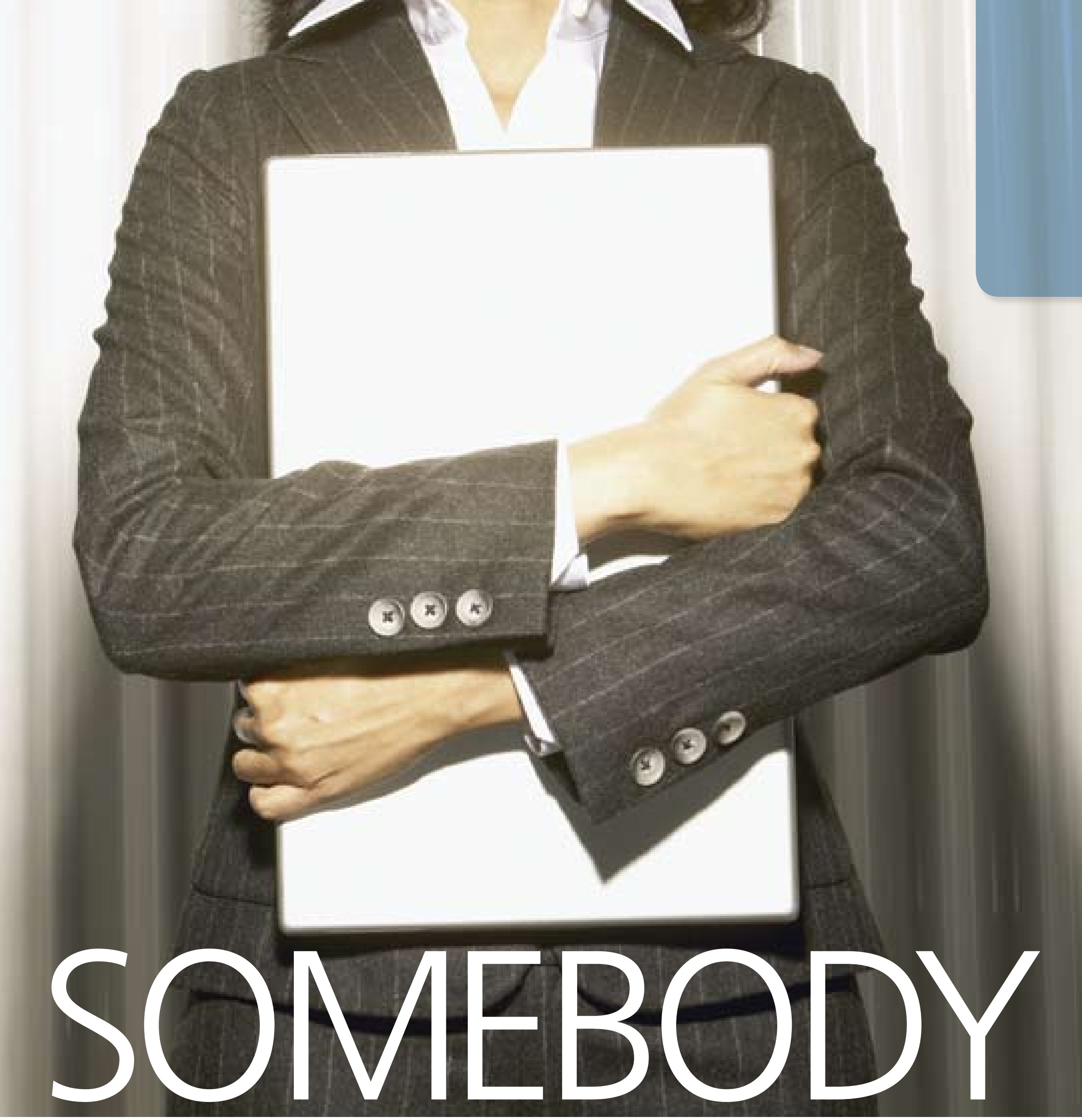

SOMEBODY Call Security

Implement a reliable strategy to protect your mobile devices and the data they carry.

If a notebook computer — or even a CD-ROM, flash drive or backup tape — containing private or sensitive data gets stolen or lost, the cost of the incident can be a lot more than simply replacing the hardware. This is especially true if your company didn't take the right precautions ahead of time.

"It costs about $35 a head to notify people their confidential data may have been compromised," states Jack Gold, founder and president of strategic technology consulting firm J.Gold Associates. "And if you have to pay for a follow-up credit report, that can be another $10 or so per person."

So, for example, one stolen notebook with 200,000 records could cost a business nearly ten million dollars. Plus, Gold adds, there's the cost of the negative publicity along with lost sales. "And that's not even considering things like fines from the Federal Trade Commission."

Notebook computers and removable media such as CD-ROMs and USB flash drives — a.k.a. "mobile data at rest" — make it increasingly easy to take company data outside of the office.

Unfortunately, taking sensitive data outside the front door and the network firewall makes this data more vulnerable to theft or loss. An estimated 35,000 to 40,000 notebooks are stolen annually, according to Richard Sanders, president of security accessory firm Compu-Lock.

An estimated 83 (or more) million records have been lost or stolen since February 2005, according to Privacy Rights Clearing House. Many of these were due to network breaches, hackers, inside jobs or other causes. However, a substantial number were due to theft or loss of notebook computers or removable media.

One of the most publicized incidents has been the May 2006 theft of a notebook brought home by a U.S. Department of Veterans Affairs analyst, which had personal data of 26.5 million U.S. veterans on its hard drive.

Other incidents, just from the month of June 2006 included the following:

- The Federal Trade Commission reported theft of two notebooks, containing personal and financial data, from a locked car.
- An Ernst & Young auditor's notebook, containing credit card information of Hotels.com customers, was stolen.
- The NY State Controller's Office lost a data cartridge with payroll data for 1,300 state agency employees.

Most stolen computers are likely to be reformatted or salvaged, without the data ever looked at or misused. And stolen mobile media is often reused or thrown out. For example, the Department of Veterans Affairs notebook was reported found in June. Initial FBI forensic tests did not indicate that data on the notebook and disk had been improperly accessed.

But if appropriate precautions to restrict access to this mobile data at rest had not been taken, the agencies or companies would still have to deal with the possibility that this data may be misused. For example, if the incident falls under the jurisdiction of California or any other state with a disclosure law, the company has to alert all potentially-impacted parties.

There are two main types of mobile device security: on-device security and mobile networking security. Here are some steps IT can take to help employees ensure that any data and mobile computers they take out of office are secured to minimize theft or loss, and secure any data from prying eyes.

On-Device Security

Obviously, it makes sense to take precautions to minimize thefts and losses. But accidents and incidents happen even to the most cautious users.

One reason is that devices and media are getting smaller, while simultaneously increasing in capacity and capability. Apple iPods, for example, can have hard drives sized to 60GB — as big as many of those on older notebook computers.

Cell phones, flash drives and DVD disks can easily hold a gigabyte or more of data. And most of today's cell phones and handhelds have enough computer power to make them vulnerable. They can also be carriers for viruses and other forms of malware.

As is the case with most computer and network security, protecting mobile devices and storage includes a combination of authentication and encryption.

Authentication — In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

Authentication means using a password or some other identifying approach, like biometrics — a fingerprint, or even a voice phrase — or a "token" such as a smartcard or an RSA Security "key" containing an authorizing code. For extra security, many experts recommend "two-factor" authentication, such as a password plus a smartcard.

Most notebook computers, handhelds and cell phones include password-protection options. Notebook computers may offer passwords not only at the operating system level, but even at the BIOS level. Plus, there are a number of third-party authentication software and hardware tools available from companies including PGP, RSA Security and Sybase.

However, "Don't count on passwords alone to protect data on hard drives," notes Chris De Herrera, PocketPC FAQ site manager and mobile expert. "XP passwords can be gone through. Someone can crack the ADMIN account with SysInternals or a Linux boot CD. Or they can remove the drive and plug it into another machine as a 'slave drive.'"

Also, De Herrera points out, device passwords won't protect data on removable media — CD/DVD-ROMs, USB flash keys and so forth. So the next step is to also use encryption on a file, folder or partition basis — encoding data so it's not stored in "cleartext" that anybody can read if they open the file.

Encryption — Today's desktop/notebook computer operating systems including Microsoft Windows XP, Apple Mac OS X and Linux feature options to encrypt folders or entire partitions, ▸

with a password or key required by the encryption mechanism to decrypt a file.

With Windows XP's Encrypting File System (EFS), for example, "You can right-click on a folder, and choose the encrypted option, and be prompted for a password," says De Herrera. However, he cautions, be careful. "There's no recovery or 'back door' if you forget or lose that password."

Microsoft's upcoming Windows Vista will also offer BitLocker Drive Encryption, which, according to Microsoft, "ensures that data stored on a computer running Windows Vista is not revealed if the computer is tampered with when the installed operating system is offline."

BitLocker can encrypt the entire Windows volume. Users will either need a startup key (PIN number) or USB flash drive with a digital key. Newer notebooks whose hardware includes the Trusted Platform Module (TPM) can be used without the key; if the TPM is missing or changed — for example, by a would-be data thief.

A number of third-party encryption tools are available for use with notebook computers, mobile devices and even removable media. PGP offers encryption software. Most versions of Zip include an encryption option. Many USB keys intended for professional use include password protection and encryption software on the drive. Others include encryption hardware on the key, and there are also encryption programs designed to be carried and used on USB drives.

Encryption not only prevents unauthorized parties from accessing your data, but also — if the encryption used satisfies regulatory requirements — may relieve your organization from the obligation to report lost data.

Managing Mobile Media and Devices

One important advantage of many third-party tools is central key management. This tool keeps copies of key information, so that if someone forgets or loses their key, or another person needs legitimate access to locked data, IT can help resolve this quickly.

"Some tools even let you have multiple keys and change keys periodically," notes De Herrera. Companies like GFI have begun to offer central management tools for mobile devices and media which can centrally manage access.

If you don't want to rely on the operating system or security software, Seagate offers Full Disc Encryption (FDE) on its Seagate Momentus notebook-sized hard drives, which can use either a static password, or two-factor authentication, such as an RSA Security token, a smartcard or biometric.

But what about data on USB keys, CD-ROMs and other removable media? A growing number of USB key vendors are including build-in encryption features. For example, Kingston's DataTraveler Elite - Privacy Edition, secures data on the fly via 128-bit hardware-based AES (Advanced Encryption Standard). RSA Security offers a USB token with a removable SD (Secure Digital) card and encryption hardware for that card. And msystems' mTrust Drive is a secure USB flash drive designed for company use.

According to Mark Rogers, business development manager, Verbatim Corp., msystems' "mTrust Manager allows corporate users to centrally manage security features such as device password policy, as well as optionally restrict the use of company-issued drives to approved PCs."

If your company uses any handhelds or SmartPhones it's also time to start securing them, advises Todd Thiemann, director of device security marketing, Trend Micro. "Predictions are that by 2009, more SmartPhones will be shipped than PCs, making them a very appealing target. So it's important to encrypt data on these devices, so Trojans and spyware can't get to them."

If your data is protected adequately, loss of data-bearing devices or media will be reduced to a manageable nuisance, rather than a major bottom-line expense. The cost per person or device will be similar to what you're spending on antivirus and other protection — and a lot less than even one lost data incident is likely to cost.

In addition to protecting stored data, you'll also want to be sure that your company's notebook computers and mobile devices are protected when they are used. Every notebook and handheld should have, at minimum, antivirus software, and if it will be used to access the company network, some virtual private network (VPN) capability.

Securing Wireless Networks

In addition to your mobile devices and data, it's also critical to secure the networking infrastructure used by mobile devices. This should help to eliminate the possibility of eavesdroppers capturing passwords or sensitive data, or breaking into the mobile device or into the company network.

WEP (Wired Equivalent Privacy), the original feature for securing 802.11 (Wi-Fi) connections, has been surpassed by WPA (Wi-Fi Protected Access), which provides better encryption, and requires authentication. WPA PSK uses pre-shared keys, and is intended for individuals or companies that can't run an 802.1X authentication server.

WPA and WPA-2 also support EAP (Extensible Authentication Protocol), which lets the wireless network work with a third-party authentication that your company may already be using, such as a RADIUS (Remote Authentication Dial-In User Service) server, according to Jason Acosta, SonicWALL presales system engineer, CDW.

However, cautions Craig Mathias, principal at the technology consultancy Farpoint Group, "WPA only secures the 'air link.' It doesn't deal with the overall problem of network security." Mathias's advice: "First, the data has to be encrypted at all times, except when it's being used by an authorized person. Second, use VPNs — SSL [Secure Sockets Layer] or IPSec [IP Security] which rely on upper-layer security rather than wireless security. And third, use two-factor authentication, not just password-encrypted channels."

To secure your company's wireless LAN environment, consider using wireless switches which reside in wiring closets or other secured areas and work with "lightweight" access points.

SonicWALL's SonicPoint G lightweight access points are designed to work with SonicWALL's fourth-generation security appliances. "The SonicPoints offer auto-provisioning capabilities and are centrally managed," notes CDW's Acosta. "The idea behind them is to have central management of a secured wireless network from one appliance."

The SonicPoints can be used to detect "rogue" access points and also offer intrusion detection/intrusion prevention capabilities. In addition to the WEP, WPA PSK and WPA EAP wireless encryption/authentication protocols, SonicWall offers it's own Wi-FiSec — IPsec over wireless, says Acosta.

Notebook computers and removable media make it increasingly easy to take company data outside of the office.

Physical Security

A determined thief can probably steal your notebook, but simple precautions will minimize opportunity. APC, Targus and other companies make a variety of computer "sleeves," briefcases, sidepacks, rollerbags and backpacks, designed to make it easy to transport your notebook and keep it with you at all times. Most of these also offer some physical protection against bumps, bounces, drops and vibration.

Most notebooks include a security port for a cable or alarm. Compu-Lock's NoteSaver cable locks use flat-key locks that cannot be easily picked or broken like circular-keys. Compu-Lock also offers cables with aircraft-quality vinyl-coated steel, in its looped-end NoteSaver Travel Cables, and for stationary use, its Office Cable product.

In addition, Compu-Lock markets a motion-sensitive alarm. "The user carries a control unit, so that if anybody else moves your bag, or picks it up, the alarm goes off," says Compu-Lock's Sanders.

General Advice for Mobile Computing

One challenge for security devices is to establish effective policies and procedures. Jack Gold, founder and president of the strategic technology consulting firm J.Gold Associates, recommends the following for maximum security when using mobile devices.

- Educate users on the importance of security and ways to avoid the loss of their mobile devices.
- Use password protection on the devices, whether built-in or third-party applications.
- Get a mobile management system to enforce data security policies for as many as possible of your mobile/wireless devices.
- Encrypt files or entire contents on devices, as appropriate.
- Enable device lockdown and "kill" functions so that, for instance, if a device does not connect to the corporate network for a specified period of time, or if it does attempt to connect after being reported missing, it automatically wipes clean the data from its memory.
- Don't let the only or primary copy of your data leave the building.
- If backups are encrypted, be sure to save the specific key, so you can access that backup; the key for a later backup may not work on older backups.
- Do an inventory of hardware components and software.

"Securing your mobile devices and data is part of the cost of doing business," says Gold. And it's bound to be cheaper than the alternative.