

Laptop Security, Part One: Preventing Laptop Theft

Josh Ryder 2001-07-30

Laptop Security, Part One: Preventing Laptop Theft

by Josh Ryder

last updated July 30, 2001

Laptops have become a valuable part of the computing arsenal. They allow users powerful mobile computers with the same capacity and software of many desktops. They also allow connectivity, even outside the office, thus freeing people to take their workplace with them. This is extremely valuable for employees who must travel frequently while remaining in continual communication with their offices. Unfortunately, the mobility, technology and information that make laptops so useful to employees and organizations also makes them valuable prizes for thieves. This article, the first in a two-part series devoted to laptop security, will give a brief overview of how users can prevent laptop theft. In realization of the fact that no matter what users do, laptop theft will always be a possibility, the second article in this series will discuss steps that users can take to minimize the loss of valuable information through laptop theft.

The Cost of Laptop Theft

Imagine, if you will, that you are the executive of a major international mega-corp who is giving a presentation to a group of American Business Editors and Writers. After delivering a successful speech to the group, you move about the crowd, taking questions. Meanwhile, your laptop sits happily up on the podium you used to deliver your presentation. When you return to the podium, you discover that in the few short minutes that you've been away, someone has pinched your laptop. Sound improbable? This actually happened last September to Irwin Jacobs, CEO of Qualcomm (see ["Where the Hell is My Laptop?"](#))

The theft in itself was bold, but not totally surprising. What was, however, interesting to note was Jacob's candidness about the data stored on his laptop. Several witnesses reported that he stated that the laptop had contained highly sensitive data that could be of great value to foreign governments. At the time, Qualcomm was in negotiations with several of China's telecomm providers to license their CDMA cellular technology.

Was Jacob's foolish for bringing a laptop containing mission critical confidential data to an

insecure public location? Yes. Is he alone? Definitely not. In 1998, 520 security experts responded to a [Computer Security Institute](#) survey, the results were quite revealing. Laptop theft ranked second to viruses as the biggest computer crime that they had to deal with. According to a report released by the [Safeware Insurance Group](#), "approximately 387,000 notebook PCs were stolen in 2000, up about 20 percent from an estimated 319,000 in 1999." Further, it was estimated that at least 57 percent of businesses in the year 2000 incurred losses from computer equipment theft.

Of course, not all laptop thefts are committed in an attempt to grab valuable proprietary information, some laptop thieves head straight to the pawn shop. However, according to William Malik, vice president and information-security research director for market researcher Gartner Group, informal surveys indicate that about 10 percent to 15 percent of those laptops are stolen by criminals intent on selling the data. Indeed, in the case of Qualcomm CEO Jacobs, while his hardware was estimated at about \$4000, the information carried upon it was thought to be worth millions.

What Can I do to Protect My Laptop?

So given the risk of laptop theft and the potential losses that laptop theft can cause, what are some of the steps that individuals and organizations can implement to prevent it.

Cables

One of the cheapest and most cost effective solutions to deter thieves is to attach a security cable to your laptop. In most cases, the very fact that you have made the effort to physically secure the laptop to an immobile object will be enough to cause a potential thief to look for easier prey. Before you start shopping around for a security cable, there are a few important items to know:

- Does your laptop have a Universal Security Slot (USS)? Roughly 80 percent of the laptops currently produced come with a place to attach your security cable to the laptop chassis. If your laptop supports this, you should use it.
- If your laptop does not have a USS, does the cable come with some form of adhesive pad with which you can securely attach the cord to? While using an adhesive pad may not be ultimately as effective as attaching the cable to your laptop chassis, you should not discount it entirely. Many electronics retailers currently use some form of adhesive

contact sensors on many of their display models to prevent theft.

- While buying a good sturdy cable is important, make sure that the lock itself is sturdy. Tubular cylinder locks are preferred to tumbler locks as fewer thieves are readily equipped to pick the cylindrical variety.

Pitfalls of Cables

Of course, readers should be aware that, as is the case with almost any security measure, laptop cables are not infallible. Let's take a look at a hypothetical case. A hypothetical company, Foo Corp., had been alerted by the authorities that a gang of laptop thieves was moving through their area, they decided it was high time that they beef up their laptop security policy. One method that they decided to use was to physically secure laptops to desks using a cable connected to the USS (Universal Security Slot) which is then attached to a desk or other heavy stationary object. Confident they had a solution that would make stealing laptops much less, they slept peacefully that night. However, in the morning, they discovered that several of their laptops had in fact been stolen. Oddly, none of the cables had been cut. Instead of trying to break the strong link, the clever thieves instead attacked the desks to which the cables were attached. Not only did Foo Corp. have to deal with the information and property loss resulting from the laptop heist, they also suffered damage to several desks and workstations.

An alternative ending to the previous story illustrates another downfall to relying solely on cables for laptop security. The next morning, several employees started complaining that they couldn't access the network. A crack team of crusty old sysadmins were released unto the company, each roving about trying to determine what the users managed to screw up this time around. What they were confronted with surprised them. Each of the computers that were unable to connect to the network were not suffering from software misconfiguration, instead their network cards had been removed from their PCMCIA slots. So while the cable lock system had prevented the thieves from easily stealing the laptops themselves, everything that was attached to them like external CD-ROMS, and PCMCIA cards were still easily taken.

Laptop Safes

Another effective method of protecting your investment is to use a laptop safe. Paradise Systems sells a product called [Car-Safe](#), which is designed to protect your valuables while they are being stored/transported in the trunk of your vehicle. For the traveler who moves from office to office, Anchorpad Security offers Anchorpad Sentry, a portable safe that you can safely

attach to any work surface. As a bonus, when the laptop is locked in the Anchorpad Sentry, all of the PCMCIA cards and peripherals are also secure? a luxury that one does not have with a simple security cable. Finally, if laptops are kept in the office at night, consideration should be given to a laptop computer strong box.

Technological Solutions: Motion Sensors and Alarms

We've all heard and rolled our eyes at the seemingly ubiquitous wail of car alarms. But how often do you hear a 110 decibel (which would be similar to standing at the front row of a rock concert) alarm sound in your office building, or next to you in the airport? Unexpected loud noises make people wake up and take notice, something that aspiring thieves find very discouraging. Laptop security companies realize this and have created alarms for portable computers.

While the signalling mechanism of an alarm system is usually the same, the triggering mechanisms are both varied and specialized. [TrackIT Corporation](#) has a product available that creates a "maximum separation zone" around the user and the laptop. The idea is simple enough: if the user move out of range of your device, or is moved out of range of the user, the alarm will sound. Once you move back within range, the alarm will stop. Thus, if someone tries to surreptitiously remove the laptop, the alarm will sound, drawing attention to the attempted laptop theft.

This method of protection is especially useful in busy or crowded areas such as airports or train stations where it would normally be quite difficult to track your stolen bag/computer. Unfortunately, restrictions on transmitter strength as well as susceptibility to interference from the environment, such as metal beams, other radio sources, or powerful electromagnetic sources, reduces the usefulness of this product to those areas free of such obstacles. False alarms caused by walking through a "dead zone" will not only annoy those around you, but may cause complacency when the alarm is triggered.

Another possibility is to buy an alarm that relies on nothing more than movement of the object that it is attached to. [Fellowes](#) provides just such a device that users can attach to the laptop. If the object that the sensor is attached to is moved, an alarm will sound. Entering the 3 digit security code will reset or disable the alarm once the device has been recovered.

A third option is [Caveo's Anti-Theft PCMCIA card](#), which will passively monitor the position of a

laptop computer. When the system is armed, if the sensors detect that the laptop has been moved outside of the designated work zone, several events can occur. Of course, an alarm can sound (if it has been enabled), but more importantly, Caveo can shutdown and effectively lock the computer by preventing it from booting without a proper authentication action (more on this in a moment.) It can also optionally secure the keys to your encrypted files. The Anti-Theft card contains motion sensors that monitor the angle and velocity of your laptop. Using these extremely sensitive sensors, users can create a unique gesture password that can be used to arm and disarm the system. For example, my "password" could be a tilt forward, left, back, and right. If those four movements were not performed in sequence, the system would not unlock (and may even sound the alarm).

Non-Technical Solutions: Common Sense!!

Unfortunately, people who deal with technology a lot often think that security is purely a technological issue. However, arguably the most important part of information security is to minimize human error. With that in mind, the laptop user can help to ensure the security of the laptop simply by following a few common sense solutions, such as the ones listed below.

Keep the Laptop Out of Sight

If thieves can't see a laptop, they can't steal a laptop. While showing off your shiny new Vaio to your co-workers is probably okay, carrying it around in a clear plastic bag out in the real world is just asking for trouble. When the laptop is not being used, it should be safely tucked away in a locked desk drawer or in its bag.

Choose an Inconspicuous Carrying Case

Following from the first point, choosing a flashy, expensive-looking bag will gain users more than the attention of their peers. An inconspicuous laptop is a safer laptop. Users should keep carrying implements as basic as possible. An appropriately padded school bag or backpack will do just as good a job of physically protecting the laptop while providing much better concealment from eyes looking for valuable booty.

Keep the Laptop Close at Hand

Don't start leaving your bag "just for a minute" because it may sprout legs and disappear. If

possible, remain in physical contact with it at all times. If you want, go crazy and buy a set of police issue handcuffs?pretend you're a spy carrying top-secret documents. Just don't leave your bag alone.

Label and Tag the Laptop and All Accessories

Make sure that everything that can be labeled is labeled with the name of the individual or organization that owns it, and ensure that these labels are conspicuous. The potential theft value of a laptop or peripheral is reduced greatly when additional work is required to remove the identifying marks. Conspicuous identity labels also significantly increase the risk of a potential thief being caught in the act of theft.

Communicate Employee Responsibility for the Laptop

One of the most common uses of laptops is for employee presentations at conferences and such. This means that laptops are often being used and cared for by people who do not own them and who do not necessarily have to pay for their replacement. This can be problematic. A clearly written, clearly communicated policy that states the employee's responsibility for the laptop can significantly reduce the risk of theft, if only by increasing the employee's risk awareness. While the details of employee responsibility and liability will vary greatly from company to company (and will be influenced strongly by labour and liability laws) all companies that lend out laptops should have a policy in place that spells out the risks of laptop theft, the responsibility of the user and the liability of the user. Also, the organization should have all users sign off on this policy each time a portable computer is taken out of the office, thus ensuring that the user is aware of the risk of theft and his or her responsibility in the protection and, potentially, replacement of the device.

To read **Laptop Security, Part Two: Preventing Information Loss**, click [here](#).

[Privacy Statement](#)

Copyright 2006, SecurityFocus