opinion/2353616/mobile-now-exceeds-pc-the-biggest-shift-since-the-internet-began

Netstandard (2013). 13 Best Practices for Developing Your Mobile Device Policy. Retrieved from: http://www.netstandard.com/13-best-practices-for-developing-your-mobile-device-policy/

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

Pearson, T. A. Singleton, T. W. (2008). Fraud and Forensic Accounting in the Digital Environment, *Issues in Accounting Education*, 23(4), 545-559.

Richardson, R. (2011). CSI 2010/2011 Computer Crime & Security Surve. Retrieved 11/15/13 from http://gatton.uky.edu/FACULTY/PAYNE/ACC324/CSISurvey2010.pdf

SANDISK (2008). SanDisk Survey Shows Organizations at Risk from Unsecured USB Flash Drives; Usage is More than Double Corporate IT Expectations. Retrieved 10/22/13 from: http://www.sandisk.com/about-sandisk/press-room/press-releases/2008/2008-04-09-sandisk-survey-shows-organizations-at-risk-from-unsecured-usb-flash-drivesusage-is-more-than-double-corporate-it-expectations/

SANS. (2012). SANS Mobility / BYOD Security Survey. Retrieved (1/16/2014) from http://www.sans.org/reading-room/analysts-program/SANS-survey-mobility

Shih, D., Lin, B., Chiang, H., and Shih, M. (2007). Security Aspects of Mobile Phone Virus: A Critical Survey, *Industrial Management and Data Systems*, 108(4), 478-494.

Stanford (2014). Secure Computing. Retrieved 1/10/14 from https://www.stanford.edu/group/security/securecomputing/mobile_devices.html

Souppaya, M. and Scarfone, K. (2013). Guidelines for Managing the Security of Mobile Devices in the Enterprise. NIST Special Publication 800-124 Revision 1. Retrieved from: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf

Swamy, R. (2014). Android devices targeted by 99 percent of all mobile malware in 2013: Cisco. Retrieved from: http://gadgets.ndtv.com/mobiles/news/android-devices-targeted-by-99-percent-of-all-mobile-malware-in-2013-474106

Tenable-Security. (2012). Mobile Device Vulnerability Management Flagged as Top Concern for Security Professionals in 2012. Retrieved (1/16/2014) from http://www.tenable.com/press-releases/mobile-device-vulnerability-management-flagged-as-top-concern-for-security

Tran, E. and Atkinson, M. (2002) "Security of Personal Data Across National Borders," *Information Management & Computer Security*, 10(5), 237-241.

Zhang, Y., Lee, W. and H., Yuang. (2003). Intrusion Detection Techniques for Mobile Wireless Networks. Wireless Networks, 9(5), 545-556.