## Laptops vulnerable to theft at the office

The office is the most common place laptops are stolen, tallying 29 percent of all laptop disappearances worldwide, according to a recent survey by mobile data security provider Credant Technologies.

"Everyone knows to guard their devices when they're traveling, but the results we found about the office were quite shocking," says Credant CEO Bob Heard. "What we discovered were corporate environments that are careless and even reckless with laptops, many of which contain crucial company and personal data."

Nearly 87 percent of respondents reported having company-related e-mail on their stolen laptops; 67 percent had other important business information stored; and 90 percent reported that their stolen laptop contained sensitive and confidential corporate data that was not intended for public view.

The survey also found that nearly three quarters of the stolen laptops did not meet regulatory compliance requirements for data encryption, mainly the stringent privacy regulations dictated by Health Insurance Portability and Accountability Act (HIPAA), California Senate Bill 1386 and other regulations. Twenty-one percent of respondents report they used no security measures or encryption of any kind on their stolen laptops. Only 10 percent of respondents report using a full-disk encryption security product.

"Eighty-two percent of all our survey respondents claim they never recovered their stolen laptop," Heard says. "That's sensitive information floating out there in the wrong hands."

Compliments of Lynn Meanney, following is an article that appeard in today's The New York Times regarding computer tracking technology, including Absolute's product...Jim

# Steal This Laptop and It Will Tell the Cops Where to Find You

**By WILSON ROTHMAN**
Published: October 5, 2005

YOU don't have to tell Joe Leimer that the vast majority of computer thefts are inside jobs. As the information technology manager of Jubilee Home Solutions, which remodels kitchens and bathrooms, Mr. Leimer issues dozens of laptops to its traveling salespeople. Experience has shown that some of the computers will be lost or stolen; after "being burned once," Mr. Leimer decided to be prepared.

This summer, when Jubilee's Dallas office reported that a former employee had refused to return his laptop, Mr. Leimer activated Absolute Software's Computrace program, now routinely installed on company-issued computers. The thief was tracked to a motel parking lot, where he was using a free Wi-Fi network, a connection that proved to be his downfall. Mr. Leimer, using Computrace, reached through the Internet to erase the computer's hard drive remotely. It was soon returned, no questions asked.

During the last few years, computer tracing systems have become vital to what information technology managers call "asset protection." These services can track where a PC connects to the Internet, and, with the help of a subpoena, translate that information into a street address.

Most of the services include a form of data protection, from password-protected encryption of the whole computer to data-deletion systems like Absolute's. Many also offer plans that reimburse customers for stolen equipment if it is not recovered by a certain time. Some, though not all, offer to track computers across national borders.

Three of the largest companies in the industry, Absolute, CyberAngel Security Solutions and Stealth Signal, have enjoyed high recovery rates, and offer services to consumers, too, like parents who worry that a child's laptop may be stolen at school. But corporate theft is the bigger problem, many in the business say.

Crucial to the recovery is a company's partnership with law enforcement. First, the customer must report the theft to the police, then call the tracking company with a report number, the name of the police department and an officer on the case. Then the tracking company waits for a signal from the computer.

The computer reports in with an Internet Protocol, or IP address, a number that indicates its location in cyberspace. The tracking company knows which Internet service providers possess which IP addresses. With the support of law enforcement and a subpoena indicating that the IP address is required for a criminal investigation, the tracking company asks the Internet service provider to report which customer was using that IP address at that time.

Recovery time can vary widely. Stealth Signal offers an optional 60-day recovery warranty.

These companies are devising more ways to track stolen PC's. CyberAngel has formed a partnership with Skyhook Wireless, which specializes in locating Wi-Fi products. As a stolen laptop moves around, it records the various networks it passes by, creating a connect-the-dots trail to follow. "We'll have the Wi-Fi security integrated before the end of the year," said Bradley Lide, CyberAngel's chief executive.

Absolute is investigating a different sort of wireless tracking. Companies often equip laptops with cards that connect them to cellular data networks. Absolute wants to be able to make "silent calls" to laptops via those network cards. The company could then delete sensitive data immediately, and even download files from the laptop. "Most stolen PC's will connect to the Internet eventually, but you don't have to wait," Mr. Haidri said. "Why not call the thing up yourself?"

One sensitive issue is whether to tell employees that their computers - owned by the company - are, in essence, bugged.

"We keep confidential that this software is even installed on employee computers," Mr. Leimer said. "We don't want them leaping to the quick assumption that we don't trust them. We totally trust them, but if somebody's leaving the company, it could be centered around a reason of trust. And if a laptop gets stolen, that's just something that happens."