



**C**ompared to the notebook and Tablet PCs employees take with them out of the office and use at home or on the road, computers used at an office are comparatively easy to secure, whether against Internet threats or physical risks. However, with use of notebooks and tablets on the rise, businesses must consider additional steps to protect their assets.

“For notebook security there are usually two concerns: the confidential data on the hard drives, and the assets being out ‘in the wild,’” says Jeremy Weiss, network security specialist at CDW.

So while you can’t guarantee your employees’ notebooks or data won’t be damaged, lost or stolen, even a few easy, affordable steps can reduce the odds of something happening and minimize the repercussions that follow.

### Start With the Basics

Notebook security starts with the same security you should be providing for all the desktop computers in your company — firewalls and antivirus/antispysware software. Comprehensive applications and suites are available from McAfee, Symantec and other vendors. Operating systems, Web browsers and other applications should be configured for reasonable security (e.g. no automatic downloads and installs of ActiveX, JavaScript or Java

applets). Operating systems and all security applications must be kept up to date in terms of patches, versions and configurations.

“Firewall software is particularly critical for mobile users,” says Beth Cohen, director of operations at Broadleaf Services, a data protection services company. The firewall that comes with Windows XP is adequate — as long as you make sure it’s on, she adds — but third-party firewalls are very effective and easy to implement.

Independent security system consultant Douglas Mechaber also suggests running a host intrusion detection/prevention system for notebooks. “Mobile users should want to know every time something is trying to access your hard drive.”

In addition, IT should also set up each notebook so that access to the system, applications and files is restricted to authorized users. Access can be controlled by using passwords, biometric identification or a physical token, such as an RSA SecurID key or card. Optimal security, most experts agree, requires using a combination of any two of these.

“If you do use keys or digital certificates, good key management is essential,” says Chad Cook, vice president of information security at Lime Group, a N.Y.-based financial service firm. “Be sure your keys and certificates are stored on some removable/separate device, like a hot-pluggable USB device, and not on the notebook, or people could recover the keys from the hard drive. And be sure that IT has copies of the keys, or somebody does, in case you lose your key fob.” ▶

# Notebook Security 'In the Wild'

Keep data and networking safe from prying eyes, and minimize hardware losses.





## Secure It Before You Lose It

The cost of replacing a damaged, lost or stolen notebook can vary, depending on the circumstances and insurance policy. Less easily replaced is data on that notebook that hasn't been saved elsewhere.

"You have to have some kind of backup in place, whether it's an external USB flash drive, portable hard drive or a network-based backup, to secure a copy of the data," stresses Broadleaf's Cohen.

Even more importantly, the negative consequences of confidential data ending up in the wrong hands can be catastrophic. Last year was rife with stories in the news of lost and stolen information — tapes and notebooks with thousands, even millions of private records containing Social Security numbers, credit card numbers and other financial/identity data. "A password doesn't protect the data on the hard drive if the notebook or even just the drive is stolen," points out Cohen.

"Take the big-picture perspective. Your goal should be to centralize security because it's easier to manage dozens or hundreds of machines centrally than one at a time."

— Chris De Herrera, Mobile/Wireless Expert and Operator,  
[www.TabletPCTalk.com](http://www.TabletPCTalk.com)

The legal repercussions have increased as well. For example, California's Security Breach Information Act (S.B. 1386) requires companies that do business in California or even have customers in California must notify consumers whenever their personal information may have been compromised.

One solution is to treat notebooks as dataless workstations, storing data only on removable devices or media, and set software to not leave temporary files on the hard drive. Many USB flash drives include software that sets up an encrypted partition in the flash memory, including for temporary files created by your applications.

But if sensitive data must be put on the hard drive, it needs to be encrypted, says CDW's Weiss. "For most companies buying notebooks, we recommend encrypting all data on the hard drive."

Current operating systems include encryption utilities; for example, Windows XP supports per-file, per-directory and per-partition encryption. Mac OS X can create a virtual disk. There are also a number of third-party encryption utilities available.

At minimum, advises Chris De Herrera, mobile/wireless expert and operator of [www.TabletPCTalk.com](http://www.TabletPCTalk.com), "Use passwords on Word and Excel documents as an intermediate form of security, and encourage people to use password encryption even in zipped files."

Encrypting data does have risks, cautions De Herrera. "If you forget the password, there is no recovery. If you corrupt your hard disk, there is no recovery." Encryption can also complicate backup procedures.

## Secure Network Connections

Firewall, antivirus/antispyware software and using alternatives to Internet Explorer — such as Firefox or Safari — as your Web browser will help protect against threats attempting to break in through network connections. But it's also essential to secure any connection made between these notebooks and your company's networks, servers and users' desktop systems.

"For connecting back to your company network, use a virtual private network [VPN]," advises Broadleaf's Cohen. "Through the VPN, you can use Remote Desktop to get to your server."

If your company provides notebooks to employees, you can use IPsec (IP Security Protocol) VPNs to provide a full network connection to your company's network, allowing direct, secure access to servers, applications and files. Alternatively, you can use SSL (Security Sockets Layer)-based VPNs; almost all current Web browsers include SSL, allowing them to establish secure connections to Web servers (e.g. for mail access, or to specific Web-enabled applications). If the Web browsers on a notebook support ActiveX or JavaScript, you may be able to provide improved network-like VPN connections using SSL.

"To support VPN access to the company network, you'll need VPN software or an appliance at the company side," says Cohen. "On notebooks, you can use the Microsoft VPN client that comes with XP, or a third-party one, depending on what you have and want."

Steve Kent, chief scientist at BBN Technologies, urges companies to use VPNs not just to prevent disclosure of information sent over the VPN, but also for protection if you're using passwords to log in.

If your company uses Microsoft Exchange Server 2003, "Another way to securely access e-mail is using RPC over HTTP [Remote Procedure Call over Hypertext Transfer Protocol], which allows full Outlook 2003 MAPI clients to connect to Exchange 2003 Servers using HTTP/HTTPS," recommends James Hettrick, director of information systems for the City of Loma Linda, California. This doesn't require a separate VPN, he adds. "The notebook secures through the server." (This approach requires getting a digital certificate for the server.)

Make sure your notebook users understand that a VPN only protects the connection to the company network, BBN's Kent adds; the usual precautions must be made to protect the notebook and its data while the user is on the road.

## The Role of IT Policies

Assuring security of your company's notebook computers is best done as a company-wide effort, managed by IT.

"Take the big-picture perspective," urges TabletPCTalk's De Herrera. "Your goal should be to centralize security, because it's easier to manage dozens or hundreds of machines centrally than one at a time."


CDW's Weiss agrees. "Many of today's security software programs can be set up by an administrator with profiles adjusted for local and remote use."

Similarly, suggests De Herrera, "Set up your networks to address the needs of your mobile users. Use features like Policies, which

Microsoft provides in Active Directory, part of Windows Server 2000 or 2003, to define security settings as a set of parameters you'll enforce on every computer every time it logs on. As an administrator, you have to choose to implement these policies. And these affect everyone, not just notebook/remote users."

De Herrera also recommends using a patch management program, such as Microsoft's Windows Server Update Services (WSUS) or a third-party utility, to ensure that the operating systems and software on remote systems are kept up to date. "Enterprise customers have access to some tools that end-user versions don't include; that's one reason to consider enterprise-level software even if you're a smaller business," he suggests.

If employees in the field use USB flash drives, tokens or any portable/removable storage devices, they should keep these objects separate from their notebook when not in use — in a pocket or on a keyring, and not in the notebook carrying case. This way, if the notebook is stolen or lost, the data can still be safe. Similarly, don't keep sensitive data or passwords on handhelds.

Finally, it's important to include a testing phase when you implement security, stresses Michael Stein, president of Members Only Software, a D.C.-based company specializing in business software for associations and non-profit organizations. "Make sure passwords are being demanded, that users can access their notebook and connect remotely from outside the office." 

## Exterior Protection: The Importance of Physical Security

"For medium-sized businesses, buying notebooks ranging from \$1000 to \$2000 each can be a big expense and they want to protect it," says Jeremy Weiss, network security specialist at CDW. Sturdy computer bags and carrying cases will help protect notebooks from being banged into, dropped or knocked about. APC, Kensington, Targus, Tripp Lite and others offer a variety of options, including some as stylish as they are functional.

Basically, employees should treat notebooks like they would any valuable property. "Don't leave your notebook in plain sight in public places, especially the front seat of your car," comments Michael Day, chief technical officer at IT consultancy Currid & Company.

Alarms and cable locks are available from such vendors as APC, Kensington, PC Guardian and Targus. While these won't stop the determined thief, they'll deter casual opportunists. Newer locks that fit in the video port will make it hard to take the computer without damaging it.

To help recover computers that go astray accidentally, consider "Reward For Return" label services, such as StuffBak. "We recommend a 'PC low-jack' service that helps mitigate the risk if the unit is lost or stolen," says CDW's Weiss.



CDW offers technology service support from top manufacturers and service providers across all product categories.