

## Firms ready to put leash on laptops

Companies expect employees to 'guard them like a wallet' to prevent theft and protect sensitive data

10:14 PM CDT on Saturday, July 15, 2006

By PAMELA YIP / The Dallas Morning News

If you use a laptop computer to do your job, you may soon have to deal with tougher security policies instituted by your IT department.

The recent rash of data breaches from stolen laptops is spurring companies to tighten policies on how employees use laptops and the information that's stored on them, say lawyers, consultants and company representatives with expertise in information technology and data security.

"The Veterans Affairs one was the one that really grabbed people's attention, just because it's so massive," said William Nolan, an employment attorney and partner at Squire, Sanders & Dempsey in Columbus, Ohio.

"We're just starting to have clients recognize the telecommuter issue and looking at, 'Are we exposing ourselves at all by allowing people to carry what they carry on their laptops?'"

Burglars stole a laptop from the Maryland home of a data analyst at the Department of Veterans Affairs in May.

The computer contained Social Security numbers and other personal data on 26.5 million veterans and military troops.

Even companies that don't deal with consumer data are paying more attention to laptop security, worried about everything from the loss of trade secrets to simply the value of the computer.

Consider:

- Boeing Co., which has experienced two high-profile laptop thefts since November, now requires employees to access most sensitive information through company servers instead of downloading the data to a laptop. Also, employees working with payroll data must use a cable lock to physically secure their laptops to a desk at all times, even during working hours.
- At ING Americas, none of the company's laptops can leave the premises until encryption software has been installed.



BARRON LUDLUM/DRC  
 Laptop security concerns range from the loss of trade secrets to the computer's value.

The move followed ING's disclosure last month that a laptop containing retirement plan information on 13,000 employees in Washington, D.C., was stolen from an agent's home.

"All laptops were locked down effective June 16 until they could go through the verification process and installation of state-of-the-art encryption," spokesman Dana Ripley said.

•And more companies are holding employees financially liable for their laptops, said Mark Gannaway, the Dallas-based president of insurer Safeware, based in Columbus, Ohio.

"Many of our individual policyholders are corporate employees insuring their corporate laptops because their employer has elected not to pay for the insurance but to hold the employee accountable for the unit," he said.

Safeware said thefts of laptops that it insures soared 20 percent last year and are expected to rise another 20 percent this year.

Behind the push

The push for laptop security is being driven by several factors.

The main one is that laptops are becoming so pervasive. Many employees who formerly used a personal computer at work and their own PC at home are now using a laptop exclusively, even at the office, so they can do their jobs wherever their busy schedules take them.

"There's a trend toward the mobile workforce," said John Livingston, chief executive of Absolute Software in Vancouver, B.C., which helps companies track and recover stolen laptops. "That's an overwhelming trend that's not going to go away. Now we're faced with having to protect the data on these mobile devices."

A second factor is laws such as the Sarbanes-Oxley Act of 2002, which was a response to the corporate fraud at Enron Corp. and WorldCom Inc. The law holds companies to higher standards in financial reporting, and many are including data security as they tighten internal controls.

"If your systems are not secure, if the processes for how those systems are used can be manipulated or compromised, then you leave yourself open to potential instances of fraud or circulation of misinformation and error," said Jennifer Berman, managing director at CBIZ HR Advisory & Training Services, a business consulting firm in Chicago.

Other laws requiring data security are the federal Gramm-Leach-Bliley Act of 1999, which governs financial services companies, and the Health Insurance Portability and Accountability Act of 1996.

But it was a law passed by California in 2002 that brought the issue into the spotlight. The law requires any business, nonprofit organization or state agency to notify California residents if there's a possibility that their personal information was accessed without permission. That has spurred the announcements of potential data breaches and has brought widespread attention to the problem.

"More companies are starting to formally adopt information security programs to demonstrate their compliance with the laws that are being adopted," said Chris Volkmer, an attorney specializing in data security at Winstead Sechrest & Minick PC in Dallas. "It will be a continuing management issue because the exchange of data is going to get more pervasive. The problem will multiply."

Many organizations have learned painful lessons about how vulnerable laptops can be.

The Veterans Affairs Department dealt with a firestorm of criticism after it announced the potential loss of data on millions of veterans. The agency promised to provide free credit monitoring services to those affected.

The laptop and hard drive were recovered after an informant, motivated by a \$50,000 reward, pointed police to them. The sensitive data on the laptop hadn't been copied, the FBI said.

### Reinforcing the rules

Boeing instituted tougher policies after a laptop containing employees' Social Security numbers and addresses was stolen from an employee last November. The employee was authorized "to be working with that type of data but was not following our security procedures," spokesman Tim Neale said.

In April, a laptop was stolen from a Boeing human resources employee at an airport. The computer contained Social Security numbers and, in some cases, addresses and phone numbers of 3,600 current and former employees.

In both cases, Boeing said, the information wasn't encrypted. The laptops weren't recovered, but there's no indication that anyone's information has been used illegally.

Boeing has reinforced its policy that employees access sensitive information through company servers instead of downloading data to their laptops.

"If it needs to be temporarily saved to a laptop hard drive, it must be saved to an encrypted folder," Mr. Neale said. "We recognize that at times employees might need to work off their hard drive rather than off a server. Proprietary files saved to hard drives must be deleted from the hard drive as soon as possible."

### Detailed rules

The rules are very specific. For all Boeing employees, laptops must be secured in a locked drawer or office when an employee leaves the office or cubicle at the end of the workday, for the weekend or for vacation.

"If taking a laptop outside of a Boeing office, employees must ensure it is physically secure at all times," Mr. Neale said. "If left in a car, it should be locked in the trunk, not left on the seat. If taken home, and the employee subsequently leaves the house to do errands, the house should be locked or the computer locked in a drawer or closet. If left in a hotel room, it should be locked in a safe. If taken to a hotel conference room, and the employee is walking in and out of the room, it should be locked via cable to a table."

### Usage agreements

More companies are requiring employees to sign computer usage agreements that spell out how workers will use their laptop and the information on it, said Ms. Berman of CBIZ.

"That usage agreement should cover everything from the hardware to the software," she said. "It should include use of Internet technology to anything that could otherwise compromise the computer itself, like

viruses and physical security."

Employers should also reinforce that employees are to "guard that laptop like it's their own wallet," Ms. Berman said. "It shouldn't be any less than that."

Changing technology means such agreements should be updated regularly.

For example, said Mr. Nolan of Squire, Sanders & Dempsey, "Should an employer prohibit employees from working on a wireless connection when they're working at home?"

Many companies have far to go, experts said.

"What I see are policies that exist that no one ever pays attention to," said Mike Cantrell, an expert in computer forensics and data security at Secure Source in Southlake, an international risk-consulting firm. "We'll go into a client's office and say, 'What are your policies? Do you even have policies?'"

Those that do may not review them often enough with employees, he said.

"A lot of companies are a little bit lax in what they allow their employees to do," Mr. Cantrell said.

For many companies, it comes down to cost.

"Companies don't want to pay for that type of security until something happens that either forces them or wakes them up to that situation," Mr. Cantrell said.

It's difficult to quantify such an expenditure, said Mr. Volkmer of Winstead Sechrest & Minick.

"This is one process that doesn't add dollars to the business, so that's a difficult choice to know how much you're going to have to spend," he said. "You have the reputational risks, as well as the risk of claims from your business partners, your customers, your employees. The liability is still a developing area in the law."

The laws themselves are still developing.

Texas is one of several states that have followed California's lead in requiring data breaches to be publicized.

Seeking one law

But Congress is trying to consolidate all the state laws into a single federal measure.

"You've got a patchwork of legislation," said Phil Dunkelberger, chief executive of PGP Corp. in Palo Alto, Calif.. "You need to have one federal law with some best practices in it."

Competing congressional bills are in various stages of the legislative process.

Some of the bills say that if personal data is encrypted, a company shouldn't have to notify consumers, on the presumption that the information would be difficult to access by identity thieves and therefore is an unlikely threat to consumers.

Consumer advocates would prefer full disclosure, while business advocates argue that no one is helped by false alarms about lost data, as seems to have been the case with the Veterans Affairs laptop.

Chris Voice, chief technology officer at Entrust Inc. in Addison, which provides security software and services, said a safe-harbor provision for companies that use encryption would spur more companies to action.

"It's going to accelerate the deployment of the types of technology to better protect people's information because it provides an incentive for organizations to do the right thing," he said.

E-mail [pyip@dallasnews.com](mailto:pyip@dallasnews.com)

## **LAPTOP THEFT**

10%

of laptops will be stolen within the first 12 months of purchase.

90%

are never recovered.

49%

of companies have had laptops stolen with the last 12 months.

57%

of corporate crimes are linked to stolen laptops.

80%

of computer crime consists of "inside jobs" by disgruntled employees.

73%

of companies had no specific security policies for their laptops in 2003.

## **TIPS TO PREVENT THEFT**

Use visual deterrents such as a cable lock.

Never leave laptops unattended. Lock them in something.

Carry your laptop in a backpack or tote bag instead of a telltale laptop bag.

Use complex passwords and change them regularly.

Back up valuable data regularly.

Understand the liability and technical dangers of pirated software and file sharing.

Use anti-virus and anti-spyware software, asset tracking and recovery software, encryption solutions and firewalls.

Stay informed on changes in technology and criminal behavior.

SOURCES: The companies; Computer Security Institute; Absolute Software; FBI

## **WHAT SOME LOCAL COMPANIES ARE DOING**

### **Tenet Healthcare Corp.**

In health care, it's always been imperative to guard patient and employee information zealously, spokesman Steven Campanini said.

The Irving company, which operates 70 hospitals in 12 states, is converting to a system that will automatically encrypt files that employees download to their computers. "Access to sensitive information is on a need-to-know basis," he said.

Tenet, which has a privacy officer, constantly reminds employees of the importance of safeguarding sensitive information, he said. "We cannot afford to be reactive to the current environment."

### **Electronic Data Systems Corp.**

Spokeswoman Kimberly Walton said the Plano-based computer services giant utilizes encryption software on its computers and laptops.

"We feel that we've had good security policies to begin with, and, in light of the recent issues, we're re-examining and strengthening those policies to ensure that our clients' data are safe," she said.

"We also routinely stress to our employees the company policy and security policy on how best to secure our clients' data," she said.

### **Southwest Securities Inc.**

Spokesman Jim Bowman said there haven't been any major changes to Southwest Securities' laptop policy.

"We hope it was pretty tight to begin with," he said.

"We take commercially reasonable steps to secure our information technology assets. But our policy is not to discuss what those steps are, because doing so would potentially defeat the purpose of our efforts."

---

Online at: <http://www.dallasnews.com/sharedcontent/dws/bus/stories/071606dnbuslaptop.149e180.html>