



SUBSCRIBE HERE

Back Issues



- Home
- Current Issue
- Subscribe
- Buyers' Guide
- Sourcebook
- Job Postings
- Industry Calendar 2007
- Editorial Submission Guidelines
- Product Info
- Newsletter
- Industry Associations
- First Monday
- Government Security Reports
- Marketing Info
- Rent Mail Lists
- Rent E-mail Lists
- Contact Us



SAVE THIS EMAIL THIS PRINT THIS MOST POPULAR

RSS MY Yahoo! newsgator Bloglines

The Case of the Missing Laptops

Aug 1, 2006 12:00 PM
 By Jacqueline Emigh

Parking lots constitute a risky place for laptop computers. "We've had units stolen out of cars when an employee goes into a restaurant to grab a hamburger, for instance," says Sean Shivley, IT inventory manager for Smart Documents Corp., a healthcare software and consulting company. Security Tracking of Office Property (STOP), a Norwalk, Conn.-based vendor, has helped law enforcement officials to recover laptops stolen from cars and other places.

Through pure coincidence, March 26, 2005, turned out to be a particularly red-letter day for STOP, marked by recoveries of three laptops nabbed by thieves from automobiles.

First, a laptop snatched from a rental car turned up in a trash bin in San Diego. Later, a homeowner in Vienna, Va., discovered two laptops lying on the street near the house. The PCs in Virginia had disappeared from the trunk of somebody's car the night before.

Brand new laptops also get misplaced or stolen during shipment to customers, from either delivery trucks or loading docks. Additional venues for computer theft include airports, hotel rooms, houses and college classrooms, experts say. In other scenarios, employees and students either refuse or conveniently "forget" to turn in their previously issued laptops.

Some thefts seem to be prompted by corporate espionage or just plain nosiness. Yet, stolen laptops also turn up for resale in places ranging from Web-based auction sites to pawn shops. Ironically, the security risks can be even bigger for smaller mobile devices such as PDAs and cell phones.

It doesn't take heaps of criminal know-how to snatch a cell phone off an airplane seat while its owner catches a nap on a red-eye flight. Yet that same mobile device might contain confidential contact information such as unlisted home phone numbers, and if it is one of the newer models, it might even hook up over the Internet to a sales database on a corporate network.

The good news is that mobile device security keeps getting better all the time. Approaches with proven track records run the gamut from "tattooing" the portable hardware with special ID numbers to high-tech, Lojack-type techniques that send out alerts whenever stolen devices are used for Internet access.

In the first group of products, STOP produces physical security plates for laptops with numbers that are registered in a Web database. The bar code numbers on the plates are also indelible, says Doug Belfiore, a company executive. Even if a thief manages to remove the plate, a tattoo mark remains permanently on the device.

"STOP is planted in the physical world," Belfiore says. "We rely on the age-old 'branding' concept that says, 'this belongs to somebody else, so don't use it.' And we 'brand' the equipment in ways that don't give away the owner's personal information."

Last May alone, STOP helped to recover at least 17 lost or stolen laptops. In Houston, six units — pilfered the day before from a hotel — were found in a shed behind a vacant house by the deputy sheriff's office.

The crooks in Houston managed to remove the plates from the backs of the machines; however, police were able to use STOP's indelible tattoos to identify the rightful owners.

Lojack for laptops

Absolute Software Inc., Vancouver, has come up with a software-based solution called Computrace. When a Computrace-enabled computer is reported lost or stolen, an alert is sent to a company-operated monitoring center. If the computer is then used for internet access, Computrace is able to identify and disable the device, according to John Livingston, Absolute's chief executive officer. Along the same lines as STOP, Absolute then works with law enforcement officials and other government agencies to get the laptop back to where it belongs.

In one case, for example, a laptop reported stolen from a college in Illinois started calling the Internet from an Army barracks elsewhere in the U.S., and then suddenly, from Iraq.

As it turned out, the caller in Iraq bought the laptop in Illinois — without realizing he had purchased stolen goods — just before enlisting in the National Guard. When Absolute got in touch with the new guardsman in Iraq, the soldier immediately sent the PC back to the U.S. for return to its owner. In a show of support for overseas troops, Absolute supplied the guardsman with a replacement PC.

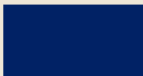
Often, laptop recovery efforts help police to solve other criminal cases. In Texas, law enforcement officials used Absolute's Computrace to track

Search GO

SMALL BUSINESS REVIEW Resources for Successful Small Business Owners
Give Yourself A Raise and a Bonus
 We provide you with tools you need

SMALL BUSINESS REVIEW Resources for Successful Small Business Owners
 Learn how to increase sales and improve productivity with concise, actionable tips on finance, management, human resources, marketing and regulations.
 We provide you with tools you need

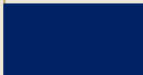
- THE LATEST
- First Monday
 - 2006 Product Of the Year



Online Directory

ACCESS CONTROL & SECURITY SYSTEMS
 GOVERNMENT SECURITY

Your Ultimate Online Resource for Security Technology.



down a stolen laptop to an auto repair shop. Upon entering the shop, police spotted not just the laptop but a stolen luxury SUV valued at over \$50,000. Numerous arrests followed.

Beyond the successes so far, vendors are either enhancing their techniques for theft detection or are planning to do so in the near future.

STOP, for instance, is considering augmenting its bar-code technology with embedded RFID chips. "This would allow computers to be tracked at building exits, as well as throughout (corporate, government agency and college) campuses," Belfiore says.

In another example of changes in the works, Absolute has now moved beyond offering its technology as software only. Over the past year, the company has forged deals with major laptop manufacturers Dell, Gateway, Fujitsu, Hewlett-Packard and Lenovo to embed Computrace directly into the bios of computer hardware.

"When it's embedded in the bios, Computrace cannot be removed, even if the hard drive is taken out," Livingston says. Absolute has also integrated a "stealth" system, aimed at preventing thieves from knowing that Computrace is aboard at all. The technology also contains the capability to wipe data off of any Computrace-enabled stolen computer that appears on the Internet.

Absolute customer Smart Documents has now deployed 925 Computrace-enabled Dell laptops, mainly among mobile workers such as salespeople and "scanning representatives," who visit clinics and hospitals to process requests for medical records.

Although most of the PCs were purchased before the embedded version of the technology became available, at least 60 of them are indeed embedded with Computrace, Shivley says. "We love Computrace, and so does the local police department. I've also recommended it to a lot of other people," he adds.

Since beginning to use Computrace, Smart Documents has seen seven laptop thefts, with six of the PCs being recovered typically within 30 days.

"I know that the seventh laptop was stolen too, but it has not called in to the Internet yet. Either it got trashed or the hard drive was removed," Shivley says.

Smart Documents also uses Computrace for asset tracking and certain IS (information security)-oriented functions. "(Computrace) will tell you whether there are any units that have not been active for the past 21 days, or whether anybody has violated (company) policy by downloading software off the Internet, for example," according to the IT supervisor.

Student laptops recovered

William Penn University in Oskaloosa, Iowa, on the other hand, has issued Computrace-enabled Gateway laptops to all students in its program for working adults. All of these PCs from Gateway use the embedded version of Computrace.

"We've experienced pretty good success recovering two of the three laptops that have been stolen since then," says Curtis Gomes, the university's information technology supervisor.

One of these three PCs was stolen from a car and another from a classroom. In the third case, an adult student allegedly kept the computer after completing the program and then sold it to someone else.

Gomes strongly suspects that the PC, which disappeared from the classroom, was grabbed by a younger student who'd been removed from the university's main campus program due to poor grades.

"He was frustrated because he had gotten kicked out," he says. Subsequently, the alleged thief moved to California.

Miniature mobile devices

Absolute has also been finishing up yet another edition of Computrace. The latest one is specifically designed for Windows Mobile-based PDAs, Livingston says. Versions for other sorts of miniature mobile devices are expected to follow.

Many other vendors produce IS software that protects PCs and servers in other manners, for example, by encrypting (or "scrambling" data), keeping out unwanted network traffic or chasing out malicious software code, known as malware.

Some of these companies are also teaming up with mobile hardware makers or mobile carriers on embedded security. In this category, anti-malware expert McAfee Inc. is pursuing an entirely IS-oriented approach geared to protecting the data of mobile phone users. Beyond a recently inked deal with Cingular Wireless, McAfee is partnering with Motorola, Verizon Wireless, Sony Ericsson and the Japanese-based Docomo, says Todd Gebhart, a senior vice president at McAfee.

Gebhart is quick to acknowledge that the world has yet to see any kind of massive viral outbreak on cell phones. But newer devices such as "feature phones" and "smart phones" are already facing some IS issues, according to Gebhart, who points to infected IMs (instant messages) and security holes in wireless Bluetooth technology as a couple of examples.

"We believe that right now is a good time to be thinking about mobile security. Security should not be an afterthought," Gebhart says.

McAfee's IS technology for mobile phones also contains complementary capabilities, not yet implemented for centralized device lockdown and software "clean-up," Gebhart says.

Despite the almost unarguable benefits of mobility for today's workforce, keeping a steady watch over these moving targets for theft and tampering can be a daunting task. But with the effective tools already available and others now in the pipeline for the future, the job is getting easier.

ABOUT THE COMPANIES

For information, circle the Reader Service number (listed below) or visit securitysolutions.com

Absolute Software Inc.	27
Security Tracking of Office Property (STOP)	28

[Want to use this article? Click here for options!](#) 
© 2006 Prism Business Media Inc.

[Back to Top](#)

Key: [W] Paid Content [H] Enhanced for the Web

[Contact Us](#) [For Advertisers](#) [For Search Partners](#) [Privacy Policy](#) [Subscribe](#)
© 2006 Prism Business Media Inc. All rights reserved.