Global Information Assurance Certification Paper

Colin Kwok
Security Essential GESC Practical Assignment
Version 1.4b, Option 1
May 22, 2003

Corporate Laptop Security Guide

Abstract:

Using a corporate laptop outside the corporate firewall may be making a hacker's dream come true. Every time an employee logs onto the Internet, any hacker can access the files in the laptop. Even worse, it could also bypass the corporate firewall and access the victim's corporate network with Virtual Private Network (VPN) tunnelling and encryption technology. Laptop has been targeted not only for it's physical worth but also for the sensitive data contained within.

Introduction:

Laptop computer is the common place today and so is their theft. Laptop theft is catastrophic for the victim. Most of the time, losing a laptop often does not matter as much as losing the data it contains.

According to the Safeway Insurance group, there were 53% more laptops stolen in 2001 than in 2000. The total number of stolen laptops will continue to be high over the next few years as laptops are becoming more and more popular. The average financial loss resulting from a laptop being stolen grew by 44%, from $62,000 in 2000 to $89,000 in 2001; just a small percentage of the sum actually relates to the hardware cost. The total financial loss due to laptop theft has been second only to loss due to computer virus over the past seven years[1].

In 2002, Fortune 1000 companies experienced losses of more than $45 billion from thefts of proprietary information, according to the American Society for Industrial Security[2].

Think that this someone else's problem and the chances that it will happen to us are slim? I had the exact thinking until couple years ago. About one dozen of few week new laptops were stolen after a break in one day in the office. It completely changed my thinking. I cannot express enough the anger and hopeless feelings that the users felt when they heard that their files and data were gone permanently especially for those users who liked keeping everything on their laptop instead of the network drives.

A stolen laptop is not simply talking about embarrassment, inconvenience and value of the computer itself, but it also leads to even serious network security problems if the laptop and the information is in the wrong hands. In fact, an FBI study revealed that 57% of all network breaches were originated from stolen computers[3]. Each IT security breach costs UK firms a turnover of more than US$ 144,000.

In an incident of a missing unattended laptop from the U.S. Department of State's Washington, D.C., headquarters, two top-level system administrators were fired and four others received career-ending reprimands for losing laptop that contain sensitive nuclear weapons proliferation data[4]. This has clearly indicated that not only users but also IT personnel are responsible for the security of the computers and related equipment.

I am confident that you have already heard some or more horrific stories about missing or stolen laptop computers. I think now is the time to take a close look at actions we can take to prevent laptop computer theft. One of the main factors is the awareness and common sense of the laptop users while planning and technology will also play important roles.

We have understood why protecting laptop is very important. Now we will find out how we can protect the laptop and the data within. We will look into physical security, data protection, system security and recovery. We will find out how we can protect the laptop, using the built in security measures from the laptop and operating systems, as well as third party products and tools.

Physical security:

Most common places reported for missing laptops are at airports, offices, convention centers, public washrooms, waiting areas, public transits and taxis. Physical security is pretty straightforward and involves lots of awareness and common sense. Protect your laptop as you would safeguard other valuables while traveling.

Use a non-descriptive carrying case
The carrying case shipped with your laptop most of time is very fit, convenient and handy for the model of the laptop purchased. Instead of using the carrying case with the big laptop manufacturer's logo on it, consider buying a form fitting padded sleeve for your laptop, and carrying it in a backpack, courier bag, briefcase, or other common inconspicuous carrying bags. It will effectively fade away a theft's attention to other potential targets.

Engrave the laptop or use of Asset Tag
Use metal tamper resistant commercial asset tags[5] or permanent engraving on the outer case of the laptop with your company name, address, and phone number and it may greatly increase your odds of getting it being returned if missing. Clearly marking your laptops deters thieves and may prevent it from simply being resold in underground markets because of the markings and red tapes.

Get a cable lock and use it
Almost all laptops nowadays are equipped with a Universal Security Slot (USS) that allows them to be attached to a cable lock or laptop alarm. While it may not good enough to stop professional thieves with a bolt cutter, it will effectively deter casual thieves. If you can connect your laptop to a docking station, always access the station's built-in locking device.

Never leave your laptop unattended in your office or hotel room unless you have secured it appropriately or hidden it out of sight. In case you need to leave your laptop in your car, make sure to lock it under the metal trunk or out of sight.

Register the laptop with the manufacturer
Fill up the registration card with the serial number and other related information and send it back to the manufacturer. It not only activates the product warranty, but it will also increase your odds of getting it back missing or stolen. If a thief ever calls in for technical support or sends it in for maintenance, the manufacturer will alert the authority and trace the laptop for you. Remember to keep a list of serial numbers and production information like lots of people do for their credit cards. In case a laptop is missing or stolen, police will definitely need that information in to order to trace it back to you.

Data security:

Today's world is filled with threats to your information systems' security and personal computers. How do you recognize and safeguard against these security threats to the priceless data in your laptop? It takes more than a firewall, a security policy, and a locked door to keep out the viruses, hackers, and worms. Information and data is priceless. We are looking into how we can lock down the threats and protect the data stored in your laptops. We will try to preserve the data in case the laptop goes missing or is lost and end up in the wrong hands.

The 'human element' will always be the weakest link in the security chain. Therefore, management should remember to include training and other "social" elements when determining a security solution.

Use and enforce Security policy
Security policies are an absolute must for any organization. A security policy is typically a document that outlines specific requirements or rules that must be met. They will also directly reflect the unique needs of your organization. Security policies and baseline security standards underpin the security of your information and your organization. Just having a security policy document itself is not enough, the contents must be delivered effectively and enforced to have the desired results. Any employee found to have violated a security policy might be subject to disciplinary action, up to and including termination of employment.

Enable a strong BIOS and Hard drive password
The very first line of defence for your data is to enable a strong BIOS password. Once BIOS password is enabled, the thief needs to enter a correct password before the system will boot up. Some laptop manufacturers will also provide a feature of hard drive password. Once enabled, no one can access the information on the hard drive without keying in the correct password.

Employ a more secure operating system and lock it down
Choose an operating system that can provide secure logon, file level security and data encryption ability. Microsoft Windows 2000 Profession and Windows XP can provide these features. Lock down the system by disabling all the unnecessary built-in services. For example, Internet Information services should be removed from the system if you are not going to host a website on your laptop. In addition, it would be much more secure to completely uninstall all unneeded services instead of just disabling them from the start up.

Use the NTFS file system
Install Windows NT/2000/XP on NTFS files system all the time. For any reason that this cannot be allowed, such as on a multiple operating system machine, at least store your sensitive data on a NTFS partition on your laptop and apply the folders and files permissions. With the file level security and data encryption features provided by the Windows 2000/XP, it only runs on NTFS file system and not any other file systems.

Enforce file and folder permissions
File and folder permission is set to Full Control for Everyone in Windows by default. Network administrators and IT Managers should plan and enforce the file and folder permission once the operating system has been installed. Providing minimal file and folder permission to groups and assigning them to users is still one of the simplest ways to help protect files from illegal access.

Disable the Guest Account and disable display last logged-in user
To successful log onto a computer, matched user name and password is required. Windows 2000/XP disables Guest account by default. Removing display the last logon name will dramatically decrease the chances to break into the laptop by hackers. It can be easily done by enabling "Do not display last user name in logon screen" under Security Options in the Local Security Settings[6]. It will definitely prevent hackers from using password guessing or brute force attack, as no user name is known.

Enable strong password
The password is one of the main defences for unauthorized system or data access. Always use strong passwords to protect your data[7]. A good password should contain at least eight characters with letters and numbers that cannot be found in any kind of dictionary and should be changed regularly. To enforce strong password in Windows 2000/XP, it can be done by enabling "Passwords must meet complexity requirements" under Password Policy in the Local security Settings. Once this feature is enforced, passwords must contain characters from at least three of the following four classes: Arabic numerals, special characters, upper and lower case letters with minimum six characters long[8].

Rename the Administrator Account
Even though the default Administrator account cannot be disabled or deleted, it can be renamed. Replace it with a common name does not sound like it has special right on the laptop. You can also create a new user account named "administrator" without any rights which cannot logon locally to frustrate some amateur hackers. Unfortunately, experienced hackers can bypass this logon process by using a special Linux floppy boot disk. Disabling booting from floppy, CDROM or other removable drives from the BIOS settings will help prevent this from happening.

Assign minimum rights and permissions possible for laptop user
The network administrator or IT manager should analyze the needs of users rights or permissions for the users who will be using the laptop. The principle of least privilege is the key for any systems to enhance security. Laptop users should have minimal access rights required to perform their duty. Some people think the laptop user should receive full administrative rights so that they control their computers without any problems. It is indeed very wrong thinking. In fact, from my experience, it can create lots of other problems in addition to the weakening of security.

Enable EFS (Encrypting File System)
Microsoft offers a powerful Encryption File System (EFS) since Windows 2000 to provide additional layers of security for data storage. It must work on top of NTFS file system and employs PKI technology to guide files and folders. It will help prevent a hacker from accessing your files by physically mounting the hard drive on another computer and taking ownership of files. Without the user's private key, users can access or decrypt the data only through an account that has been authorized as a recovery agent. The administrator is the default recovery agent in Windows 2000 while there is no default recovery agent in Windows XP. Be reminded that when an encrypted file is copied to other non-NTFS partition on the same disk or other media, the file will lose its encryption feature.

Much data encryption software is available on the market providing a wide range security levels. However, it is illegal to possess encryption software in some countries. Consult a travel security expert to avoid the risk of legal problems before traveling overseas.

Disable Infrared Port on laptop
The Infrared port is getting popular nowadays as it can be used to hook up printers or to transfer data between laptop and other electric equipment without a cable connection. As same token as wireless network, someone can access your files using IR port if it is enabled. Disable the IR port though the BIOS settings by just putting an electrical tape on top of it.

Apply patches and hot fixes
It is important to keep up-to-date with both service pack and hot fixes as they always patch important security holes. However, it is just as important to test them in your environment before apply them to your production systems. Although software suppliers in general have extensively tested their patches and hot fixes before releasing them to their customers, as your might have already heard, there are always some cases where some patches or hot fixes cause other problems because of conflict between other software or hardware within the system.

Deploy Smart card and EToken

A Smart card[9] is one of the latest additions to the world of security. Similar in size to today's plastic card, the smart card has a microprocessor or memory chip embedded in it that, when coupled with a reader, has the processing power to provide many different applications. As an access-control device, smart cards make personal and business data available only to the appropriate users. Smart cards provide data portability security and convenience at the same time.

Etokens are technologically identical to Smart Cards but are designed to fit into a key chain. It does not require any card readers or user configurations, Smart Etoken simply plugs directly into an USB ports to function.

These smarts cards or Etokens can remotely synchronize with back-office authentication servers to provide users with a one-time password. It is one of best solutions for secure network authentication for remote laptops to connect to a corporate network.

Make use of Biometrics

Biometrics[10] technology is the hottest item in all security related industries especially after the September 11th attack. It provides new measures for blocking or denying access by only allowing users who authenticate their identity with their physical characteristics such as fingerprints, facial recognition, hand geometry, iris pattern, retinal scan, voice recognition etc. All biometric systems work basically the same way. Firstly, a capture device scans and saves the identification of the user on record. To access data, the user presents his/her identification and the system will grant permission if scanning results match the stored pattern. Unlike passwords or tokens, biometrics is extremely difficult to crack, duplicate or exploit through a replay attack.

Disallow wireless card and wireless networking

With the big drop in pricing and improvement in performance and stability, wireless networking is becoming more popular especially in home networking. The down side is anyone can pick up the signal with the same frequency and capture your transmissions. Even worse, hackers can access your data or read your email as easy as in a Local Area Network (LAN) within the wireless working range. For a corporate laptop with business and sensitive information stored within, it is not recommended to communicate or transfer data to other computers through wireless link unless a reliable tunnelling and encryption system is employed between the connections.

System Security:

If you are ever planning on hooking up your laptop to the Internet or a corporate network while on the road, remember that unless you have your anti-virus software with up-to-date signatures or definitions, and a good software firewall in

place and enabled, you are surely asking for troubles. The use of a combination of anti-virus and personal firewall software has proven to be an effective way to protect your laptop from virus and hackers' attacks.

Disable unnecessary services

Many services are enabled by default when installing the operating system. Make sure you know what is running on your laptop. Network administrators and IT Manager should analyze the needs of the users and should disable all the services that will not be required for operating. Netstat is a handy tool to show what is actually running or listening on your systems.

Some experts also suggest disabling Universal Plug and Play as this service may lead to certain vulnerabilities and security threats to the system. For further information and discussion on this, please refer to
http://grc.com/unpnp/unpnp.htm

Type of software based Firewalls

Software firewall is a program that runs on computers, and blocks any unauthorised incoming packets In general, corporate based and personal firewalls are the two main types of firewall. Corporate based firewalls are set up to protect network servers and workstations and prevent intruders from hacking back into their systems via the company's Internet connection. But once users leave the corporate buildings and connect to the web from home or a hotel room, their data is vulnerable to attack. Personal firewalls can be used to protect your laptop from unauthorised access attempts normally attempted though Internet or network connections.

Employ a personal firewall on your laptop

Microsoft ships out a basic firewall with its Windows XP operating system, it provides basic packet filtering feature but does not attempt to manage or restrict outbound connections at all. Personal firewalls[11] such as ZoneAlarm and BlackIce offer an effective and inexpensive layer of defence. This software can be easily configured only to block hacker attacks that use standard protocols such TCP or UDP ports and to allow chosen programs to access the Internet. In case of emergency, it also has an emergency stop button that allows you to block all access to the Internet immediately.

A wrongly configured firewall is worse than being without a firewall. At all be familiar with your firewall software, including having your own technical people show you how to modify settings and make sure you understand how it works.

Keep in mind that firewalls protect your computer from unauthorised access attempts. Although a firewall stops hackers from getting in, it will not remove any existing 'backdoor' software from your machine. For this, you will need anti-virus and anti-spyware products.

In order to test how much information your personal firewall can leak out to the Internet, try to run the leak test online from Gibson Research Corporation website http://grc.com/lt/leaktest.htm. Check and keep maintaining your firewall application in good shape.

Use Anti-virus software

Most of the anti-virus software[12] available on the market can do the job in terms of preventing your system from virus or worm attacks. However, the most important thing is that users make sure they are running the latest virus definitions or signatures and enable detection at all time. Otherwise, your computer is still not protected from any virus newer than your definitions or signatures.

More than sixty four thousand viruses have been found and on average, more than 500 viruses are discovered per month. There is always a leak time between when a new virus is found and when updated definitions or signature become available. This is the most dangerous period and we have learnt a good lesson from the famous "I Love you" virus. It absolutely requires users to be aware in order to reduce the chance of virus attack at all times. The following is the review of the most common tips to prevent virus infection on your laptop.

- Do not open any files from any unknown and/or suspicious source.
- Do not open any file attachments from email unless you know what it is. If in doubt, confirm with the sender as some viruses can replicate themselves and spread though emails.
- Do not open any file attachments with a questionable or suspicious subject line. Always save the file onto the hard drive first if you really need to open it.
- Do not download any files from unknown websites.
- Be cautions when downloading files from the Internet. Make sure the web source is a legitimate and reputable one.
- Do check with your IT staff or search well known security vendors' website for more information if in doubt.
- Do download the files to the hard drive or a floppy disk and test it with your up-to-date anti-virus software before opening.
- Do report to your anti-virus vendor if you find any potential virus related files or situations.

Many new viruses and worms contain Trojans or have backdoor capability. Once the computer gets infected with this type of virus, the hacker can easily use a remote control client to access or hi-jack your computer whenever the computer is connected to the Internet.

Be aware of Adware and Spyware

Adware is a software application in which advertising banners are displayed while the program is running. Spyware is software installed quietly in the user's

computer and can send data back to a third party without asking the user's permission. Spyware usually collects demographic and usage information from your computer, usually for advertising purposes. Even though Adware and Spyware are technically different, Adware and Spyware can be run in the same software at the same time. In addition to privacy and security concerns, resource-hogging Adware and Spyware can cause system and browser instability and slowness. Soon, you will find that your mailbox is filling up with piles of advertising junk emails.

Freeware, shareware and lot of out-of-the-box software may contain Adware as well as Spyware. Sometime, product updates may change a previously Ad-free version into an Adware product. All this makes for a confusing mess and users need to pay full attention when installing any type of software and really read the software agreement. Avoid Spyware[13] at all costs as it is not easy to detect without special tools. Install a firewall and be on guard as to who is asking for permission to connect online

Use VPN (Virtual Private Network) for remote connection

Now, many companies are creating their own VPN[14] (virtual private network) to accommodate the needs of remote employees and distant offices.

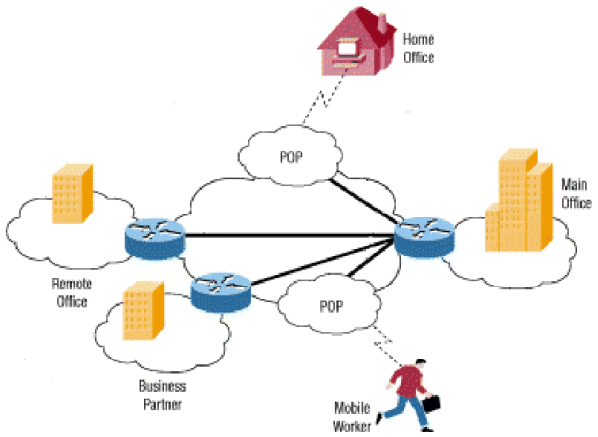

Image courtesy Cisco Systems, Inc

A Virtual Private Network (VPN) is a private data network that makes use of the public networks including but not limited to Internet in maintaining privacy through the use of tunnelling, such as PPTP or IPSec over L2TP technologies. The main purpose of a VPN is to provide the same capability and security as private leased lines at a much lower cost and without special installation by using the shared public infrastructure.

In order to remotely and securely connect to the corporate network, VPN is one of the most convenient and easy ways to achieve the requirements. With an Internet connection, a laptop user can use a VPN to create a private tunnel

through the Internet to connect to a corporate remote access server. In addition, all the data will be encrypted during transmission through the VPN. Make sure you disable the Internet connection sharing for the VPN connection from the Network and dial up connections.

Use of PKI and certificates
With the use of a VPN, there is a big problem with key management. PKI or public key infrastructure will take care of the authentication and integrity requirements to establish a connection securely. Public-key encryption uses a combination of a private key and a public key. The private key is known only to your computer while the public key is given by your computer to any computer that wants to communicate securely with it. To decode an encrypted message, a computer must use the public key, provided by the originating computer, and its own private key. A very popular public-key encryption utility is called Pretty Good Privacy[15] (PGP), which allows you to encrypt almost anything.

Backup and recovery

Backup your data regularly or disk clone your hard drives
It's needless to stress the importance of backing up your data regularly as everyone should have known about it. It is indeed a lifesaver. Thanks to the removable storage technology such as CD writer, USB memory sticks, PocketZIP[16], ZIP drives and external hard drives within built-in backup software, personal backup for laptops can be done in just a matter of a few mouse clicks away.

Disk cloning[17] can copy the entire contents of one disk to another or to a compressed image file. It can restore your data and/or operating system back or mounting onto another laptop in few minutes of time. Back up the data in an encrypted form, password protected if possible, keeps it in a safe place. Most important is to make sure to save your backup media or drives in a secure place and carry them separately from the laptop or the laptop's carrying case.

Use tracking software to trace your laptop
Many commercial stealth software enables your laptop to check in to a tracking center periodically though Internet connection. In the event your laptop is lost or stolen, these agencies work with the authorities and Internet service providers to track and recover your laptop. CompuTrace, SecureIT, Stealth Signal, and Ztrace[18] are some examples of companies who can provide tracking services for corporations and individuals.

Conclusion:

Don’t be the next victim! A determined thief or industrial spy may still be able to get to your laptop if they set their mind to it, but why make it easy for them? It is more important than you think to make sure your laptop computer does not end up in the wrong hands. Arm yourself now and protect your laptop as well as your priceless data. Use common sense when traveling and try to stay in physical contact with your laptop at all times. If you are traveling with trusted friends or business associates use the "buddy system" to watch each other’s back. No product can ensure complete security on its own. Make sure your system is up-to-date in terms of product patches, current anti-virus software with updated signatures or definitions, reliable firewall and back up your data regularly. Do not forget to carry or save your backup media separate and away from your laptop. Although people are the weakest link in the security chain, the key for all computer security is knowledge, training and common sense. Users have to follow the policy/procedures and do their own share in order to protect their laptops in terms of both physical and data security. Be reminded that you have not only lost a laptop computer but the date you lost can cause harm to your job or business. Security Starts with Users and make security a habit.

Reference:

1. Laptop theft statistics
URL: http://www.microsaver.com/tips/tip_1028.html
*Safeware's industry esitmate is projected from actual reported claims by the company's national client base.

2. Laptop loss statistics
http://www.nwfusion.com/net.worker/columnists/2001/0326zbar.html

3. FBI security studies
Source: 2002 Computer Security Institute/FBI Computer Crime & Security Survey

4. Missing notebook computer in U.S. Department of State's Washington, D.C., headquarters.
http://www.infosecuritymag.com/articles/february01/features_laptop_security.shtml

5. S.TO.P. Theft prevention tags
http://www.computersecurity.com/stop/prevention.htm

6. Security policy
http://www.sans.org/resources/policies/#resources

7. Disable last logged-in user name
http://support.microsoft.com/?kbid=310125

8. Enforce windows complexity password
http://support.microsoft.com/default.aspx?scid=kb;en-us;279890

9. Smart cards
http://www.smartcardbasics.com/overview.html
http://www.smartcardclub.co.uk/smartcards_guide.htmlhttp://www.uk.rainbow.com/ikey/

Etokens
http://www.loc.gov/z3950/agency/zing/srw/token.html
http://security1.gartner.com/story.php.id.113.s.1.jsp
http://www.atstake.com/research/reports/acrobat/rr2001-04.pdf
http://www.articsoft.com/index.htm

10. Biometrics:
http://www.biometrics.org/html/introduction.html
http://www.sibgonline.com/public/index2.asp
http://www.biodigest.com/

11. FireWalls
http://www.firewall.com/
http://www.zonelabs.com/store/content/home.jsp
http://blackice.iss.net/

12. Anti-Virus software
http://www.symantec.com/
http://www.mcafee.com/
http://www.trendmicro.com/en/home/us/enterprise.htm

13. Anti-Spyware and Adware
http://www.lavasoftusa.com/
http://www.cexx.org/adware.htm
http://www.pestcontrolmag.com/pestcontrol/

14. Virtual Private Network (VPN)
http://www.vpnc.org/
http://vpn.shmoo.com/
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/deploy/confeat/vpninter.asp

15. PGP
http://www.pgp.com/

16. Iomega PocketZip
http://www.iomega.com/na/products/product_detail.jsp?PRODUCT%3C%3Eprd_id=4971&FOLDER%3C%3Efolder_id=175253&ASSORTMENT%3C%3East_id=63191

17. Disk Clone
http://www.tlcug-ark.org/reviews/diskclone.html
http://www.powerquest.com/partitionmagic/
http://www.symantec.com/sabu/ghost/ghost_personal/

18. Tracking and Recovery
http://www.computrace.com/public/products/computraceplus/default.asp
http://homepages.ihug.com.au/~ipex/secureitpro/secureitpro.htm
http://www.stealthsignal.com/web/international.asp
www.ztrace.com

Backup
http://www.aecworkforce.com/enews/012102_trends.htm
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/ittasks/maintain/backuprest/Default.asp

Hardware Security device
http://www.secure-it.com/products.htm