consultant'schallenge

INNOVATIONS

Ensuring Quick Theft Recovery

Securing your firm's computer assets via Internet LoJack technology.

By Sean Tierney

The Consultant:
Sean Tierney is an independent computer consultant for Lights Out Production in Scottsdale, Ariz. This small consulting firm offers a wide array of technology-related services, including Web site construction, e-learning materials and various Information Technology services.

The Firm:
Holden Brodman is an eight-lawyer firm based in Scottsdale, Ariz. Holden Brodman is dedicated to resolving commercial disputes that involve the legal representation of lenders, secured creditors and businesses.

The Challenge:
To install a software that would enable the recovery of a stolen notebook computer and its stored data.

The Scenario

You are in the cattle drive approaching the security checkpoint at the airport on your way to a much-deserved vacation in Mexico. You have three different trials next month, and although you have some work to do during your vacation, your thoughts are focused on the roll of the surf, the sand between your toes and the frosty drink with the umbrella you soon will be holding. As you shuffle through the metal detector, you are awakened from your tropical daydream by the buzzer you just set off, which probably was caused by that new oversized belt buckle your in-laws gave you for your birthday.

As you are led aside to be frisked by security, you don't realize that somewhere in between fumbling with boarding passes, sending your luggage and shoes through the X-ray machine, emptying the contents of your pockets and getting your friendly pat-down, your laptop has casually been lifted from the conveyor belt and is on its way to any one of the many destinations serviced by the gates in your terminal. More importantly, your clients' data is in the hands of a thief, and unless you had the foresight to run an encrypted file system, sensitive information regarding your firm and clients has been compromised. Your vacation just took an unfortunate turn before it even started.

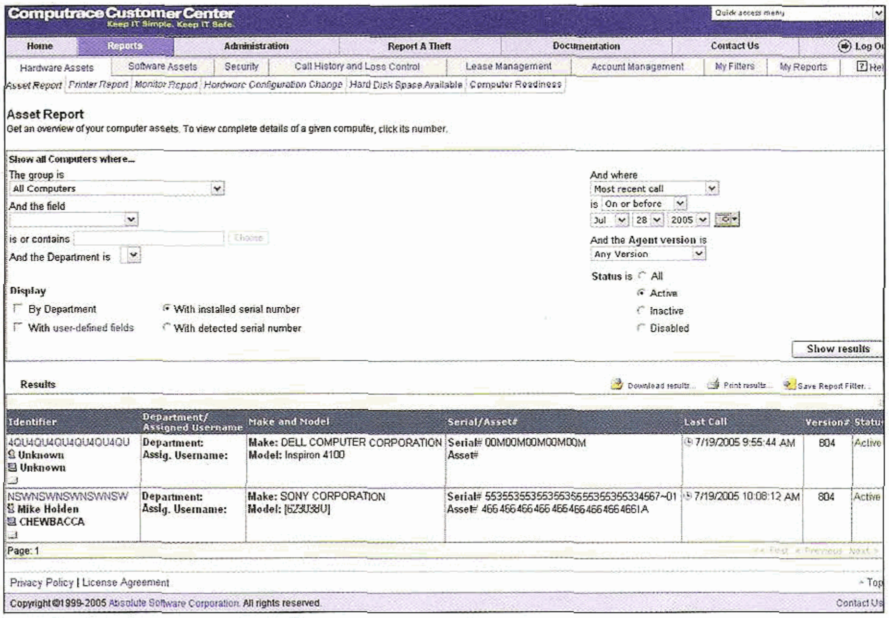
Does this situation sound far-fetched? Here are some sobering facts from an FBI survey: In 2003 this scenario or one similar to it occurred more than 600,000 times; laptop thefts accounted for $4.1 million in damages in 2004; stolen computers are used in 57 percent of all network breaches; one in eight laptop computers will be stolen this year; the most serious financial losses occurred through theft of proprietary information (26 respondents reported $170.8 million) and financial fraud (25 respondents reported $115.75 million); and only 3 percent of stolen laptops are recovered.

The most serious financial losses from stolen laptops occur through theft of proprietary information and financial fraud.

Unless you have had your head in the sand recently, you are aware there has been an epidemic of data theft within major financial institutions. According to the Federal Trade Commission, there were 246,570 complaints about identity theft in 2004, some due to hardware theft. The stolen hardware assets represent only a fraction of the monetary loss compared to the negative public relations costs associated with the cleanup efforts and mandatory damage-mitigating measures these companies must take to reduce the impact of these data thefts to their customers. Wouldn't it be nice if there was the equivalent of the LoJack for laptops – a means to silently track down your computer in the event it's stolen?

The Client's Need

Mike Holden of the law firm Holden Brodman is aware of the data theft epidemic and wanted to guard his firm against such an embarrassment. Being the managing partner of a small law firm, his concern was not so much with the threat of internal theft or departmental drift, but more so with the threat of someone on the street snatching a notebook from an unsuspecting litigator lugging gear back and forth from trial. I assessed the options for securing the firm's assets and found a solution.



Computrace Customer Center
Keep IT Simple. Keep IT Safe.

Asset Report

Get an overview of your computer assets. To view complete details of a given computer, click its number.

Show all Computers where...

The group is: All Computers

And the field:

is or contains: Choose

And the Department is:

And where: Most recent call

is: On or before

Jul 28 2005

And the Agent version is: Any Version

Status is ○ All ● Active ○ Inactive ○ Disabled

Display

□ By Department ● With installed serial number

□ With user-defined fields ○ With detected serial number

Show results

Results

Download results... Print results... Save Report Filter...

Identifier	Department/ Assigned Username	Make and Model	Serial/Asset#	Last Call	Version#	Status
4QU4QU4QU4QU4QU4QU Unknown Unknown	Department: Assig. Username:	Make: DELL COMPUTER CORPORATION Model: Inspiron 4100	Serial# 00M00M00M00M00M Asset#	7/19/2005 9:55:44 AM	804	Active
NSWNSWNSWNSWNSW Mike Holden CHEWBACCA	Department: Assig. Username:	Make: SONY CORPORATION Model: [623U38U]	Serial# 55355355355355355555355355334567~01 Asset# 466466466466466466466466466 1A	7/19/2005 10:08:12 AM	804	Active

Page: 1

Copyright ©1999-2005 Absolute Software Corporation. All rights reserved.

Computrace allows law enforcement officials to recover stolen laptops through a software that is installed in your computer and contacts the Monitoring Center to report its location when it's stolen.

The Options

My initial thought in searching for any type of software was to explore what open source options exist. Knowing security is of utmost importance to attorneys, I figured running the tracking software on the firm's servers would appease even the most paranoid Information Technology administrator. However, I quickly realized the software's role was only a piece of the puzzle in terms of recovering a stolen laptop, and equally important was to access a high-speed data center and an experienced recovery team to facilitate the recovery efforts of local law enforcement. I turned my search toward commercial services that provide full solutions and found four vendors that stood out: Stealth Signal Inc., zTrace Technologies, Absolute Software Corp. and CyberAngel Security Solutions Inc.

The Decision

Our main concern with a technology that uses such an intimate connection with a person's personal data is the privacy, security and reputability of the company that will house the data. While the product offerings from all four vendors were similar, Holden and I agreed Absolute Software's Computrace was the best product to suit the firm's needs. This was due mainly to the confidence and credibility conveyed through its Web site and the favorable reviews the company received from a handful of online sources. Absolute also has deals with major original equipment manufacturers to bundle its software as a pre-installed option.

We took the consensus of major equipment manufacturers as an affirmation we made the right choice. Other factors that contributed to our decision were the $1,000 per-machine guarantee, the fact that Absolute Software's dedicated in-house recovery team comprised of ex-law enforcement personnel, the software's ability to be installed automatically through the network if we decide to track all office workstations in the future and the wealth of reporting features offered through the company's Web-based administrative interface. The price was comparable across all four vendors.

Implementation

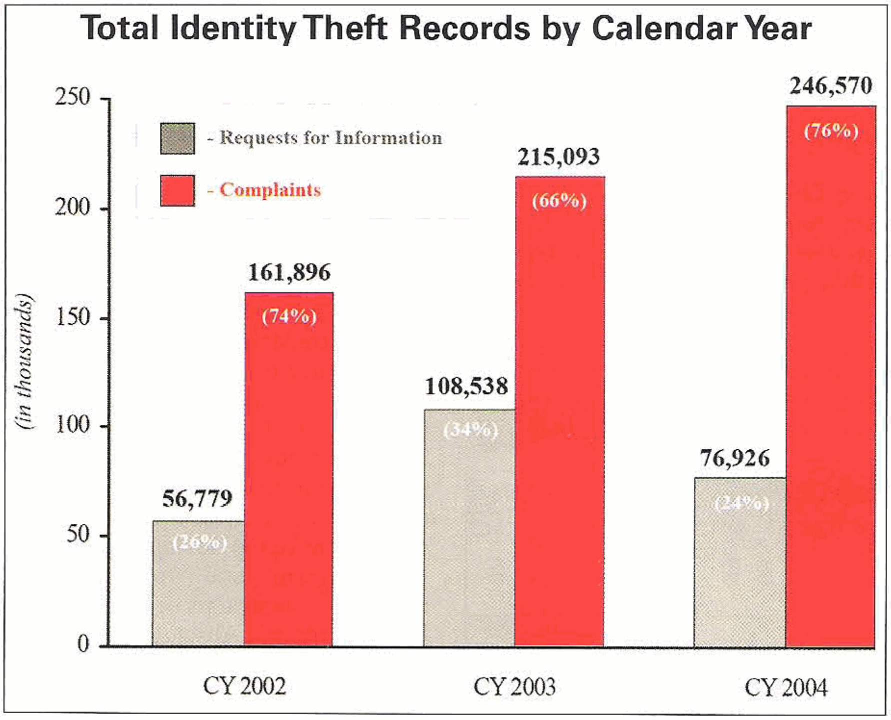
The implementation was painless and it took only about 30 minutes to install the tracking software on all of Holden Brodman's laptops. Once I established an account on Absolute's Web site (www.absolute.com), I was presented with an administrative console from which I could download the Computrace agent, the software that resides on each machine to be tracked. It should be noted that Computrace supports both Macintosh and PC systems. I placed the installer file on my keychain universal serial bus drive and then went from laptop to laptop installing the program and rebooting the machines. The laptops each made their first call into the Absolute data center, and one-by-one appeared in the administrative console.

Absolute claims its tracking software is tamper resistant, which is an understatement. It will survive a reinstall of the laptops' operating systems as well as an Fdisk reformat. The software is stealthy, so even if the thief is looking for tracking software, Computrace is nearly impossible to spot – much like a silent burglar alarm.

How it Works

The Computrace agent silently calls Absolute's Monitoring Center every 24 hours and reports its Internet Protocol address or phone number. In the event the agent is damaged, it has the ability to restore itself back to working condition by downloading the necessary pieces it needs from the Absolute data center. Along with an IP address or phone number, the Computrace agent also returns Media Access Control addresses, statistics about disk usage, and installed hardware and software. The connection is RC4-encrypted so all personal identifiable information, such as serial numbers and MAC addresses, is transmitted securely over the wire.

In the event the computer is stolen, the call frequency is increased to once every 15 minutes and the recovery team is alerted. At this point, you might have the same question I did. "How do they translate an IP address to a physical location to which the police can be sent?" It's not a magical process at all, but rather a legal one. Here is the sequence of events:



A chart from the Federal Trade Commission's annual report on identity theft. A downloadable version of the full report can be found at www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf.

- The owner of the stolen laptop files a police report and reports the theft through the administrative console on the Web site, specifying the number of the police report.
- A recovery team member gathers the information called in from the stolen computer and compiles documents for the local detective to use to subpoena the access records from the Internet Service Provider through which the stolen computer called in.
- The detective appears before a judge and presents the documents to obtain access records from the ISP in question.
- The ISP is required by law to surrender the access records, which then are used to identify the physical address from where the call originated. By this time it might be a week after the first call was made. If the laptop still is calling from the same location, it's a compelling reason for the judge to grant a search warrant for those premises.
- If a search warrant is issued, the detective investigates the location. If no warrant is issued, the officer can do what is called a "knock and talk" at the location to try and shake down the occupant. According to the recovery team member I interviewed, 90 percent of the time a detective proceeds without a warrant, the thief folds without thinking to demand a warrant.

The Field Test

As skeptical as I was, I needed to see this process in action myself. I installed the software on my laptop and reported it stolen. Within 10 minutes of my computer calling into the data center, I received a call from the recovery team. The officer read back the correct IP address as well as some extra information about my router. He correctly stated he believed it was calling in from Chandler, Ariz. As he went over the steps of the recovery process, I had visions of a special weapons and tactics team rappelling through my roof. Figuring the test had gone far enough, I explained to the officer who I was, gave my credentials and asked to cancel the theft report. Assuming the legal process for identifying the actual physical address works as claimed, I could have expected to receive a visit from a police officer within several days.

> **I installed the software on my laptop and reported it stolen. Within 10 minutes, I received a call from the recovery team.**

Recovery Process

The Computrace software worked as advertised, and the recovery team was prompt and courteous. The potential flaws I see with this type of recovery mechanism are the same that would exist with any technology relying on the Internet as a transport medium. It must connect to the Internet to be able to call in. Recovery attempts could be confounded by connecting the stolen computer through open Wi-Fi hotspots and other public anonymous access points. The agent can be removed by doing a low-level binary Department of Defense grade format of the hard drive.

In all fairness, these are picky points considering how well the system works. It's probably safe to assume that any machine stolen these days will be used at some point to connect to the Internet. Unless the thief also is stealing a wireless connection, he or she probably would connect from a residence or business. Only the most tech-savvy thief would know how to do a DoD-grade format of the hard drive. I understand Absolute Software is working to embed the Computrace agent in the basic input/output system of computers and already has it working on all new Lenovo (formerly IBM) ThinkPad laptops. Short of switching the transmission method to some type of radio frequency to circumvent the potential problems listed above, this is just about the ideal setup one could expect from this technology.

Holden Brodman was very satisfied with its tracking software. "We now have a reasonable safeguard in place for securing our notebook computers and a software-licensing compliance tool to boot," Holden said. "Consistent with our commitment to uphold the best interests of our clients, we are taking this extra step to ensure a favorable outcome, even in an unpredictable, worst-case scenario. And that feels pretty good." loc

Sean Tierney is an independent computer consultant based in Scottsdale, Ariz. Tierney has more than 10 years of programming experience as a developer of ColdFusion Web applications and specializes in the creation of custom 3-D graphics and animations for trial. He is a Macromedia Certified Advanced ColdFusion MX Developer.