Global Information Assurance Certification Paper

Laptop Computer Security
Richard Childers
October 30, 2000

This paper discusses the issues surrounding laptop computer security and offers some basic approaches to securing laptops.

A laptop can be quickly dropped into a bag or slipped into a binder and carried away. Recent crime statistics show laptop computers are becoming the target of choice with thieves. According to the latest loss statistics, published by Safeware Insurance company, 319,000 laptop computers were reported stolen in 1999. In addition to thieves, people engaged in information espionage, also target laptops as rich sources of sensitive information, information that is usually completely unprotected and available once the laptop containing it is acquired.

While the loss of an asset worth between $2,000 to $7,000 is a serious concern, the loss of the data contained on the laptop is often more important and valuable than the cost of the laptop itself. It is not uncommon for a laptop to be a portable office containing contact lists, customer information, product plans, business plans, financial information, proprietary software and other confidential information that could cause great harm in the hands of a competitor.

Despite the security risk, laptop computers will continue to increase in popularity as their processing power increases and physical size diminishes. Given that laptops will not go away, what steps can be taken to reduce the risks of using this technology?

One of the side benefits of the high theft rate of laptop computers is the growing number of companies offering security solutions. There is a wide choice of solutions ranging from simple cable locking systems to complex 911 type tracing software that can locate a stolen laptop when it is connected to the Internet. None of these solutions is a magic bullet. Each addresses particular security risks. Therefore it is essential to select those solutions that are appropriate and proportionate to the value of the laptop equipment and data you need to protect. For example a cable locking system might be sufficient for the average home user or middle manager. But for a top executive or senior government official encryption software and tracking software is warranted due to the potential harm that the loss of confidential information could cause. The key point is to look at the risks and determine what level of security makes sense to deploy.

Just as you shouldn't depend only on a firewall to protect your network, you shouldn't depend only on one method to protect your laptop assets. At the minimum, implement security mechanisms to protect both the physical asset and information contained by the laptop. A layered security approach makes it difficult for thieves to steal the laptop and difficult for them to sell it. Reducing profitability encourages thieves to look elsewhere for easier targets.

With this in mind the following seven steps are recommended to secure laptop computers.

1. Develop a laptop security policy.
2. Prepare laptop safe practices guidelines.
3. Identify your laptop assets with tamper resistant tags.
4. Provide physical security using a cable locking system.
5. Backup up the laptop data on a regular basis.
6. Use encryption to protect data on your laptop.
7. Establish standard procedures for staff to follow when their laptop is stolen.

Start with a laptop security policy. The policy designates what security measures are to be employed to secure laptop computers at your company. This policy should specify who is responsible for implementing these security measures and describe how compliance with policy is verified. The policy can also provide some direction on what procedures to follow when a laptop is reported missing or stolen.

Next develop a set of safe practices guidelines to raise laptop users awareness of common high risk situations where laptop theft can occur. By Increasing staff awareness many laptop thefts can be prevented. A safe practices guide is a low tech, low cost measure that can significantly reduce the number of laptop thefts your company experiences.

Another relatively low cost measure is to identify your laptops to make their recovery easier and the resale on the black market harder. There are a number of solutions available to identify your laptops. For example tools are

available to permanently engrave or brand a serial number and company name and logo on to a laptop, such as the electric engraver shown in figure 1.

Figure 1. Hand-Held Dremel® Electric Engraver
www.seton.com

There are also a variety of tamper resistant tags available that can be applied to the laptop to identify the asset as belonging to your company. One well known anti theft tag is the Stop Tag shown in figure 2.

Figure 2.

The manufacture of the Stop Tag states it takes 800 pounds pressure to remove this tag. Even if the tag is removed from the laptop there still remains the tattooed message "STOLEN PROPERTY" for the thief to deal with. This Stop Tag can be obtained from World Security Corp (http://www.worldsecuritycorp.com).

Physical security can be addressed using either a simple cable locking system or a locking system the employs a motion detector with an audible alarm. There are many manufacturers of cable locking systems. Prices run in the $40 range depending on the quality of the cable. The Kensington, in figure 3, is one of many manufacturers that sell a quality locking cable. The principle benefit of using a cable locking system is it prevents spur of the moment thefts. The thief must come prepared with cable cutters to steal a laptop.

Figure 3. Locking cable by Kensington:
http://www.kensington.com/

Unfortunately too many thieves these days are equipped with cable cutters. This has prompted many companies to consider deploying a cable locking system equipped with an audible alarm system that sounds should the cable be cut or the laptop moved. The DEFCON alarm system, in figure 4, is a good example of an alarm product. Pricing is in the $45 range depending on quantity ordered.

Figure 4. DEFCON by Targus
http://www.targus.com

Even the best measures to physically secure a laptop will not guarantee against theft, accidental loss or carelessness, therefore steps must be taken to protect the data stored on the laptop. The first and perhaps most basic step is to educate laptop users to backup their data on a regular basis, both at work and while travelling. At work, important files can be copied to network shares on the company file servers. When on the road, files can be backed up to floppy disks (but make certain these disks are kept in a separate bag from the laptop). There are also a number of online backup alternatives available to modern road warriors, such as:

- Driveway Corporation (25Meg Free Storage) http://corp.driveway.com/
- thedatabank.com Inc. http://www.thedatabank.com/def.htm
- BackupNet International Inc. http://www.backup.net/
- NovaStor Corporation http://network-backup.com/
- Synectics Business Solutions Inc. http://www.backjack.com/

Backing up files protects against data loss or corruption. But it doesn't protect the confidentiality of the data should the laptop be stolen. To insure confidentiality it is necessary to encrypt the data stored in the laptop. There are a great many encryption software programs available on the market today. When selecting encryption software make certain the algorithms used are in the public domain and not proprietary. Only algorithms that have been publicly examined by cryptographers can be trusted to be secure. Triple DES, Blowfish and CAST are examples of public domain algorithms.

One approach to hard disk encryption applies encryption either to user selected files and directories, or creates encrypted volumes on the disk drive into which the user places confidential files. This approach relies on the user to encrypt confidential data, or ensure the confidential data is storied in an encrypted volume. If the user forgets, or chooses not to do this then the data is not protected. Another concern is that cached data and temporary files may not be protected unless they are specifically identified to be encrypted. Some companies that provide this type of encryption are listed below:

- PC Guardianhttp://www.pcguardian.com
- PC Dynamics http://www.pcdynamics.com

- Reflex Magnetics Ltd. http://www.reflex-magnetics.com

Another approach encrypts the entire hard drive and leaves nothing to the discretion of the user. Using this approach the user simply logs onto the laptop at boot up, provides a user name and password and then continues to work as normal. A company that provides this type of encryption is Protect Data Security Inc. (http://www.protectdatasecurity.com). Their encryption solution has the important advantage of not letting the end user decide what data to encrypt or not to encrypt. Everything is encrypted. Boot protection is a key component of this approach, in that, it allows only authorized users to access the data on the hard drive. The user must input a user name and a quality password at boot up to access the hard disk. Without the correct user name and password, the laptop hard disk must be formatted and a new operating system installed before the laptop is usable. The product is also designed to be managed from a central helpdesk which makes supporting large numbers of laptop users economical.

The final step is to develop a standard set of loss procedures for staff to follow when a laptop is stolen. Provide these procedures to laptop users when they first receive their laptop. The help desk should also have a copy so they can provide staff with consistent support when they call to report a theft. These procedures should cover such items as:

- Reporting the loss to the police with the laptop's serial and model number.
- Notifying your company help desk of the theft.
- Reporting the stolen laptop serial number to a stolen computer registry, such as Nacomex USA (www.nacomex.com) or the National Computer Registry (http://www.pcid.com).
- Document the confidential files storied on the laptop, and verify if and where back up files are available.
- Determine if clients are affected by the loss and notify them if appropriate

The seven steps outlined in this paper provide a solid basis for securing your laptop computers. They cover policy, user awareness, physical asset protection and data protection. While physical protection is perhaps the easiest to implement don't shy away from protecting the data on your laptops. Treat it with as much attention as the data on the corporate servers. When the CEO's laptop goes missing you will sleep better knowing no one can read and disclose those confidential files.

References

Schwartau, Winn " Laptop Security"
URL: http://stratyx.dyndns.org/nt/tips/laptopsec.htm

Elder, Jim and Keller, Daniel P "Nearly Everything You Need To Know About Laptop Security" November 1999,
URL: http://www.aegisprotect.com/cyber-journal/Cyber-Journal%20theft%20of%20laptop11-99.html

Na'eh, Bouki and Navon, Eran " Notebook Computer owned by the Mossad's Deputy Chief gets stolen and traded for drugs"
URL: http://www.inforwar.com.class_2/99/class2_020999a_j.shtml

Borenstein, Seth and Poletti, Therese "How loose is your laptop"
URL: http://www0.mercurycenter.com/svtech/news/indepth/docs/laptop061500.htm

Schultz, Teri and Kehnemi, Sharon "Albright Tightens Security after Missing Laptop"
URL: http://www.foxnews.com/national/042400/laptop.sml

Vijayan, Jaikumar "Intel standard aims to tighten notebook security" May 15, 2000
URL: http://www2.itworld.com/cms/ett_content_article/0,2849,1_1839,00.html

Safeware Insurance's 1998 Loss Study - May 1, 1999
URL: http://www.safeware.com/99pressreleases.htm

Security Tips - Laptop computers
URL: http://www.rcmp-grc.gc.ca/tsb/pubs/bulletins/bull42_5.htm

The Cost of Laptop Theft From Wally Bock's Briefing Memo
URL: http://www.brockinfo.com/docs/laptheft.htm

Most Reported laptop thefts occur inside the office January 26, 1999

URL: http://www.kensington.com/about/press/security012699.html

Laptop Security
What's the best Way to ensure your Notebook and (probably more important) your DATA doesn't get stolen?
URL: http://www.notbookreview.com/security.html

Safeguard Your Laptop - Tutorial
URL: http://www.duluthnews/dnt/krt/laptop/html.2.htm

Stop Tag Computer Security
http://www.worldsecuritycorp.com/stop_tag_brochure.htm

Last Updated: July 24th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor