Fall September 28, 2007

Management of security policies for mobile devices

Andrew Green, *Kennesaw State University*

Management of Security Policies for Mobile Devices

Andy Green
Kennesaw State University
1000 Chastain Rd MS 1101
Kennesaw, GA 30144
770-423-6005
andy@andy-green.org

ABSTRACT
This paper discusses management of security policies for mobile devices. The increasing use of mobile devices in the workplace is covered, as well as new software applications that allow employees to use their mobile devices to increase their productivity. Various risks to businesses arising from compromised mobile devices are discussed. Mobile devices are defined, as are some common attack vectors currently present in most devices. A framework for creating mobile device security policies is discussed, and sample policy language for mobile devices is offered.

Categories and Subject Descriptors
H.1.m [**Models and Principles**]: Miscellaneous

General Terms
Management, Documentation, Design, Economics, Security, Human Factors, Standardization, Theory, Legal Aspects, Verification.

Keywords
information, security, management, mobile, device, PDA, policy, standards, smartphone, cellular, technology, risk, bluetooth, telephone, ipod, camera, attack, usb, laptop, computer.

1. INTRODUCTION
Mobile devices have become a fact of life for businesses, both large and small. Mobile devices allow employees the freedom and flexibility to work away from the traditional office setting, increasing employee productivity. According to Bob Monk, project manager at Drive Assist, after equipping half of the staff and all of his sales force with "smart phones", "…productivity doubled almost immediately" [5]. However, productivity increases are not limited strictly to these devices. Portable USB storage devices are also mobile devices that can help increase employee productivity. Smaller, portable versions of email clients, web browsers, calendar applications, IM chat clients, and video viewers are available for installation and usage on portable USB drives, allowing employees to carry a miniature computer with them.

Information Security Curriculum Development Conference'07, September 28-29, 2007, Kennesaw, Georgia, USA.

Recent surveys indicate the growing usage of mobile devices in the workplace. According to a 2005 study released by Nokia, 21% of United States employees carry personal data assistants (PDA), while 63% carry mobile telephones, all for business use [4]. One survey found USB storage drive usage in the workplace at 73% in 2006, up from 65% in 2005 [3].

As the availability of mobile devices increases, their cost decreases, and businesses try to find new and better ways to improve worker productivity, use of mobile devices in the work place will only continue to increase. Thus, it is imperative that businesses develop a sound security policy for these devices in their work space.

2. MOBILE DEVICES DEFINED
For purposes of this paper, mobile devices are defined as one of the following:

- Laptop computers;
- Portable Digital Assistants, or PDAs;
- Full-featured mobile telephones with personal computer-like functionality, or "smart phones" [6];
- Portable USB devices, such as "thumb drives", MP3 devices such as Apple iPod or Microsoft Zune;
- Digital cameras;

3. RISK TO BUSINESS
Any time company data is lost or compromised, the business is at risk. This risk can come from various sources, including:

- decreased market share due to loss of consumer faith;
- legal action taken by consumers and partners;
- legal penalties and fines from federal and state legislation such as HIPAA, Gramm-Leach-Bliley, Sarbanes-Oxley, and California SB1386;
- competitors use of lost/compromised data;

4. ATTACK VECTORS

As the use of mobile devices has increased in the workplace, so has the number of attacks against these devices. In a 2007 study released by McAfee Inc., the well-known anti-virus vendor, 83% of mobile operators said they had suffered infections on their mobile devices [2]. Compromised mobile devices attached to a company's computer network offer criminals a way to access that network for their nefarious purposes.

Data theft by employees is also a major concern with mobile devices. "Podslurping", or copying large amounts of company data to a USB device, is a technique that is on the rise. According to Abe Usher, CISSP, a security industry veteran with 10 years of experience, taking business data with one of these devices is simple: "…in 2 minutes, it's possible to extract about 100MB of Word, Excel, PDF files--basically anything which might contain business data--and with a 60GB iPod, you could probably have every business document in a medium-size firm" [7]. To reinforce his point, Usher wrote and released an application that allows users to store data on their iPod or similar mobile storage device [7].

Bluetooth technology is another possible attack vector with mobile devices. Bluetooth allows short-range, wireless connections between various devices, such as mobile phones, laptop and desktop computers, printers, and digital cameras [1]. Bluetooth devices are susceptible to various attacks, including "bluebugging", and "bluesnarfing". Using these vectors, an attacker can either gain access to data contained on the device, or actually use the device to place calls, conduct IM sessions, or access the web [1].

Wireless technology is yet another possible attack vector when securing mobile devices. Mobile devices frequently have "WiFi" capability integrated into their design, or as an add-on. However, if not configured properly, mobile devices using "WiFi" can offer attackers another avenue of entry into a corporate network. According to Lisa Phifer, "Cradled PDAs can become Wi-Fi bridges into corporate networks" [4].

There are a number of business applications that have been developed for use on mobile devices. In the 2005 Nokia study referenced earlier in this paper, "…commonly-used mobile applications included e-mail, instant messaging, corporate database access, sales force automation, field service, CRM and ERP/supply chain applications" [4]. Security researchers are constantly discovering vulnerabilities in these applications, which can be exploited by attackers to gain access to a business system.

5. SECURITY POLICY CREATION

Businesses should seek to standardize the creation of their security policies, for many reasons. There are many acceptable frameworks and templates currently in use by businesses today, such as Charles Cresson Wood's "Information Security Policies Made Easy", and a framework offered by Lisa Phifer in her April 2006 column published on the SearchSecurity.com website. For this paper, the Issue-Specific Security Policies framework offered by Whitman and Mattord in their textbook "Management of Information Security, 2nd ed." will be utilized [8]. This framework was chosen over others because of its ease of understanding and use, as well as clearly defined sections that make policy composition easier.

1. Statement of Purpose
2. Authorized Uses
3. Prohibited Uses
4. Systems Management
5. Violations of Policy
6. Policy Review and Modification
7. Limitations of Liability

5.1 Statement of Purpose

In this section, management addresses the need for the policy. This section also identifies the parties responsible for policy implementation and enforcement. Finally, this section describes the technology being addressed. For mobile devices, this section could read something like:

"This document describes the security guidelines for mobile devices. Mobile devices must be secured in order to secure proprietary company data, prevent the spread of malicious applications like viruses or Trojan horses on company computer assets, and prevent unauthorized access to company networks. This policy is implemented and enforced by senior management, company IT and InfoSec staffs, and supervisors.

Examples of mobile devices include:

- *laptop computers*
- *Portable Digital Assistants, or PDAs;*
- *smart phones;*
- *portable USB devices, such as "thumb drives", MP3 devices such as Apple iPod or Microsoft Zune;*
- *digital cameras;*

5.2 Authorized Uses

In this section, authorized users and technology usage are detailed. For example:

"Employees for whom the company purchased a mobile device are authorized to use them strictly for purposes related to conducting business on behalf of the company. Furthermore, consistent with existing company policy regarding privacy, employees are reminded they have no expectation of privacy when using company mobile devices."

5.3 Prohibited Uses

Here, users are told what the technology cannot be used for. For example:

"Employee usage of mobile devices for activities not related to company business is prohibited. Examples of these types of activities include "web surfing" for non-business purposes, making or receiving personal telephone calls, listening to personal music stored on the device, checking personal email, file transfer or storage on the device. Employees are prohibited from using a company mobile device to engage in any type of criminal, offensive, or disruptive behavior, as well as any type of behavior that would bring the good name and character of the company into question. Employees are also prohibited from loading any type of software application on the device, as this is handled by company IT staff as needed."

5.4 Systems Management

In this section, policy authors focus on users' relationships to systems management. For mobile devices, this section can be extensive. A possible systems management section could read as:

"Employees using mobile devices must ensure they meet the following requirements when using a mobile device, as well as any applications or data contained on the mobile device:

Power-on authentication: *Users must be required to enter a password upon powering on the device, to minimize risk if a device is lost or stolen.*

File/folder encryption: *Users must ensure files and folders that contain company data are encrypted.*

Antivirus software: *Users must ensure the antivirus software installed on the mobile device is up-to-date and running at all times.*

Lost/stolen/missing device: *Users must immediately report a lost/stolen/missing mobile device to their supervisor.*

Secure wireless transmission: *Users must never transmit any data over an unsecured wireless channel. Use the VPN client installed on the device; ensure the wireless network you are attached to is encrypted, or both.*

Firewalls: *Users must ensure the firewall client installed on the device is running and updated.*

Passwords: *Users must use strong passwords to encrypt mobile devices*

5.5 Violations of Policy

In this section, users are told of the penalties involved if they violate the policy, as well as how to report suspected violation of the policy by others. An example for mobile devices could be:

"There are penalties involved with violating this policy. On the first violation, the user will receive a written warning from his/her supervisor regarding the incident. On the second violation, the user will be suspended without pay for a week, as well as receive another written warning. On the third violation, the user's employment with the company will be terminated.

These penalties are the minimums involved with each offense, and management reserves the right to escalate punishments based on the particulars of any given violation.

All employees are encouraged to report any suspected violation of this policy. These reports may be filed anonymously by using the ombudsman page on the company intranet. No personally identifying information is requested on this page, nor is any kept in server logs."

5.6 Policy Review and Modification

In this section, users are told how and when this policy will be reviewed. An example for the mobile device policy could be:

"This policy will be reviewed yearly, with any updates being published the first Monday in November. The policy will be reviewed by a committee appointed by the company CISO. This committee will be appointed by September 1st of each year, and will be announced on the company intranet. Additionally, contact information for the committee will also be published, so that employees may provide any feedback they feel the committee may need when reviewing this policy.

5.7 Limitations of Liability

Here, the company seeks to protect itself legally by expressly stating any limitations of liability if the policy is not followed. For example:

"The company is not liable in the event an employee willfully violates this policy, resulting in any type of criminal or civil penalty. The company will not offer employees any type of protection or assistance if they are prosecuted or charged with a crime while violating this policy. The company denies any responsibility or acceptance of blame for an employee who willfully violates this policy.

6. CONCLUSIONS

Mobile devices in the enterprise are a good way to increase employee productivity. However, without proper management and control, they provide another avenue for attack on company information assets. These devices cannot simply be treated as telephones, USB drives, or music players. They are mobile computing devices, and company policy must treat them appropriately. Prudent IT and InfoSec professionals, and business management would be well served to begin laying the foundation for mobile device security sooner, rather than later.

7. REFERENCE LIST

[1] "Bluetooth". (2007). Retrieved June 25, 2007, from http://en.wikipedia.org/wiki/Bluetooth

[2] Brenner, Bill. (2007, February 13). "Mobile carriers admit to malware attacks". Retrieved June 25, 2007 from http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1243513,00.html

[3] "Hackers using a new threat, Web@Work survey". (2006, May 18). Retrieved June 25, 2007 from http://www.crime-research.org/articles/hackers-using-new-threat/

[4] Phifer, Lisa. (2006, April 25). "Policies for reducing mobile risk". Retrieved June 25, 2007 from http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1184648,00.html?bucket=ETA&topic=300021

[5] Pritchard, Stephen. (2007, June 18). "Mobile apps will boost productivity". Retrieved June 25, 2007, from http://www.computerweekly.com/Articles/2007/06/18/224847/mobile-apps-will-boost-productivity.htm

[6] "Smartphone". (2007). Retrieved June 25, 2007 from http://en.wikipedia.org/wiki/Smart_phone

[7] Sturgeon, Will. (2006, February 15). "Beware the 'pod slurping' employee". Retrieved June 25, 2007, from http://news.com.com/Beware+the+pod+slurping+employee/2100-1029_3-6039926.html

[8] Whitman, M., & Mattord, H. (2007). *Management of Information Security* (2nd ed.). Boston: Thomson Course Technology.