





ENHANCING MOBILE SECURITY

LEARN HOW TO AVOID POTENTIAL
THREATS WHEN YOU ARE ON THE ROAD.

BY JEFF BEARD

ILLUSTRATION BY BRIAN ROOD
WWW.BRIANROOD.COM

These days, mobile computing seems to epitomize the clever quote, “No matter where you go, there you are.” We create, edit, read, reply, attach, print, fax, instant message, text, talk, meet, greet, link, file, blog, upload, download and conduct business on-the-go by all kinds of technological means. That is a lot of data whizzing around outside the firewall, using a wide variety of mobile devices: wireless laptops, cell phones, e-mail, personal digital assistants, smartphones, thumb drives, universal serial bus and optical storage, Internet storage, public PCs and more.

It’s not difficult to imagine what could happen if just one of those devices containing sensitive information was compromised. Indeed, some news headlines have provided good examples, and disclosure of confidential information, private or public embarrassment, and potential loss of clientele are just the tip of the mobile risk iceberg. In one reported case, for a mere \$15.50, a Seattle computer consultant picked up a BlackBerry on eBay that contained high-level e-mails, names, addresses, phone numbers and transactions relating to Morgan Stanley, its clients and executives worldwide, as well as the seller’s personal financial information. The seller was a former vice president of mergers and acquisitions at Morgan Stanley. His e-mail account was closed, but much of the data still resided on the device. He simply didn’t know data could remain on a device long after he removed the battery.

With such a wide range of mobile devices and varying levels of user knowledge, how can we keep data and systems, and ultimately our organizations and clients, safe? It’s important to recognize that security is a process, not a product. Yes, various security products can be installed and configured to enable security features. However, the underlying processes need to be sufficiently understood to make that security a reality. Thus, it’s a mix of effective products and procedures, along with a security-minded culture and education that often supports a quality security approach.

The following guide offers some ideas and suggestions for reducing risks associated with mobile computing. Keep in mind that security always entails a balancing act between empowering authorized people to use it effectively and restricting unauthorized or undesired actions. Often, the human element can be the weakest link in the chain. Training might be required to use some of these security tools. Other ones work quietly behind the scenes. It’s key to design and implement a usable security program – one that provides excellent protection but doesn’t prevent its users from accomplishing necessary business tasks – a very delicate balance indeed, open to many debates.

Here is a look at the various mobile security risks and ways to minimize them. Most effective security strategies focus on the fundamentals because if the fundamentals are not suitably addressed, all the bells and whistles will not do you much good.

LAPTOPS AND TABLET PCS

Generally, laptops are the workhorses of the modern knowledge worker because you can do just about anything from everywhere with them. But therein lies the security challenge. Consider the following three items to be the trifecta of basic laptop intrusion security.

- **Software firewalls.** The ever-important software firewall blocks intrusion attempts when working outside the firm and serves as a second layer of protection when working behind the corporate hardware firewall. Some firewalls even can detect and prevent spyware and other malware from “phoning home” from the laptop. This is absolutely essential when accessing the Internet from any public network, particularly via Wi-Fi at hotels, conference centers,

coffee shops, airports and more. Even more helpful is the ability to receive new firewall updates as circumstances require because new exploits constantly are evolving.

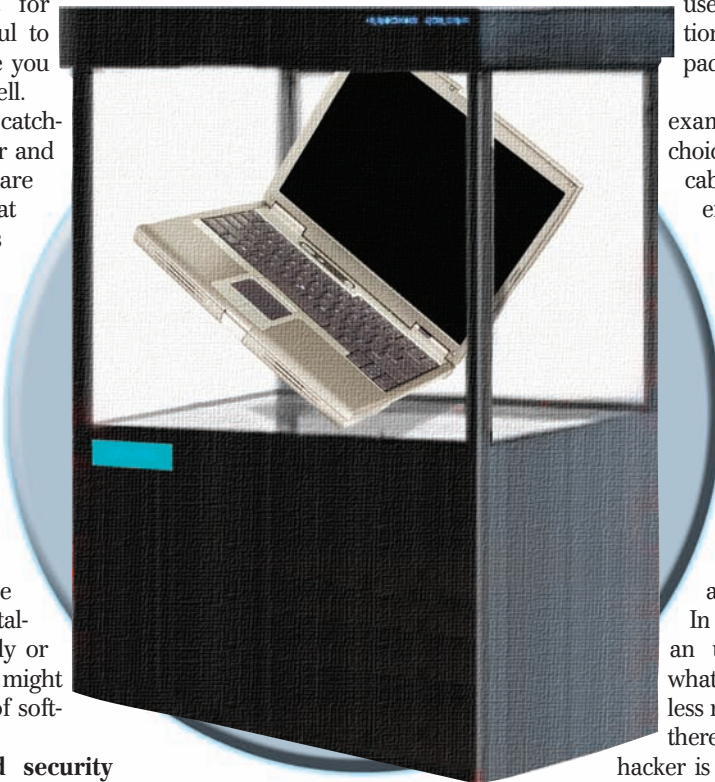
- **Antivirus software.** Another essential element of practicing safe mobile computing, antivirus programs act like the immune system for your PCs. They fight off infections as they occur, and sometimes help to prevent others. But the antibodies are only as good as the last update, so it's key to have them auto-update frequently. That is good while you are in the office, but for extended trips, it's helpful to have them updated while you are out of the office as well.
- **Antispyware.** This is a catch-all program that scans for and removes adware, spyware and other malware that firewall and antivirus programs might not have detected.

The following group of items also are important to maintain laptop security.

- **Limited or no local administrator rights.** If the user doesn't have the privileges to install software locally, then it also could thwart some unauthorized malware installations, either intentionally or unintentionally. It also might ease the administration of software license tracking.
- **Operating system and security patches.** New software flaws are discovered almost daily. Many are the result of poor software coding, and hackers are quick to exploit these weaknesses. Your Information Technology staff should be managing this for you. If you are a solo or small firm attorney and don't have IT staff, then visit www.windowsupdate.com to scan your PC and download the necessary security patches.
- **Pop-up and content blockers in Web browsers.** Often, malware gets installed without a user ever knowing how it got there (at least that is the user's official story). With some browsers, notably Internet Explorer, some sites can engage in

drive-by downloadings of adware and spyware. While nothing seems to stop all pop-ups and active Web site content, using a decent pop-up blocker can prevent some of these miscreants from jumping aboard. Some newer browsers already include pop-up blockers.

- **Disable print and file sharing on Internet connections.** This is critical to help prevent intruders from gaining access to your files when you are online.
- **Utilize a virtual private network solution.** A VPN uses software



installed on the PC to encrypt network transmissions between the PC and your office network. This makes it more difficult for anyone to intercept and decode sensitive information.

DEALING WITH MOBILE WI-FI SECURITY RISKS

Wi-Fi computing is ubiquitous and convenient, but it presents some of the most challenging security risks: easier and anonymous hacking, reduced security, hijacking of signals and access points, and more. Proper configuration of the Wi-Fi

client software is critical. First, it's important to restrict Wi-Fi connections to use access points only in *ad hoc* mode. This prevents riskier peer-to-peer connections, particularly when the user often is unaware of the difference in connections.

One of your best forms of defense is using encryption. Install and train your staff on how to use a VPN solution, particularly since most public hot spots don't use encryption (for ease of access). Show staff members how to employ Wi-Fi encryption when using home wireless networks. Also, educate them on the importance of accessing secure Web sites that use Secure Sockets Layer encryption (indicated by the little golden padlock in your browser).

User education is key. For example, consider the end-user choice of a hotel network. In-room cabled Ethernet connections generally are more secure than Wi-Fi, the latter of which easily can be hacked by other guests in surrounding rooms.

Be aware of one of the newest risks in wireless computing: look-alike Wi-Fi networks. A hacker basically sets up a Wi-Fi network signal near a legitimate one. The hacker's signal is stronger and uses the same network name to overpower and replace the legitimate one.

In a hotel or coffee shop setting, an unsuspecting user then sees what appears to be the proper wireless network and jumps on. Because there isn't any Wi-Fi encryption, the hacker is free to snoop and gather a lot of confidential information, particularly if the mobile user isn't using other forms of encryption such as SSL or a VPN.

PDAS, SMARTPHONES AND BLACKBERRYS

The smaller the device gets, the easier it is to lose. Many of these types of devices already are pretty small, wireless and can contain a lot of sensitive e-mails, attachments, calendar items and contact information. They can be secured by employing a combination of:

- Passwords to prevent easy access if a device is lost.
- Automatic lockout after "x" amount of time or other conditions.

- Remote wiping of data. A user can call his or her IT support, report it stolen or lost, and the information can be wiped remotely from the device via a wireless connection. If the device isn't located in a wireless coverage area, the wipe command takes effect when it's brought into one. Another option is to wipe the device after "x" number of invalid login attempts.
- Strong encryption of stored and transmitted data.

One or more of these security precautions could have prevented the BlackBerry eBay incident previously mentioned.

Also, disable infrared, Bluetooth and Wi-Fi when it isn't needed. All three are relatively short-range wireless technologies, which means the intruder needs to be in relative physical proximity. Many devices leave one or more of these modes on all the time, which means the device can be hacked simply by carrying it around when it's turned on. Bluetooth

confidential information being hacked and distributed — all with the user completely unaware it occurred until it's too late. The best way to prevent this is to turn off Bluetooth altogether, or at least turn it off when it isn't in use. This also will save battery life. If Bluetooth is needed regularly, say for a hands-free headset, configure the device so it isn't in "discoverable" mode. This makes it more difficult for others to hack it, but it doesn't provide an absolute guarantee of security.

Because small devices are easy to lose, attempt to keep the data in sync with another data source so you have a backup. BlackBerry devices and similar gadgets are backed up on your mail server and related enterprise servers. Many cell phones either come with or have the option to sync to a PC via a data cable and syncing or backup software. By using these features, you still will retain important phone numbers and other information even after the phone is long gone. Syncing the data back to a replacement device usually is a lot easier than manual entry and re-creating lost data.

PHYSICAL SECURITY

Laptops, PDAs, cell phones and flash or thumb drives are lost all the time. By using local encryption on devices that support it, the data remains safer than leaving it in plain text. A number of flash drives now come with encryption software and even built-in biometric readers (e.g., fingerprint readers).

Consider storing your portable devices in a hotel room safe when you are out of the room. Use a security cable such as the Kensington Microsaver and the shrieking Targus DefCon alarm. No lock is unpickable, but it adds another layer of security.

Also, keep your devices and laptop bag close to you at all times in airports and other busy locales. Even the type of laptop or mobile gadget bag you carry can increase your risk of theft, particularly if the bag obviously is a laptop bag. Consider more nontraditional bags as a psychological, if not a physical, deterrent.

PUBLIC PCS

Unless you are surfing for fun or accessing nonconfidential information, just say "no" to public PCs, which often are compromised and infested with garbage. It's fairly common for public PCs at hotels, airports, coffee shops and other locations

to have trojans, adware and spyware installed. Even if you access sites with SSL encryption, a keylogger can still record the site addresses visited, your login names and passwords, and transmit them to another location without you knowing. If you absolutely must use a public PC to access secure information, then be sure to change your password the first chance you get from a secure and trusted PC.

HOME COMPUTING

It used to be that IT departments didn't even want to think about supporting home computer environments because they were not the firm's assets or under the firm's control. In today's world, threats encountered at home easily can make their way into a corporate network and *vice versa*. Neighbors and wardrivers (those who search for Wi-Fi wireless networks by automobile) can compromise home networks and their data via wireless and cable networks. Think of the data someone might access or share between work and home.

An improvement to corporate security can be an outreach program to alert users to home network best practices. Some of the issues are similar to mobile PCs covered earlier. It's helpful to emphasize best practices through the use of hardware and software firewalls, antivirus software and frequent updates, and antispyspyspyspyspys software. Use a VPN solution to connect to the office and encrypt the data once it leaves your home. (In comparison, Wi-Fi encryption only encrypts the data between the PC and the wireless router, so both are highly recommended.) To make sure you have a secure wireless network:

- Enable the highest encryption possible, such as Advanced Encryption Standard over Wi-Fi Protected Access rather than the much weaker Wired Equivalent Privacy protocol, which is more commonly broken. This helps keep wardrivers and curious neighbors at bay.
- Change the Service Set Identifier name (i.e., network name) and disable its broadcast.
- Change all the default router passwords to strong passwords of at least eight characters, with a mix of case, letters, numbers and special characters.
- Enable Media Access Control address filtering.



phones are particularly notorious for this. Techniques known as bluesnarfing, bluejacking and bluebugging have proliferated. The Paris Hilton phone hacking incident is a good illustration of what can happen with personal and

- Limit the number of allowed connections to the number of home PCs.
- Run the network as a pure “g” environment (no legacy 802.11b devices), if at all possible.
- Disable the router’s remote management feature to protect outsiders from gaining access to its settings.
- Place the wireless router away from outside walls to limit the signal leakage outside the home.
- Change all router passwords and other security information on a regular basis.
- If your router supports “isolation,” consider enabling it to prevent wireless PCs from “seeing” and communicating with each other.
- Limit file and folder sharing.

BACK UP

No matter how careful you are, odds are sooner or later you will encounter a problem while mobile. Although not technically a security measure, having a good data backup system can help rescue your information in a bad situation. While portable USB hard drives and CD burners are great backups, they are not secure if they are not encrypted. If they are lost, anyone can view the contents with another computer and have a field day with your data.

Secure thumb drives present a fairly convenient and reasonably secure mobile backup solution. Internet backup services can be convenient and tempting, but you should consider their overall security (*i.e.*, Do you really know how secure their service is?), as well as their terms of service and legal obligations should something bad happen. Also, consider whether your data is encrypted during transmission.

POLICIES AND USER EDUCATION

No security discussion would be complete without covering policies and education. These include employment, usage and more. A corporate network and Internet use policy is fairly common in law firms these days. However, there still is some spirited debate as to whether an organization needs specific policies to address various types of technology uses. For example, some companies have policies outlining the use of and restrictions on instant messaging, Internet chat, e-mail and blogging. Proponents of such policies cite the benefit of having expressed

more clarity in the guidelines, as well as specific examples of what to do and what not to do.

Some critics are quick to point out that this approach lends itself to creating just as many questions as answers. For instance, if you have a policy restricting certain activities in Internet chat rooms, then do you need to create one to address instant messaging, cell phone text messaging and each subsequent technology as it’s developed? That could make for a lot of policies and duplication of work. Also, with respect to blogging, is the firm regulating the employee’s speech and behavior at the office or on personal blogs updated from home as well?

An alternate approach might be to craft usage and confidentiality policies broad enough to encompass a wide variety of online activities, which provide a reasonable amount of flexibility and comfort room for the employer and employee. The downside to this approach is the potential uncertainty in its application on a case-by-case basis.

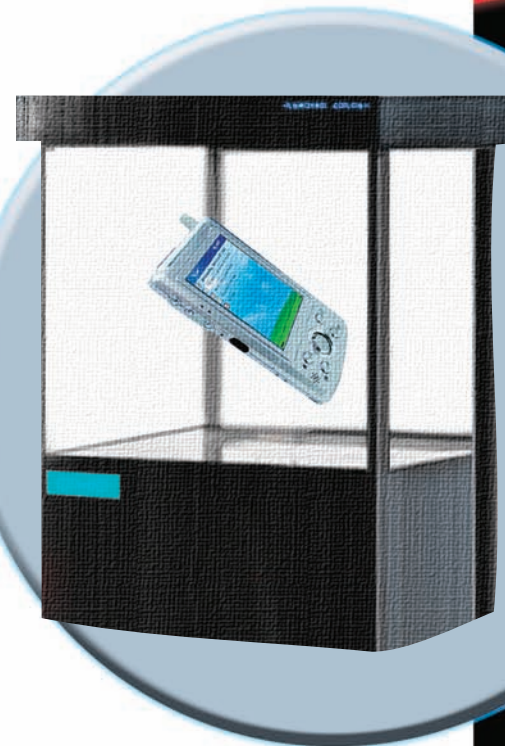
The goals of any good security policy should include setting clear expectations regarding the:

- ownership of the firm’s systems and data;
- right to monitor employees’ activities and employees’ consent to do so;
- underlying reasons to protect the organization, its employees and its clients;
- penalties for noncompliance with the policy, and employees’ rights and responsibilities; and
- devices allowed into the facilities and allowed to be supported (*i.e.*, Do you allow camera phones to enter at all, or restrict their usage in non-public areas? Do you lock out USB devices such as thumb drives and iPods to protect against data theft? Do you allow guests to connect their devices and log in to your network?).

Even the best policy will have limited effectiveness if exceptions are regularly made for privileged users. Don’t kid yourself that others will not find out. The tone should be set from the top down that these are necessary and important requirements to be followed. After a policy has been crafted, consider holding training sessions using everyday examples so your users understand how

to properly use various security features and comply with the policies.

Even stressing the return of the organization’s equipment upon employment



separation is key. There probably are more than a few PDAs, cell phones, laptops and thumb drives floating around with company data “borrowed” from employees long gone.

Mobile computing is fun, convenient and productive. Just remember, security is a process. It takes the combined and coordinated effort of IT, business management and the end users to provide a reasonably effective and secure environment. As we are likely to see many more forms and numbers of mobile devices, security is very much an iterative process. Plan on reviewing your security plans and policies on a regular basis. Perhaps most challenging is the need to align them and provide balance with the business needs of the end users. While it can be daunting to craft protections and policies for all these risks, it’s not impossible, and it can be established in baby steps if needed. **.loc**

Jeff Beard is the legal services Information Technology manager with Caterpillar Inc., a Fortune 100 company headquartered in Peoria, Ill. He is a former practicing attorney, and is a frequent national author and presenter on contemporary legal technology and practice management issues. This article was submitted in his individual capacity, and does not necessarily reflect the views of his employer.