

LAW and ORDER

Laptop Security

by Kevin Gordon

Thefts of police laptops—and the critically important information they contain—is a major issue for administrators. According to Safeware Insurance, about 600,000 laptop thefts occurred in one recent year, resulting in \$720 million in actual losses and perhaps \$5 billion in proprietary information loss. These statistics only concern thefts, not those left behind at the hotel, airport, etc.

The Gartner Group estimates that 80% of all laptop thefts are internal by some employee or contractual employee who has permission to be on site. Laptops are stolen from businesses and agencies for the same reason cars are stolen from a shopping mall...they are there and easy to get. An estimated 59% of computer attacks can be attributed to laptop theft, and only 3% of stolen computers are ever recovered.

The recent, widely publicized Veteran Affairs laptop theft isn't alone in the area of laptop or computer security. Recent headlines have included the Bank of America, MCI, LexisNexis, etc. The typical laptop thief isn't interested in the data on the laptop and, in fact, probably isn't even aware of what data is on the laptop.

How do we protect such equipment? We start with the user—the officer who is in control of the data and the laptop. That is usually the weak link. The biggest challenge, of course, will be changing user attitudes and habits. Security consultant Paul Korzeniowski says there are three phases to laptop security. The first is the physical security of the unit, the second is controlling access to the data, and the third is tracking/recovery of the unit.

There are many methods to secure the unit, starting with a simple cable that costs about \$20. This method of tying the unit down is a start but certainly isn't theft-proof. Like a cheap lock, the cable will not prevent theft but will slow them down, but in some office environments, that may be all that is needed. Just as important is that it serves as a constant reminder to the employee that the laptop is like having \$1,000 cash on your desk, and it should be secured.

Other options include a variety of alarm sensors. Controlling access to the data by uses of passwords and biometrics as well as vendor-provided tracking can address the second and third phase of security. The proper level of security should be used, and what that is changes with each unit and situation. Don't forget such simple and often overlooked areas such as marking the laptop outer case with your agency contact info. Just like a putting a tag on a suitcase, make it easy for honest folks who may find it to get it back to you.

[Absolute Software](#), a leading provider of computer theft recovery and security asset tracking, provides a top 10 list of security recommendations for securing your laptop. 1. Use visual deterrents. A cable lock or other locking mechanism can act as a deterrent to would-be criminals. Although they can be ripped off the plastic exterior of a laptop with a strong tug, they do force some criminals to think twice before taking the risk.

2. Avoid leaving unsecured laptops unattended. Lock them in cupboards, laptop carts or other secure facilities when not in use. If they must be left in a vehicle, they should be covered up or locked in the trunk. 3. Keep laptops inconspicuous. Laptops should always be carried in inconspicuous carrying cases, such as backpacks or tote bags, instead of telltale laptop bags.

4. Use complex passwords, and change them regularly. Don't use simple passwords that can be guessed easily. Always use a combination of numbers and letters, and never leave your password in obvious places on or near the computer. Also, password-protect your screensaver to avoid unwanted access to your computer if you've stepped away.

5. Leverage anti-virus software, encryption solutions, anti-spyware and firewalls. Prevent unauthorized access and spyware from invading your computer, and protect valuable information with data encryption software. Make sure your systems are properly installed and kept up to date. 6. Back up valuable data on a scheduled basis. Data back-up needs to happen as frequently as possible to minimize the risk to organizations in the event of theft or loss. The information or "knowledge" that is stored on the computer is more valuable than the computer itself.

7. Understand the dangers of pirated software and file sharing. Both piracy and over-deployment of purchased licenses can lead to significant lawsuits or other financial penalties. Not only is it illegal, but pirated software can increase susceptibility to viruses, Trojans and other attacks. 8. Stay informed. Continue to educate yourself on the tools and techniques used today by cyber criminals, as well as the latest scams and other security risks to company data.

9. Use asset tracking and recovery software. Laptop recovery tools are highly effective, especially those based in the BIOS of computers. They not only recover the hardware but stop the root cause of internal theft by catching the thieves. And regulatory compliance today requires that companies know not only what is on a computer, but where it is, and who is using it.

10. Invest in advanced data protection. Leverage advanced data protection technology to remotely wipe sensitive information in the event that your computer is lost, stolen or nearing the end of its lifecycle.

Kevin Gordon spent 25 years in law enforcement and retired as a chief of police. He is a national and regional officer of the International Police Association. He can be reached at Kevin@KGordon.com.

This article was printed in Law and Order Magazine, September 2006.