



## Theft Prevention Strategies for Laptop Computers

There are several theft prevention strategies that you can take to protect your laptops, notebooks or other portable computing devices. Paying extra attention to the prevention of a theft can save you and your company an enormous amount of time, money and headaches trying to recover after the fact.

Cable locks and motion detectors assist in deterring physical theft, but should the portable computing device fall into the wrong hands there is still the problem of accessible data. There are a number of devices and applications that can help you to prevent access to confidential data by unauthorized people. If other access control methods fail or are defeated, data encryption systems can protect information stored on computers. The newest technology on the market are tracking systems that provide the capability to locate a laptop once it has been stolen and then booted up and connected to the Internet. There are even products available that will remotely destroy data.

Here are some strategies to protect your laptop and its data:

1. Always be aware of your surroundings and the people in them. Realize that you are target for thieves if you are carrying a laptop.
2. Never leave your laptop unattended.
3. Back up your important data daily.
4. Avoid storing valuable company data on a laptop. Store valuable data on a removable medium like a CD or zip disk, or on the company network.
5. Companies should establish a formal policy setting the appropriate security levels for different employees based on the type of data they handle. A \$40 physical cabling device may be appropriate for all users. However, more stringent access controls, authentication, file encryption or tracking services should be considered for managers, executives, or anyone who stores confidential information on their machines.
6. Cable Locks – laptop cable locks are similar to the locks used on bicycles. A steel clip provided by the manufacturer is installed on a security slot either on the back or side of the laptop. A steel cable is threaded through the clip and wrapped around an immovable object. The two ends of the cable are then secured with a padlock. While inexpensive (they retail anywhere from \$30-\$50) and easy to use, these cables can be easily defeated by tools from any hardware store.



Some sources of information concerning different versions of cable locks are Anchor Pad International ([www.anchorpad.com](http://www.anchorpad.com)), Kensington ([www.kensington.com](http://www.kensington.com)), Computer Security Products ([www.computersecurity.com](http://www.computersecurity.com)), PC Guardian ([www.pcguardian.com](http://www.pcguardian.com)), Targus Group International ([www.targus.com](http://www.targus.com)) and Kryptonite, among others.

7. Alarms and motion detectors - these devices are more sophisticated physical security measures that alert owners when someone tampers with or tries to move a laptop. Products range from simple motion detectors, to sensors that detect the unplugging of cables, to high-pitch sirens that sound similar to car alarms.

An alarm system offered by TrackIT ([www.trackitcorp.com](http://www.trackitcorp.com)) is basically a proximity device. A transmitter installed in or attached to the laptop case maintains continuous radio contact with a mobile receiver carried by the user. If the laptop is moved beyond a set distance from the user, an alarm sounds on the laptop and the mobile unit alerts the owner.

Targus offers the Defcon family of alarm units, which are basically cable locks with alarms. Defcon I is a sensor circuit that sounds an alarm if anyone breaks the security loop on the laptop or cuts the cable lock. Defcon III is essentially the same unit, except it emits a warning tone when the notebook is moved slightly and a louder alarm if movement continues.

Minatronics ([www.minatronics.com](http://www.minatronics.com)) has developed a fiber optical alarm system that acts similar to Targus's cable sensor. A fiber optic cable is passed through a security tab or any available opening on a laptop and is anchored to a stationary monitoring unit that sends continuous light pulses through the line. An alarm sounds immediately if the pulses are interrupted.

8. Smart cards - are used sparingly in laptop environments and few laptops have built-in smart card readers. However, vendors such as SPYRUS ([www.spyrus.com](http://www.spyrus.com)) manufacture portable serial port readers. More conveniently, digital certificates and other identifying credentials can be stored on Universal Serial Bus (USB) tokens from vendors such as SPYRUS, Rainbow Technologies ([www.rainbow.com](http://www.rainbow.com)) and Aladdin Knowledge Systems/eSafe ([www.ealaddin.com](http://www.ealaddin.com)). Most devices manufactured after 1998 include USB ports.

Authentication tokens such as the Secur-ID from RSA Security ([www.rsasecurity.com](http://www.rsasecurity.com)) and the DigiPass line from Vasco ([www.vasco.com](http://www.vasco.com)) are common in remote-access environments. (Similar remote login tools are offered by CRYPTOCARD ([www.cryptocard.com](http://www.cryptocard.com)).) These tokens remotely synchronize with back-office authentication servers to provide users with one-time passwords. However, while ideal for secure network authentication from a laptop or other portable computer, these devices do little to secure the device's data on its unprotected hard disk.



9. Biometrics - provides another means for blocking access by only allowing users who authenticate their identity with their physical characteristics, such as fingerprints, voice patterns or retina scans. All biometrics systems work basically the same way: A user scans his or her identifier with a capture device, which stores the pattern in a database. To access data, the user presents his or her identifier, and the biometrics system will grant him or her access if it matches the stored pattern. Unlike passwords or tokens, biometrics identifiers are extremely difficult to duplicate, crack or exploit through a replay attack.

Using scanners hooked into peripheral or USB ports, built-in laptop microphones and even laptop cameras, finger-, face- and voice-recognition biometric vendors have made strong in-roads into the laptop authentication market. For instance, the U.are.U security system, manufactured by Digital Persona ([www.digitalpersona.com](http://www.digitalpersona.com)), uses a USB-compatible sensor to capture fingerscans.

Some biometric applications for laptops combine multiple biometrics for added security. For example, Keyware's Layered Biometric Verification (LBV) system ([www.keyware.com](http://www.keyware.com)) combines spoken passphrases with optional fingerscanning. LBV also operates in "thin-client mode," eliminating the need for client-side readers or software to store credentials and protocols. Other systems combine a single biometric with a hardware device. Trinity, a system produced by American Biometric Company ([www.abio.com](http://www.abio.com)), offers optional packages that bundle biometrics with smart cards, tokens and password applications for multifactor authentication. Ethentica ([www.ethentica.com](http://www.ethentica.com)) offers a fingerprint verification system on a swappable Type II PCMCIA card, called the Ethenticator MS 3000.

10. In addition to traditional data encryption and digital signature software from companies such as PGP Security ([www.pgp.com](http://www.pgp.com)), F-Secure ([www.f-secure.com](http://www.f-secure.com)), RSA Security and PC Guardian, several vendors are offering notebook encryption hardware via PCMCIA cards. For instance, Global Technologies Group ([www.gtgi.com](http://www.gtgi.com)) offers the CryptCard, a Type II PCMCIA card with Triple-DES hard-disk encryption capabilities. In addition, OS-specific encryption applications, such as the Windows 2000 Encryption File System (EFS), are growing in popularity in laptop environments.
11. A new generation of technology is providing users with the ability to track stolen portable computers. Similar to the LoJack vehicle retrieval system, alarm and tracking software residing in an undetectable file on the hard drive will periodically contact a monitoring service via the Internet. The service verifies the missing computer's location, which is generally sufficient for police to obtain a search warrant. The recovery rate with these tracking and locator systems is about 90% when police lend their assistance, industry experts say. However, each jurisdiction places a different priority on stolen computers, and some police departments may not want to allocate resources to recover a single machine. Even with the help of authorities, recovery is a slow process-averaging about three months.



Through its monitoring center, CompuTrace ([www.computrace.com](http://www.computrace.com)) routinely updates its security application running on subscribers' laptops with new call-in schedules. Should a machine be reported stolen, the system will be programmed to increase the time between calls, which allows for a faster trace and recovery. Similarly, Lucira Technologies ([www.lucira.com](http://www.lucira.com)) markets Secure PC, an application that traces stolen laptops once they're connected to the Internet. The company's monitoring center will notify the local police of the laptop's location and even provide them with a map. The company plans to improve future versions by offering data and file retrieval without the thief's knowledge. It will not, however, wipe the hard drive clean.

Cyber Angel, by Computer Sentry Software ([www.sentryinc.com](http://www.sentryinc.com)), provides both monitoring and retrieval capabilities. Should anyone attempt to access the Internet with the laptop, Cyber Angel will immediately alert the owner via fax or email. The CSS operations center will use the initial notification to trace the laptop's location. After the alert, the program locks the modem port to prevent access to a corporate LAN, the Internet or other remote operations. An optional software module can also lock out the keyboard and mouse, making the machine virtually useless.

12. Another effective method of protecting a laptop 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. Also, when the laptop is locked in the Anchorpad Sentry, all of the PCMCIA cards and peripherals are also secure, protection that a security cable cannot provide.
13. You can also set up the destruction of information on a computer if it has been stolen and it is critical that the data not fall into the wrong hands. Beachhead Solutions ([www.beachheadsolutions.com](http://www.beachheadsolutions.com)) markets software called Lost Data Destruction. This client-based agent determines whether the computer is lost or stolen, based on pre-set, customer-designated rules. The destruction of customer-designated data is triggered in a pre-determined sequence if the computer is determined to be lost or stolen. The destruction mechanisms for any file, folder or drive, are all set on the server. Also, encryption prevents the data from being read if the hard drive is removed.

Disclaimer: There are many companies that have products that address laptop and data security. The ones mentioned above were found in our research. We do not endorse them or their products in any way.



(Sources: [http://infosecuritymag.techtarget.com/articles/february01/features\\_laptop\\_security.shtml](http://infosecuritymag.techtarget.com/articles/february01/features_laptop_security.shtml)  
<http://www.securityfocus.com/printable/infocus/1186> , [http://beachheadsolutions.com/lost\\_data.php](http://beachheadsolutions.com/lost_data.php)  
<http://www.csoonline.com/read/070104/laptop.html>, <http://www.officelock.com/Laptop-Security.htm>