

June 17, 2006

THE JOURNAL REPORT: TECHNOLOGY

Moving Targets

How companies can keep employees from losing the information in their laptops

By VAUHINI VARA

June 17, 2006; Page R9

Here's news for the mobile worker: If you lose your computer or the private data on it, the cost of replacing it could be the least of your company's worries.

Laptops, cellphones and hand-held devices are making it easier for people to work on the go. But that means those devices hold increasing amounts of sensitive company information, from financial presentations and product plans to private customer data. According to a 2004 survey by the Computer Security Institute, a group in San Francisco that provides security training, organizations experiencing laptop thefts reported costs averaging more than \$19,000 per incident, including replacement costs and reconfiguring systems and software. But many executives responsible for security say the true cost of laptop theft is harder to measure and stems from losing sensitive customer data or business plans.

On top of that, more than 20 states have enacted laws that require companies to notify customers residing in those states if an employee loses a laptop that holds customers' sensitive data. Such bad publicity can scare customers away and hurt sales.

So, what can companies do to help prevent employees from losing a laptop or the data in it? Here are six tips that security experts offer:

1) RESTRICT ACCESS. Mark Connelly, chief information security officer at Sun Microsystems Inc., gives laptops only to employees who absolutely need them and who don't work with super-sensitive data. For instance, the company's legal counsel doesn't use a company laptop even though he travels often. This employee deals with information that, if lost, could be devastating to the company, Mr. Connelly explains. "The best laptop for us is no laptop at all," he says.

Companies that must distribute laptops to employees should at least discourage or ban the use of potentially dangerous software, like programs that let users access peer-to-peer networks to download music or movies, says Stephen Northcutt, who runs security training sessions at companies for the SANS Institute, a Bethesda, Md., organization that promotes computer security. At Sun, Mr. Connelly configures laptops to make it difficult for staff to download software or change security settings themselves.

2) ENCRYPT FILES -- AND HARD DRIVES. Last year, M&T Bank Corp., a regional bank based in Buffalo, N.Y., had to mail letters to more than 1,000 customers telling them an employee had lost a laptop that held their private information. “We’re in the business of selling trust,” says John Walp, a vice president at the bank responsible for network security. “When they get a letter from the bank saying, ‘We lost a laptop that had your data,’ it doesn’t really instill confidence.”

After that happened, Mr. Walp bought software for 2,200 company laptops -- at about \$140 apiece -- that encrypts the entire hard drive, making files illegible to anyone who lacks the proper access. The company thus was better protected a few months ago when five laptops were stolen from an M&T office in Virginia. And since the laptops contained strong encryption, the company wasn’t required to disclose the theft to customers, Mr. Walp says. State laws don’t require disclosure if the sensitive data have been scrambled using special algorithms that encrypt the data over and over.

In lower-risk circumstances, it’s fine to encrypt individual files or folders. Many operating systems, including Microsoft Corp.’s Windows XP, come loaded with software that lets users encrypt files.

3) BUY REMOTE-CONTROL PROTECTION. For some companies, encryption alone may not be enough. Fremont, Calif.-based Everdream Corp. and Absolute Software Corp., of Vancouver, British Columbia, are among a few start-ups that sell software to remotely delete files.

Ron Ridge, chief information officer at Bowe Bell & Howell Scanners LLC, a maker of scanners to convert paper documents into digital format, uses Everdream’s theft-recovery technology on more than 1,000 laptops used in sales, technical support and other roles. When a thief swiped a laptop early this year, Mr. Ridge used Everdream to quickly zap the data from the laptop. When a machine is lost, the IT department notifies Everdream by fax or email. Then the next time that computer connects to the Internet, Everdream remotely distributes software to it with a command to either destroy or encrypt the data.

Privately held Beachhead Solutions Inc., Santa Clara, Calif., sells software that automatically deletes files or wipes out the hard drive unless users regularly enter a password -- say, once a week -- or if a password is entered incorrectly too many times.

4) TRAIN EMPLOYEES TO USE COMMON SENSE. Last month, the Department of Veterans Affairs said the personal information of more than 26 million U.S. veterans was stolen when an employee violated VA policy by taking the data home. That was the latest of several high-profile incidents in recent months involving stolen laptops or other devices that held private data.

Managers should institute companywide security training for anyone who works on the go -- and consequences for those who break the rules. One of the first things employees should know: Don’t ever leave your laptop out in the open. If you must leave your laptop in your car, lock it to something with a steel “cable lock,” which attaches to a slot in the PC and can be looped around a stable object. If you leave it in a hotel room, stash it in the safe. When you’re walking around with it, keep it in an inconspicuous backpack or tote bag instead of in a traditional case.

When employees travel, their company’s travel agency should grill hotels about their security practices. Some hotels require visitors to have a key to access their own hall -- added security for those who plan to leave a laptop in their room.

5) MAKE IT HARD TO BREAK INTO A LAPTOP. Require employees to use a physical smart card or key to access their PCs. Employees should also know not to save log-in information in files on a computer or, worse, on a sticky note glued to the PC itself. Instead, they should use a password that is easy to remember but long enough that it would be difficult for a hacker to randomly guess it.

Dell Inc., Lenovo Group Ltd. and others now sell laptops that come with a rectangular fingerprint scanner on the keyboard or around the edge of the screen. Turn on the PC and it flashes a screen asking you to swipe your finger on the pad. If the fingerprint matches the one you have stored in the PC, the computer boots up normally. If not, it stops.

6) WHEN YOU GET RID OF COMPUTERS, MAKE SURE THEY'RE CLEAN. Even the most security-conscious company can overlook one aspect of computer safety: Making sure a PC is secure before getting rid of it.

“People think, ‘If I delete and empty my recycle bin, that’s enough,’ “ says Sarah Hicks, a consumer-product vice president at Symantec Corp. Not so. Companies like Symantec, a Cupertino, Calif., maker of software for securing and managing IT systems, sell software that can recover accidentally deleted data. But “you can use recovery tools for malicious purposes as well,” Ms. Hicks says. The solution: Use a program that will wipe a hard drive clean for good.

--Ms. Vara is a staff reporter in The Wall Street Journal’s San Francisco bureau.