7-2011

Your Firm's Mobile Devices: How Secure Are They?

Harry R. Wright Jr.
Georgia Southern University, hrwright@georgiasouthern.edu

J. Lowell Mooney
Georgia Southern University, lmooney@georgiasouthern.edu

Abbie Gail Parham
Georgia Southern University, aparham@georgiasouthern.edu

Your Firm's Mobile Devices: How Secure Are They?

Harry R. Wright Jr., J. Lowell Mooney, and Abbie Gail Parham

Mobile communication devices are taking the world by a storm. They offer significant benefits. But when deciding whether your company can benefit from giving mobile devices to employees, it is important to think strategically. Do you have a comprehensive mobile security strategy? Do you have a well-thought-out set of policies and procedures in place?

The authors of this article take a critical look at mobile device security. Then they provide a detailed set of checklists to help you develop strategic goals; effectively manage mobile devices; protect company data; and evaluate the effectiveness of your security plan.

INTRODUCTION

A study conducted by Morgan Stanley's *Investment Management Journal* predicts that more people will access the Internet from mobile devices than personal computers by the year 2015 ("Here's How Businesses Can Recruit," 2011). With the world's rapid adoption of Web 2.0 wireless technology and expanded bandwidth, coupled with the rapid deployment of ever more powerful mobile hardware and applications, these devices, which include smartphones, iPads, tablet PCs, and PDAs, are becoming increasingly ubiquitous in the workplace.

Mobile technology moves well beyond the mere convenience of a cell phone or laptop, both of which have had long acceptance in business for their utility. The cell phone untethered employees from landline phones and laptops revolutionized the ability of employees to work remotely. But those tools pale in comparison to today's mobile devices, whose portability and ability to access corporate servers, data, and information, regardless of where the employee is geographically, are revolutionizing the way business gets done. The telecommunications companies and governing regulators around the world have recognized this coming and evolving technology for decades. At the 2008 Davos meeting, one of the most interesting panels was on the future of mobile technology. Panelist Eric Schmidt, Google's CEO, noted that the new 700MHz bandwidth spectrum introduces what he called a "huge revolution" in new mobile technology and applications (Arrington, 2008).

Yet, this marvelous benefit can be overappreciated. As various types of mobile devices enter the workplace, either as an employee's personal technology or as company technology, and as they rapidly morph into more powerful capabilities and applications, they present a strategic risk to the company, particularly from data theft and security breaches. In fact, the control and use of mobile devices emerged this year as the top business technology concern for CPAs and financial executives on the annual Top Technology Initiatives Survey by the American Institute of Certified Public Accountants (AICPA; 2011).

Published online in Wiley Online Library (wileyonlinelibrary.com).
DOI 10.1002/jcaf.20701

This article focuses on how new and developing mobile technology being deployed in the workplace should be understood and strategically managed and how the growing risk to securing them must be aggressively addressed. Also included are a series of checklists from a variety of industry experts that should help you assess where your organization is on the control and protection of mobile devices.

ADDRESSING GEN-Y MOBILE TECHNOLOGY RISKS

Ready or not, handheld devices are proliferating the workplace. As with most technology, the younger employees are beating the drum for adoption of new computing devices into the workplace. As evidence, consider that at the end of 2009, almost 530 million users browsed the mobile Web on their handset. According to Strategy Analytics, this is forecast to rise to over 1 billion by 2015. Within the next five years, mobile Web access using handsets, laptops, tablet computers, and other mobile devices will surpass the desktop PC as the most popular way to access the Internet (mobiThinking). Driving these changes is the new breed of employees now entering the workplace dubbed "Generation Y." A recent survey of 18-to-24-year-olds by Accenture found that 51 percent prefer to use a mobile handset over a laptop. By the way, only 22 percent prefer a PC. It probably will not surprise you that among those respondents age 45 and older, only 27 percent prefer a mobile device (Sybase, 2011).

In our last article, "Gen Y's Addiction to Web 2.0: Problem or Strategy?" we warned about the coming severe shortage of workers and advocated embracing Web 2.0 as one way to recruit, engage, and retain the current generation of workers. We further noted that while Generation X had transformed the analog workplace of their Traditionalist and Baby Boomer predecessors into a modern digital workplace, we predicted that Generation Y would put that digital office on steroids. Generation Y workers "expect organizational information and records, along with the applications and systems used to manage them, to be instantly available, even on their handheld devices" (Mooney, Wright, & Higgins, 2010, p. 64).

The ability to exchange data and information wherever and whenever can set your organization apart and help you recruit and retain high-quality employees who are wired for 24/7 connectivity.

As it is with most things, the surging use of mobile devices is a mixed blessing. The ability to exchange data and information wherever and whenever can set your organization apart and help you recruit and retain high-quality employees who are wired for 24/7 connectivity. Freed from their desks and an eight-hour workday, these employees can respond to customer needs faster and more effectively. Yet, how does the organization control and protect the corporate information stored on the company's servers and desktops from unauthorized access via a mobile device, or from loss or theft once data has been transferred to a mobile device? Something as simple as losing your phone can now create an enormous security risk for your organization.

While some organizations have aggressively rolled out mobile technology, many have been reluctant to open up access to their organization's information assets and business processes. Yet the workplace is already saturated with mobile technology thanks mostly to the personal handheld devices that employees own and bring to work. Too few, we suspect, have fully examined or adequately addressed the ability of either employer-issued or employee-owned mobile devices to retrieve, interact with, or extract corporate information and the risks portable technology presents to the firm. Regardless of where your company is positioned on managing mobile technology in the workplace, several strategic issues should be either reviewed or addressed.

MOBILE DEVICES ENABLE SIGNIFICANT ENTERPRISE BENEFITS

A mobile device is a pocket-sized computing device that often has a display screen with touch input or a miniature keyboard. Mobile devices can be divided into the following groups: mobile or handheld computers and tablets; communication devices such as smartphones; media recorders and players; navigational devices; and accessories such as handheld game consoles.

DOI 10.1002/jcaf

In 2009, sales of laptops exceeded sales of desktops, and *IDC Worldwide Quarterly* estimates that by 2012, 65 percent of all personal computers sold will be portables. Perhaps more important for business is the finding that by 2014 more users will access the Internet using a mobile device than by using a desktop (Jagst, 2011). According to ITU, there were 5.3 billion mobile handset subscriptions at the end of 2010, equivalent to 77 percent of the world population. Furthermore, approximately 90 percent of the world's population now lives in a place with access to a mobile network.

The shift toward using mobile devices to replace the desktop and laptop is clear, yet many have not thought about the significance of that shift being leveraged in a purely business environment. The evolving mobile device technology can, if properly utilized, enable the enterprise to achieve a number of significant benefits:

- Improved workforce productivity: Employees can remotely access company information and complete work off-site. According to the Aberdeen Group, the best-in-business enterprises have captured a 40 percent increase in employee productivity.
- Improved customer service: With real-time access to customer information, employees can significantly improve turnaround times for problem resolution. Again, according to the Aberdeen Group, the best-in-business enterprises have seen an average of 35 percent improvement in customer satisfaction.
- Increased business process efficiency: The use of supply-chain management allows companies to improve business processes by shortening the time between order, production, and shipment.
- Employee security and safety: Employees traveling on work-related business are always in touch and connected.
- Employee retention: With mobile devices, many work tasks can be performed remotely, resulting in improved work-life balance. Research by the Aberdeen Group indicates that the improvement in work-life balance can increase employee retention by up to 25 percent (ISACA, 2010).

THINKING STRATEGICALLY

In deciding whether your organization can benefit from the use of mobile devices, it is important to think strategically. Remember you need a carefully constructed mobile security strategy that covers both corporate devices and personal devices. The checklist in Exhibit 1 provides some initial considerations for developing or reviewing a corporate strategy for these devices, while Exhibit 2 illustrates the types of questions that should be considered as part of any corporate plan that embraces mobile technology.

RISKS AND SECURITY

The risk of loss, theft, or misuse of confidential information is high with mobile devices,

Exhibit 1

Strategy Goals for Mobile Devices

- Has your IT organization defined the allowable mobile device types (e.g., enterprise-issued vs. personal devices and BlackBerry vs. iPhone)?
- Have the services accessible through mobile devices been defined and explained, taking into account the existing IT architecture?
- Have the tasks for which employees may use mobile devices and the types of applications that are allowed been enumerated?
- Has your IT organization sufficiently identified the ways employees actually use mobile devices to understand how that use may lead to unpredictable risks?
- Have all enterprise-issued devices been integrated into a comprehensive asset management program?
- Has your IT organization specified the type of authentication and encryption that must be present on mobile devices?
- Have your employees been properly trained to store and transmit sensitive corporate data?

Source: ISACA (2010).

DOI 10.1002/jcaf

Exhibit 2

Four Key Questions to Address When Developing a Mobile Security Strategy

1. **How do we deny access to unauthorized users?** Require employees to set a strong password on their mobile device and to change it every three to six months. Mobile management systems can automate enforcement.
2. **What's our plan if a personal device gets lost or stolen?** Passwords aren't enough; you must be able to lock and wipe the device remotely. The first lets you "freeze" a device, which is useful if there's a good chance it will turn up again. If it's gone for good, remote wipe lets you permanently erase stored data.
3. **How do we remove corporate data from a personal device whose owner is leaving the company?** Management tools can be used to segregate enterprise and personal data. When an employee leaves, IT can wipe the enterprise data while leaving personal data unaffected. This capability protects the organization without inconveniencing the user.
4. **How do we keep prying eyes away from confidential files?** Use mobility management software to encrypt enterprise data, both as it is transmitted and when it is "at rest" in the device's memory.

Source: Sybase (2011).

Exhibit 3

Mobile Security Features

- **Enforced authentication:** Does your IT organization require users to enter a password when the device is cycled on?
- **Over-the-air data encryption:** Does your organization require that mobile devices use Secure Sockets Layer (SSL) when exchanging data wirelessly?
- **Over-the-air provisioning:** Can your IT technicians configure and update mobile applications remotely from a central platform?
- **Remote wipe and data fading:** Can they remotely clear all data and settings on a lost or stolen PDA, smartphone, or tablet?
- **Full disk encryption:** Does your IT organization use full disk encryption to make it virtually impossible for anyone without authorization to read private data on a mobile device?
- **Separation of personal and enterprise information:** Can your IT staff secure, control, and erase corporate data and applications without impacting the user's personal photos, music, or games?
- **User access rights and security policies:** How well does your IT department control exactly what data users can access with their mobile devices?
- **Network filters:** Are filters used to monitor who is attempting access to the corporate network and to block access unless a device management client is installed on the device?

Source: Sybase (2011).

DOI 10.1002/jcaf

Exhibit 4

Seven Rules for Effective Mobile Management

1. **Identify all mobile devices on the network:** Have you audited your e-mail server and other systems to make sure there are no unauthorized devices?
2. **Know which back-office systems employees need to access:** Have you identified which employees can suffice with just e-mail access vs. which need special purpose applications vs. which need executive-level access?
3. **Formalize user types and set policies:** Have you created appropriate user groups and set strict governance policies for each one?
4. **Be ready to block access:** Are filters used to control access to your back-end systems to block access to devices that don't have a management client installed?
5. **Add password and encryption policies plus remote wipe:** Has your IT organization implemented such bare minimum mobile security measures as password enforcement, on-device data encryption, remote wipe for lost devices, and inventory management to identify which devices are connected to the network?
6. **Consider separating personal data from business data:** Are your mobile devices able to store enterprise data in one area of the device and encrypt and password-protect only that area?
7. **Enable users to be self-sufficient:** Have you lessened the burden on your IT organization by using a client management application that keeps mobile devices in compliance? Do you have a robust user training program?

Source: Sybase (2011).

especially if the company does not have a strong security strategy that addresses their unique characteristics. The greatest drawback of these devices, whether deployed by the company or simply those in possession of employees, is the security risk they pose.

On the one hand, these devices have to be viewed like existing PCs and laptops, as they are also susceptible to malicious viruses and malware, Trojan horses, cyber attacking malicious applications, spam, worms, and phishing schemes. Obviously, they are more susceptible to loss, theft, and damage since they are portable. On the other hand, mobile devices must be viewed differently from other information processors in that there are unique threats to these devices such as jailbreak software, which allows strangers to hijack the device and access information, and the problems presented by the ability of these devices to connect automatically to an unknown Bluetooth device nearby or to an open, unsecured Wi-Fi.

Furthermore, with the increasing expansion and availability of new applications developed on open platforms for specific use on mobile devices,

Exhibit 5

Top Technology Questions Asked by Audit Committees, CFOs, and CIOs

1. Is our information security policy adequate?
2. Are we ensuring that our data and technology resources are protected against hacking, viruses, or other compromises?
3. Are our current internal controls and IT governance policies and procedures effective?
4. How can we best implement document retention and e-discovery policies?
5. Can our data remain safe if we utilize cloud computing/software services?

Source: AICPA (2011).

DOI 10.1002/jcaf

Exhibit 6

Ten Steps to Securing Your Mobile Devices

1. Configure mobile devices securely.
   a. Enable auto-lock.
   b. Enable password protection and require complex passwords.
   c. Avoid using auto-complete features that remember usernames or passwords.
   d. Ensure that browser security settings are configured appropriately.
   e. Enable remote wipe.
   f. Ensure that SSL protection is enabled, if available.
2. Connect to secure Wi-Fi networks and disable Wi-Fi when not in use.
   a. US-CERT recommends disabling features not currently in use such as Bluetooth, infrared, or Wi-Fi. Additionally, set Bluetooth-enabled devices to nondiscoverable to render them invisible to unauthenticated devices.
   b. Avoid joining unknown Wi-Fi networks.
3. Update mobile devices frequently. Select the automatic update option, if available.
   a. US-CERT recommends maintaining up-to-date software, including operating systems and applications.
4. Utilize antivirus programs and configure automatic updates, if possible.
   a. US-CERT recommends installing antivirus software as it becomes available and maintaining up-to-date signatures and engines.
5. Use an encryption solution to keep portable data secure in transit.
   a. Data protection is essential. If confidential data must be accessed or stored using a mobile device, make sure users have installed an encryption solution (e.g., GuardianEdge Smartphone Protection, McAfee Endpoint Encryption, PGP Mobile, and Pointsec Mobile Encryption).
   b. Do an assessment—or at least be aware—of the encryption options available for mobile devices. Some devices may offer more mature security solutions than others.
   c. Consider using thin client models so that data is centrally and securely maintained. This is one option to help avoid storing confidential data on mobile devices. It also means not having to develop new solutions every time a new mobile technology is released.
   d. Educate users to avoid using or storing confidential data on a mobile device whenever possible.
6. Use digital certificates on mobile devices.
7. Take appropriate physical security measures to prevent theft or enable recovery of mobile devices.
   a. For laptops, use cable locks.
   b. Use tracing and tracking software (e.g., Computrace, Lookout, MobileMe).
   c. Never leave your mobile device unattended.
   d. Report lost or stolen devices immediately.
   e. Remember to back up data on your mobile device on a regular basis.
8. Use appropriate sanitization and disposal procedures for mobile devices.
   a. Delete all stored information prior to discarding, exchanging, or donating devices.
9. Develop appropriate policies, procedures, standards, and guidelines for mobile devices.
10. Educate employees about mobile device security.
    a. Remind users to be cautious when opening e-mail and text message attachments or clicking on links.
    b. US-CERT recommends that users avoid opening files, clicking links, or calling numbers contained in unsolicited e-mails or text messages. Users should know what they are downloading.
    c. Be aware of current threats affecting mobile devices.

Source: https://wiki.internet2.edu/confluence/display/itsg2/Mobile+Device+Security.

DOI 10.1002/jcaf

there are now many ways to undermine the security protocols and policies of most organizations that were designed around servers, PCs, and laptops. Since the risks are more difficult to identify, managers must consciously take key steps to protect the business from risks that may be under the corporate security radar. Has your company created systems designed to take advantage of mobile security features that are unique to mobile devices that could pose a risk to your business? Exhibit 3 lists some of the most common security features used to protect mobile assets.

Systems and policies should be developed to evaluate and manage the security features of various devices that are already in the workplace or corporately deployed, particularly as to what information they are able to access on company servers or stand-alone computers. Again, this parallels commonly known concerns with PCs and laptops, but with mobile devices, several other considerations must be taken into account. Exhibit 4 describes seven rules for effective mobile device management.

ADDRESSING CONCERNS

According to the AICPA (2011), "mobile devices are receiving more attention as technological advancement shifts productivity tools from desktops to pockets amid increasing reliance on mobile applications." Research firm Gartner Inc. predicts that approximately 117 billion applications will be downloaded to mobile devices worldwide by the end of 2011. The AICPA technology survey researchers asked CPAs to identify the top technology questions asked by audit committees, chief financial officers (CFOs), and chief information officers (CIOs). Their questions are reported in Exhibit 5.

Effective remote management and data-protection tools and policies are key to preventing mobile security breaches. Protecting sensitive information on mobile devices requires an understanding of the many ways security can be compromised. Providing

Exhibit 7

Auditing Mobile Device Processes and Policies

- **Policy:** Does a security policy exist for mobile devices? Does it include rules for appropriate physical and logical handling? The enterprise should have a policy addressing mobile device use and specifying the type of information and kind of devices and information services that may be accessible through the devices.
- **Antivirus updates:** Do the auditors verify that the enterprise updates its mobile device antivirus software to prevent perpetuation of malware?
- **Encryption:** Do the auditors verify that any data labeled as sensitive are properly secured while in transit or at rest?
- **Secure transmission:** Do the auditors confirm that mobile device users are connecting to the enterprise network via a secure connection using, for example, VPN, IP security (IPsec), or Secure Sockets Layer (SSL)?
- **Device management:** Have the auditors determined whether there is an asset management process in place for tracking mobile devices? This asset management program should also detail procedures for lost and stolen devices as well as procedures for employees who have been terminated or have resigned from the enterprise.
- **Access control:** Do the auditors verify that data synchronization of mobile devices is not set to receive access to shared files or network drives that contain data that are prohibited for mobile use?
- **Awareness training:** Do the auditors verify that the enterprise has an awareness program in place that addresses the importance of securing the mobile devices physically and logically? The training should also make clear the types of information that can and cannot be stored on such devices.
- **Risk:** Do the auditors confirm that policies and procedures exist and are functioning as management intended to ensure that the company's information assets are not subjected to high risk of data leakage and loss?

Source: ISACA (2010).

DOI 10.1002/jcaf

a bullet-proof strategy requires mobile security policies and functions, security-aware employees, and a comprehensive set of mobile device management tools (Sybase, 2011). Exhibit 6 presents ten key steps to securing your organization's mobile devices.

MAKING SURE YOU ARE FULLY PROTECTED

Your organization should have a comprehensive mobile device policy enforceable on all employed devices and centrally managed by your IT staff. While flexibility is important, it should be simple to implement and support. Finally, it must be auditable so that assurance can be gained that the organization is doing everything possible to protect its investment in mobile technology. Exhibit 7 describes audit procedures for assessing the operating efficiency of your mobile device policies and procedures.

REFERENCES

American Institute of Certified Public Accountants (AICPA). (2011). Top technology initiatives survey. Retrieved from http://www.aicpa.org/INTERESTAREAS/INFORMATIONTECHNOLOGY/RESOURCES/TOPTECHNOLOGYINITIATIVES/Pages/2011TopTechInitiatives.aspx

Arrington, M. (2008, January 25). Super panel at Davos: The future of mobile technology. Retrieved from http://techcrunch.com/2008/01/25/super-panel-at-davos-the-future-of-mobile-technology/

Here's how businesses can recruit best talent after recession. (2011, April 17). Alexandria Echo Press. Retrieved from http://www.echopress.com/event/article/id/83854/group/homepage/

ISACA. (2010, July). Securing mobile devices. Retrieved from http://www.isaca.org/Knowledge-Center/Research/Documents/SecureMobileDevices-Wht-Paper-20July2010-Research.pdf

Jagst, M. (2011, March 14). Mobile computing takes accountants to a new level of productivity. Retrieved from http://www.cscpa.org/Content/24470.aspx

Sybase. (2011). Enterprise mobility guide 2011. Retrieved from http://resources.idgenterprise.com/original/AST-0032585_MobilityGuide_2011_Sybase.pdf

FURTHER READING

Best Practices Guide, Mobile Device Management. (n.d.). Retrieved from http://content.maas360.com/www/content/wp/11-Mobile-Device-Management-Best-Practices.pdf

DeFelice, A. (2011, April). Survey highlights emerging tools for firms of all sizes. Retrieved from http://www.journalofaccountancy.com/Issues/2011/Apr/20103506

Definition of mobile device. (n.d.). Retrieved from http://en.wikipedia.org/wiki/Mobile_devices

Forrester Consulting. (2010). Managing and securing corporate and personal mobile devices in financial services. Retrieved from http://content.maas360.com/www/content/wp/ForresterFinancialSector-WP.pdf

Harris, S. (2009, April 28). Mobile devices: Definition and security issues (part 1 of 5). Retrieved from http://www.informit.com/blogs/blog.aspx?uk=Mobile-Devices-Definition-And-Security-Issues-Part-1-of-5

Harris, S. (2009, April 30). Mobile devices: Security implications and countermeasures (part 2 of 5). Retrieved from http://www.informit.com/blogs/blog.aspx?uk=Mobile-Devices-Security-Implications-and-Countermeasures-Part-2-of-5

Increased business use of mobile devices is top IT challenge. (2011, February 15). Retrieved from http://www.accountingweb.com/topic/technology/increased-business-use-mobile-devices-top-it-challenge

It's all about security: Things to know before you open the doors to smartphones and tablets in your enterprise. (n.d.). Retrieved from http://resources.idgenterprise.com/original/AST-0032586_Its-All-About-Security-WP.pdf

Kerravala, Z. (2010, June). Mobility powers the next wave of growth for unified communications. Retrieved from http://resources.idgenterprise.com/original/AST-0025326_Mobility_Powers_Next_Wave_of_Growth_for_UC_-_Yankee_Group.pdf

Messmer, E. (2011, March 8). Corporate data breach average cost hits $7.2 million. Retrieved from http://www.networkworld.com/news/2011/030811-ponemon-data-breach.html

Mobility at a crossroads: Are you missing new business opportunities in mobility management? (n.d.). Retrieved from http://resources.idgenterprise.com/original/AST-0032587_Managed-Mobility-Crossroads-WP.pdf

Muir, J. (2003, July 13). Decoding mobile device security. Retrieved from http://www.computerworld.com/s/article/82890/Decoding_Mobile_Device_Security?taxonomyId=017

Petrassi, J. (2010). The Internet moves to mobile devices. Leading Edge Forum, CSC Papers 2010. Retrieved from http://assets1.csc.com/lef/downloads/CSC_Papers_2010_The_Internet_Moves_to_Mobile_Devices.pdf

Vogel, V. (2010, November 11). Mobile device security. Ten steps to securing your mobile device. Retrieved from https://wiki.internet2.edu/confluence/display/itsg2/Mobile+Device+Security

DOI 10.1002/jcaf

Harry R. Wright Jr., JD, is an associate professor of legal studies at Georgia Southern University in Statesboro, Georgia. His teaching and research interests include employment law, international trade, business ethics, and computer law. Dr. Wright has conducted continuing education programs in the computer and information systems areas for the legal and accounting professions and has been a frequent guest speaker on computer-related topics. **J. Lowell Mooney**, PhD, is a professor of accounting at Georgia Southern University in Statesboro, Georgia. Dr. Mooney worked for several years in the information systems organization of a major telecommunications firm. His teaching and research interests include the Internet's impact on business operations, computerized accounting information systems, and performance evaluation systems. **Abbie Gail Parham**, MBA, CPA, CMA, CFM, SAP Certified, is an assistant professor of accounting at Georgia Southern University in Statesboro, Georgia. Parham has work experience in public accounting and private industry, where she was a cost accountant for a Fortune 500 company. Her teaching and research interests include managerial accounting, fraud and ethics, and student learning and retention using Process-Oriented Guided Inquiry Learning (POGIL).

 DOI 10.1002/jcaf