

November 15, 1998

Thwarting Laptop Theft

Small, powerful machines popular with business executives and criminals alike

In October 1997, a major airline lost 22 laptop computers worth \$75,000 when thieves used glass cutters to enter a first-story office. The following month, law enforcement authorities in the Washington, D.C., area apprehended a ring of four people who had stolen approximately 40 machines in Fairfax County, Virginia. And in June 1998, Canadian police sought public assistance in identifying a man who was captured on videotape by a security camera while leaving a building with three laptop computers. Authorities believe the man is responsible for stealing approximately \$200,000 in laptop computers from businesses in downtown Edmonton since the beginning of the year.

As technology continues to evolve at a breakneck pace, modern computers are becoming increasingly smaller and more powerful, giving business travelers the same productivity on the road as in the office. Today's laptop computers boast processors as fast as 300 megaHertz and can weigh as little as three to four pounds—or less for those who wish to opt for the new mini-laptops. Unfortunately, the very traits that make these machines desirable for business users—their powerful performance and high portability—also make them exceptionally attractive for the criminal element.

Since November 1978, The Lipman Report has chronicled the evolution of computer crime and provided readers with the latest intelligence for protecting their information assets. Much of that information appears in The Lipman Report: Selected Editions on Computer Security, published by The Lipman Report editors in August 1998. This issue examines the growing problem of laptop theft and offers advice on protecting valuable hardware and proprietary information.

A Growing Problem

According to the latest statistics published by a Midwestern agency that specializes in personal computer insurance, laptop theft continues to increase at an alarming pace. Laptop theft jumped 17 percent last year—from 265,000 in 1996 to 309,000 in 1997—while theft of desktop units decreased by 31 percent. The dollar loss from these thefts exceeded \$1 billion in hardware alone, excluding the value of the information contained on the machines. A second survey, conducted by a West Coast association of infor-

mation security professionals in cooperation with the Federal Bureau of Investigation, found that 57 percent of the 520 participating organizations reported stolen laptops during 1997, making laptop theft the third-most common form of electronic violation, after computer viruses and insider abuse.

Experts attribute much of the increase in theft to the simple fact that more and more people use laptop computers. At the same time, the vast majority of laptop users regard their computers as just another tool and fail to take adequate measures to protect these valuable machines that generally cost between \$2,000 and \$4,000. The ubiquity of often-careless laptop owners provides the criminal element with a high-yield, low-risk niche. The average laptop system nets between \$500 and \$800 on the black market, and the FBI reports that 97 percent of stolen computer equipment is never recovered.

In most cases, criminals seize laptops for the cash value of the hardware, but security experts say that economic and industrial espionage motivate an increasing number of incidents. Some organizations even place bounties on the laptop computers of executives of specific corporations, offering tens of thousands of dollars for the systems, which can contain proprietary information worth millions. Last September, for instance, on the same day that an Australian mining company was identified as a possible takeover target, thieves broke into the organization's Sydney offices and stole the laptop of the managing director, while ignoring two similar machines sitting on nearby desks.

Accomplishing the Deed

Although several new trends are emerging, one out of every 10 laptop heists still occur at airports. These thefts usually involve at least two criminals, one of whom will distract the victim while the other grabs the computer. In one scenario, the

(continued on next page)

Thwarting Laptop Theft

Small, powerful machines popular with business executives and criminals alike

(continued from preceding page)

unsuspecting traveler sets down the computer to make a telephone call. The first thief signals a partner, who pretends to use the phone next to the traveler. A third criminal then walks by and bumps into the victim, launching into a long-winded apology to maintain his or her attention. Meanwhile, the second thief grabs the computer and leaves, handing it to a fourth accomplice who disappears before the traveler discovers the laptop missing. Other common ploys involve a couple suddenly starting a loud argument to attract the victim's attention, an attractive woman stopping a male target to ask for assistance, and a distracter dropping money on the ground and asking whether it belongs to the victim.

Hotels present another fertile hunting ground for laptop thieves. Travelers frequently set their computers on luggage carts or beside them as they check in and out. In addition, guests often place too much confidence in hotel security. Even if a conference room is locked during the lunch break, for instance, the hotel staff still needs to access the room to perform services such as trash disposal or beverage refreshment. Many a well-dressed thief has entered such "secured" rooms, claiming to have forgotten his or her laptop. According to the Technology Theft Prevention Foundation, a non-profit high-tech crime prevention organization, an average of one laptop per week disappears from hotels and the convention center in Santa Clara, Calif., a popular site for industry conferences.

A recent trend in laptop computer theft targets private residences. According to the executive director of the foundation cited above, laptop thefts from the home increased dramatically for the first time in 1997. "People are telecommuting more often. They have their laptops at home, and they often don't have the security at home that they have at the office," he said. "Now, burglars not only take jewelry, cash and electronics equipment, but they also steal computers."

Cargo theft of laptop computers—sometimes at gunpoint—represents another rising trend. In December 1997, for instance, armed robbers held up a truck in Tennessee that was headed for a retailer in Ohio. The thieves stole 350 computer systems worth \$770,000. Although police recovered 49 of the stolen machines when three men trying to sell the computers in Memphis aroused the suspicions of local law enforcement, the rest remain missing.

Security Solutions

With laptop theft on the rise, security manufacturers have not remained idle. The security market boasts a plethora of security solutions—ranging from very basic to ultra-sophisticated—to help laptop owners protect their electronic assets.

The simplest theft deterrent relies not upon technology, but upon user vigilance: securing the laptop when not in use. This important task can involve nothing more than locking the computer inside a file cabinet or desk drawer. Several tools are available to secure laptop computers to fixed objects. One organization offers a solid steel locking station that bonds to any flat surface. Other companies sell cable locks, similar to bicycle locks, that fit into a standard security slot found on most computers and attach the machine to a fixed object. One such device includes a 110-decibel alarm that can be set to go off if someone cuts the cable or physically moves the computer.

A high-tech solution to the problem of laptop theft involves a software program that resides silently on the computer's hard drive and uses an Internet connection to call a central monitoring station. Some versions contact the monitoring station at regular intervals, such as every week. If the owner has reported the system missing, the station logs the origin of the phone call and dispatches the police. Another program requires the user to input a password—unprompted—each time he or she logs into the computer; only

if the user fails to supply the password does the system call the monitoring station. In August 1998, such a program enabled Chicago authorities to track down eight computers stolen from a mortgage company in May. Fourteen weeks after the theft, one of the computers phoned in with its location, an office in a neighboring town.

While these programs have assisted law enforcement in recovering thousands of dollars in stolen computer equipment, they rely upon the thieves plugging the systems into a telephone jack. Asset management tattoos offer an additional layer of security by reducing the criminals' ability to sell the computers. These metal identification plates permanently bond to the computer case; if removed, the plate uncovers an indelible "tattoo" that identifies the machine as stolen and provides a phone number to facilitate its recovery. Another asset management system consists of two tags: one that affixes to the computer and one that the authorized user carries. When a person leaves the office with a laptop, security personnel can request to see the authorization card identifying him or her as the registered user.

Another type of security device consists of a wireless transmitter that fits on the user's key-chain and a receiver that attaches to the computer. Separating the transmitter and receiver by more than 40 feet triggers a siren in the receiver, which emits a 110-decibel alarm.

Thwarting Laptop Theft

While laptop computer theft represents one of the costliest areas of computer crime, it is also one of the most easily prevented. The following suggestions can help users protect their information technology assets:

- *Maintain constant contact with the computer.* Laptop users must exercise constant vigilance, especially when traveling. Keeping track of one's possessions usually does rank as a high priority when checking in at a hotel or airport, but the bulk of laptop thefts occur in these sit-

uations when the owner is otherwise occupied. When passing through airport security checkpoints, computer owners should keep their computers until just before entering the metal detector; if this course of action is not feasible, they should ask security personnel to hold their computers until they pass through the detector. If it becomes necessary to set the computer down, security experts recommend placing it between one's legs so that a thief cannot grab it without alerting the user.

- *Avoid obvious laptop bags.* Specially designed laptop carrying cases advertise the presence of a computer to thieves, making the carrier a target. Carrying a laptop inside a backpack or duffel bag will help camouflage the computer.
 - *Secure the computer when unattended.* Computer users must never leave an unsecured laptop in a hotel room, office or even personal residence. When traveling, laptop owners should either store the computer in the hotel safe or use a locking device to secure the computer to a stationary object. Users should exercise the same vigilance when leaving a computer at the office or home. Failure to use a locking device can prove disastrous even for short absences, as one employee learned when she returned to her desk after a 10-minute conference with her boss and discovered her laptop missing. Leaving a computer within sight of passers-by makes it easy prey for smash-and-grab theft. This principle also applies to vehicles. If the laptop remains in the car, the safest location is in the trunk, hidden from view.
 - *Protect all critical information through encryption and backup.* Ideally, travelers should never store information on the laptop's hard drive that they cannot afford to lose, so if the computer does fall into the wrong hands, their business will not suffer through
- (continued on next page)**

Thwarting Laptop Theft

Small, powerful machines popular with business executives and criminals alike

(continued from preceding page)

loss of proprietary information. Even so, many computers do contain sensitive information that should remain private, such as Social Security and credit card numbers. To protect such data from prying eyes, computer users should take advantage of password locking features found in many standard software packages. Encryption programs offer an added level of security by encoding the data into gibberish, which can only be translated with the appropriate key.

An even more effective method of protecting data involves storing it in a separate location, such as a high-capacity disk or a removable hard drive. Even if the computer itself is insured and contains no trade secrets, the user and his or her company will still incur significant losses in recreating the information stored on the machine, making frequent backups mandatory. As a minimum measure, business travelers should back up all their files before departing for each trip, leaving one copy at home and keeping the other separate from the computer. One company offers an automated backup service over the Internet, allowing travelers to back up files on the road. Laptop owners use proprietary software to send their data files to two separate data centers, and they can select an encryption key that prevents even the backup service from accessing their files.

In addition to publicizing the above recommendations, security directors can implement the following policies to help protect their organization's information technology:

- *Promote employee awareness of computer theft.* When employees receive company issued laptop computers, they should also learn about the dangers of laptop theft and how to guard against it. The security department should brief employees regularly on laptop security, including bulletins about new

scams, through tools such as employee newsletters and company-wide e-mail.

- *Encourage employee responsibility through accountability.* Every organization that uses laptops needs a written policy explaining the guidelines for using and securing the equipment. The policy needs to include enforceable consequences for employees who either lose or damage equipment due to negligence or policy violations. Often, employees fail to take proper precautions, knowing that the company can reclaim hardware loss through insurance.

As Corporate America grows increasingly dependent upon technology, laptop computers are becoming as indispensable to the average business executive as briefcases and mobile phones. Their ever-increasing presence provides a fertile looting ground for everyday thieves and industrial spies alike. While insurance policies can protect hardware, companies have no means of recouping the loss of proprietary information. This sobering fact makes the issue of laptop theft even more dire in today's highly, competitive, global marketplace.

Fortunately, laptop theft is one of the most easily prevented problems to plague the business community, but prevention requires education and vigilance. Corporate security directors must receive the resources to ensure that employees understand the risk of laptop theft and to educate them in how to protect their property. Individuals must recognize that the convenience and power afforded by laptop computers also exact a tremendous price in terms of responsibility. At the very least, negligence will cause inconvenience; at worst, it can destroy a business.



The Lipman Report Editors