# Managing Mobile Computing Risks

***by Rebecca Herold, CISSP, CISM, CISA, FLMI***

As demonstrated over and over again throughout the past several months, mobile computing devices and storage media present a huge risk to business and personal information. Because of the very portability of these devices, organizations are entrusting the security of the information stored upon them into the hands of the people using them. It is vital that an effective mobile computing device and storage media security management program is in place. This program should answer the questions:

> How many people within your organization use mobile computing devices, such as laptops, Blackberries, and other types of Personal Digital Assistants (PDAs)?
>
> What have you told them about how to properly secure these devices?
>
> Do you simply rely upon having published a policy about this topic?
>
> Have you gone a step further and actually trained them about how to secure these highly vulnerable mobile goldmines of information and access paths into your network?
>
> Do you provide ongoing awareness to your mobile computer users about how to properly secure them?

## The Risks Are Increasing

Incidents involving mobile computing devices and storage media in the past few months seem to make headlines daily. The following list highlights just a few of the many recent stories of lost or stolen mobile computing devices and storage media:

> On April 16, 2006, it was reported that a computer disk—as well as the computer holding the disk—containing confidential information about Vancouver's Fraser Health Authority (FHA) employees and their participation in counseling services was stolen in March from the Vancouver office of the Employee and Family Assistance Program (EFAP) run by the Vancouver Coastal Health Authority.
>
> On March 28, 2006, Mercury News reported that since January 2005, Palo Alto, California police received 65 reports of stolen laptops. The trend appeared to be stealing the laptops from rental cars outside upscale restaurants.
>
> On March 21, 2006, Hewlett-Packard employees were told that Fidelity lost a laptop containing unencrypted information about 196,000 current and former HP employees; the laptop was stolen on March 15.
>
> On March 16, 2006, a San Francisco finance manager was stabbed and his laptop stolen in a Mission District café.

On March 15, 2006, it was reported that an Ernst & Young employee had a laptop containing unencrypted personal information for thousands of IBM's current and past employees stolen from his/her car in January.

On March 13, 2006, two laptop computers were stolen from the campaign headquarters of Oakland, California mayoral candidate Ignacio De La Fuente.

On March 1, 2006, the Toledo Blade reported a man was arrested in San Jose, California in connection with the theft of digital records for a medical group. One of the stolen DVDs contained clinic visit records for almost 200,000 patients.

On February 28, 2006, a laptop was stolen from the car of the Vermont State Colleges' chief information officer (CIO). It contained 6 years' worth of personal information about as many as 20,000 to 50,000 faculty, staff, and current and former students of Lyndon State College, Johnson State College, Castleton State College, Vermont Technical College, and the Community College of Vermont. The information included unencrypted names, addresses, birth dates, and Social Security numbers.

On February 25, 2006, it was reported that an Ernst & Young laptop was stolen from the car of one of its employees. The laptop contained unencrypted personal information for an undisclosed number of its customers, including Social Security numbers. In an ironic twist, one of the customers was Sun Microsystems CEO Scott McNealy, who was quoted a few years ago as saying "You have no privacy. Get over it."

On February 23, 2006, the Sacramento Bee reported a laptop containing health information for 1746 clients of CARES, a Sacramento HIV/AIDS clinic, was stolen during a home burglary.

On February 9, 2006, four Ernst & Young laptops were stolen from the unattended conference room where they were left over lunch.

On February 1, 2006, Eweek reported that discarded printouts containing personal information were thrown into a dumpster, and subsequently were used to wrap fish at an outdoor market.

On January 26, 2006, it was reported that an Ameriprise Financial laptop containing clear-text information, including names and Social Security numbers, for 225,000 clients was stolen from an employee's car at an undisclosed location out of state.

On December 31, 2005, an employee of the Providence Health Systems in Seattle reported computer backup tapes and disks containing information about 365,000 patients were stolen from his car at his home. The data was not encrypted. The tapes and disks were taken home by the employee for off-site storage.

On December 15, 2005, a Deloitte & Touche employee left an unencrypted CD containing the personal information about 9000 McAfee employees in an airline seat pocket.

## Mobile Computing Devices and Storage Media are Threats to Business

According to Laptopsecurity.org, in 2005, more than 1.5 million vehicles in the United States were broken into and had items stolen from them; 100,000 of these items were laptops, which means that more than 270 laptops are stolen from cars every day in the U.S.

The threats to information security created by mobile computing devices and storage media are real:

> According to Enterprise Strategy Group, 68 percent of computer administrators indicated laptops represent the biggest risk for the loss of confidential information.
>
> According to the FBI, 97 percent of stolen computers are never recovered.
>
> According to Safeware Insurance, more than 600,000 mobile computing device thefts occurred in 2004, totaling an estimated $720 million in losses and an estimated $5.4 billion in theft of proprietary information.
>
> According to a 2005 Pointsec study, one-third of organizations report that removable storage media is used within their company without authorization.

Just because the data may be "difficult to interpret," as company representatives often are quoted when asked about the loss of their laptops or storage devices, if the software used with the data is widely available, the data will likely be very easy to access. You must also consider that even though fraud or identity theft does not occur right away with the lost or stolen data, it does not mean that all is well. Smart thieves are good at doing their dirty deeds in ways that are difficult to notice, and they often wait what they consider is a safe amount of time before using someone else's personal information for their personal gain.

## Mobile Computing Device Self-Assessment

Consider giving your mobile computer users the following short self-assessment, one of many I have created and used, as one of your many ongoing awareness activities. Put this online to not only allow each individual an easy and convenient way to take it but also enable you to compile the results and determine where you need to beef up your mobile computing security efforts. Provide feedback to each of the answers based upon your own organization, policies, and procedures. I have provided some examples of the feedback you could use, but be sure to modify it to meet your own organization's needs. Also consider including some descriptions of actual incidents within your feedback to make it more interesting. Allow for each individual to take this assessment anonymously to encourage him or her to provide the most honest answers.

### *Sample Online Self-Assessment*

For each of the following questions, choose all the answers that apply to you. Please answer honestly; your responses will be anonymous, and they will help us to more successfully and efficiently implement ways to protect the personal and sensitive information stored on mobile computing devices, such as a laptop, Blackberry, PDA, and so on, as well as on mobile storage media, such as DVDs, CDs, USB thumb drives, backup disks and tapes, and so on.

1. Which of the following ways do you use to protect confidential information on your mobile computing devices and mobile storage media?

   a. Encrypt the data using a strong encryption solution provided by the organization

   b. Encrypt the data using a scrambling method developed by you or someone else in-house

   c. Use a login password

   d. Use a BIOS/boot password

   e. I don't do any of these things; I didn't know I needed to

   f. I don't do any of these things; they are too difficult to do and slow me down

   g. I don't know whether any of these things are done or not

   General feedback (remember, you need to expand upon these to fit your own organization) for each of the chosen answers:

   a) This is great! You are following our corporate policies. There are other actions you need to do, such as using passwords in addition to using encryption, as per policy.

   b) You are on the right track by trying to make the data unreadable, but using proprietary scrambling methods can be easily defeated. Use the corporate encryption solution to most effectively secure your data and to be in compliance with corporate policies.

   c) This is one very good component of overall data security for mobile devices and follows our corporate policy. Be sure you also use it in conjunction with encryption.

   d) This is very good. Using a BIOS, or boot, password is one of the layers of security you need to protect the information on your mobile computing device. See the corporate policy for other ways in which you need to be protecting the data on your mobile devices.

   e) Many significant incidents have occurred with mobile computing devices and storage media. It is critical that you take appropriate measures to protect the data on your devices. You should use boot and login passwords in addition to encrypting the data. See the corporate policy for details.

f) Yes, some security measures do seem to make it a little more difficult to use your computer or storage media. However, we have worked hard to implement technologies that are as easy and transparent to use as possible. Please contact the Information Security department if you are having trouble implementing encryption or setting your passwords. You can also see the "Mobile Device Encryption and Password FAQ" we have on our information security knowledge portal. Using passwords and encryption on your mobile devices is not only important for protecting our business and the data we are entrusted to protect but also required by our corporate information security policy, which you can also find on our information security knowledge portal.

g) The Information Security team can help you determine whether you are using encryption or passwords on your mobile devices. You can also see the "Mobile Device Encryption and Password FAQ" and the corporate "Mobile Computing Device and Storage Media Policy" on our information security knowledge portal.

**2.** In which of the following ways do you physically protect your mobile computing devices and mobile storage media?

a. Keep the mobile computing device and storage media out of view of others

b. Carry the mobile computing device and storage media with you at all times

c. Lock your car when leaving the laptop in it

d. Use something other than a recognizable laptop case, such as a padded backpack, travel bag, or tote bag.

e. Use a cable to secure your mobile devices when leaving them in an unattended location

f. Ask someone to watch it for you in public areas, such as the airport, while you go to the snack bar or restroom

g. None of the above

General feedback (remember, you need to expand upon these to fit your own organization) for each of the chosen answers:

a) Keeping your laptop out of view is a good start. How you keep it out of view is a crucial factor in keeping it secure. For example, leaving it in your car seat and just covering it with a today's advertisement insert is NOT good security practice. See the "Mobile Device Physical Security FAQ" and the corporate "Mobile Computing Device and Storage Media Policy" on our information security knowledge portal for more details about this.

b) This is a very good practice. Keeping your mobile devices with you is one of the best ways you can physically secure them. This is particularly important in airports, restaurants, conferences, and other public locations where many people are milling about.

c) Although it is good you lock your car, is also very important where you keep your mobile device within your car. Do not leave it where it is visible from outside the car…and covering it with newspapers is not an acceptable way to hide it! Put it in a container that does not make it apparent it is a mobile computing device, and lock it in your trunk or glove compartment if you absolutely have to leave it in your car. Many laptop theft incidents have occurred in people's cars parked right by their own homes. The best practice is to take the mobile computing device and mobile storage media with you.

d) It is a great practice to use something other than a recognizable laptop case, such as a padded backpack, travel bag, or tote bag. Doing so helps to keep you from becoming a target of thieves looking for computing devices.

e) Using a cable is a good way to secure your mobile devices when you have to leave them in an unattended location, such as within a hotel room or in a meeting room. It is best, however, if you take the mobile computing device with you.

f) Ooh…this one is risky. If you ask just any stranger sitting close to you to watch it, as many people do, you run a very large risk of having your device and the person gone when you return. If you ask your trusted friend, family member, or business colleague, this is an acceptable practice; the key to this is that you can actually trust them to keep their eye on your stuff and not get distracted.

g) Yikes! If you are outside the corporate facilities, you are putting your mobile computing devices and storage media at great risk. See the "Mobile Device Physical Security FAQ" and the corporate "Mobile Computing Device and Storage Media Policy" on our information security knowledge portal for more details about this, or call our Information Security team to discuss.

## Ongoing Awareness

There are many more types of questions that you can use on an ongoing basis to keep information security issues in the minds of your personnel. I wanted to provide you with just a couple, though, to get you going.

Such short, two- to three-question self-assessments provide a non-intimidating way in which you can effectively raise awareness of information security issues within your organization and help lessen the probability of incidents occurring from personnel mistakes or lack of knowledge. Additionally, doing such activities will address the many regulatory and legal requirements for providing such ongoing awareness. You can either make these self-assessments mandatory or you can motivate personnel to take them by offering prizes, such as a restaurant or bookstore gift certificate, for participating. This can be done in such a way that anonymity is preserved.

## Protect Your Mobile Computing Devices and Storage Media

There are many actions organizations need to take to protect the mobile computing devices, storage media, and the data stored upon them. The following is a long laundry list of some precautions for you to take, as appropriate and applicable to your organization:

### *Awareness and Training*

Train your personnel and provide ongoing awareness messages regarding how to appropriately secure mobile computing devices and storage media. Make sure they know how to protect their mobile computing device passwords.

Do not allow mobile computing devices to be shared; this is a train wreck waiting to happen. Shared devices eliminate responsibility for the device, and everyone using it assumes someone else is protecting it.

Communicate personnel's responsibility for the security of mobile computing devices and storage media. Implement a clearly written and well-communicated policy outlining personnel responsibility and have each person indicate in some form (written or electronic) their understanding of this policy and their agreement to follow it.

Require personnel to store only the minimal amount of data necessary on the mobile computing devices and storage media. Many well-publicized incidents have occurred with laptops containing information about hundreds of thousands of people.

### *Physical Protection*

Require personnel to keep their mobile computing devices and storage media with them at all times while they are away from your facilities. Tell them not to leave the devices in cars, unattended meeting rooms, and so on. There are portable safes you may want to consider using, based upon the risk involved with your travelers who are carrying your sensitive information.

Provide physical security mechanisms, such as locks and cables, to personnel who take mobile computing devices away from your facilities.

Consider installing motion sensors or alarms on your mobile computing devices. The last thing a thief wants in a populated area is to have a 110 or more decibel alarm bringing everyone's attention to him or her. Of course, you need to train your personnel how to use them so they don't accidentally blast their own eardrums.

### *Policies and Device Management*

Maintain an inventory of all your mobile computing devices and storage media and the people who are authorized to use them.

Use tracking labels and tags on all mobile computing devices and storage media.

Implement policies for the appropriate and acceptable use of mobile computing devices and storage media.

Document the software allowed to be used on mobile computing devices.

Establish backup procedures and tools for mobile computing devices.

Implement procedures to effectively and completely remove all corporate data from mobile computing devices when the person using it leaves the organization—if you have allowed personally owned devices to be used.

Do not allow mobile computing devices and storage media to be used for personal use.

Do not allow employee-owned mobile computing devices and storage media to be used for business purposes or storing business data.

### *Encryption*

Require all confidential and personal information stored on mobile computing devices to be strongly encrypted.

Require all the data on mobile storage devices, such as USB sticks, to be encrypted.

Provide the encryption software to your personnel, and provide them with training about the importance of using it.

Use encryption for data transfers from mobile computing devices. Never send/receive sensitive data over a wireless link unless another more secure end-to-end encryption technology is also being used. Mobile devices that retain company sensitive information must implement a form of a company's standard encryption to safeguard such information.

### *Data Issues*

Do not allow entire databases containing personal information to be stored on mobile computing devices. If personal data is necessary, use only the records the end user truly needs for business purposes.

Do not allow real personal data to be used for demonstration purposes, particularly on mobile computing devices.

Do not allow real personal data to be used for test and development purposes. Not only does this present great risk to the data, it is also against data protection laws in some countries.

### *Miscellaneous Technology Protections*

Require a software firewall to be implemented in all mobile computing devices.

Require malicious code protection software on all mobile computing devices, including a procedure to ensure that the software is maintained and up to date.

Implement a user identification and password authentication mechanism on all mobile computing devices to control user access to the systems.

Require a boot/BIOS password for all mobile computing devices.

Password-protect the systems administrator's account and root accounts on all mobile computing devices.

Also require a login password for all mobile computing devices. The more roadblocks you can establish for preventing unauthorized use of a mobile computing device, the better.

Implement procedures to ensure operating system (OS) updates will be installed in a timely matter on all mobile computing devices.

Implement procedures to disable all unused or unnecessary services on mobile computing devices.

Install and activate an inactivity timer or automatic logoff mechanism on all mobile computing devices.

Require wireless connectivity features (for example, 802.11, 802.16, Bluetooth) on all mobile computing devices to be set at the strongest level possible.

Establish procedures to update all spyware software on mobile computing devices with the same frequency as the organization's non-portable computers.

Disable file sharing on all mobile computing devices.

Enable auditing and logging on all mobile computing devices.

Disable displaying the last user logon name/ID.

Implement technology to allow you to destroy the data remotely if the mobile computing device or storage media is stolen or lost.