

## PROTECTING YOUR COMPUTER WHILE TRAVELING

July 2008



### HOTEL SECURITY

Do not rely on the hotel room safe. Leaving sensitive government or company information in your hotel room, even in a locked briefcase or the safe provided in your room, is an invitation for material to be copied or photographed while you are out.



Hotel vaults are not much better. In most cases foreign intelligence officers can gain access to hotel lockboxes or vaults without you becoming aware of the compromise.

Many travelers succumb to what we call the "Disneyland effect," behaving as if they've left the real world—and real danger behind. This is a false sense of security.



4017 Washington Road  
Mail Stop 348  
McMurray, PA 15317  
P 888-650-0800  
F 412-291-1193

Protecting computer equipment is something that everyone should be concerned with today. It seems every week there is a news report of another stolen laptop with sensitive or confidential data on it. Some studies suggest as many as two million laptop computers are stolen each year in the U.S. and the number increases when you include those stolen while traveling outside the United States. Here is a checklist that will help you prepare and protect your computer equipment while traveling anywhere as well as at special events.

- Back-up your system before you leave.
- Take all unnecessary data off your hard drive before you go.
- Use shredder software to destroy deleted files.
- Update the operating system, firewall, anti-virus and intrusion-detection software on your laptop before you leave home.
- Turn off file and printer sharing.
- Review your passwords for strength.
- Disguise your laptop – don't use a traditional looking computer case. Always use one with a strap and put it over your shoulder/diagonal across your chest.
- Avoid leaving your computer in a hotel room. Never let the computer out of your sight – make sure someone you trust is watching it at all times.
- On computer equipment that is shipped cargo, use melted seals and plastic seals to ensure the devices have not been opened.
- Consider attaching personal anti-theft proximity devices to your bags.
- Use BIOS and hard drive password locking on your laptop.
- Encrypt folders containing sensitive data.
- Turn off your Bluetooth or WiFi connections when you are not using them.
- Use encryption like a Virtual Private Network (VPN) whenever you are using a public Internet connection.
- Set up a restricted user account on your laptop for use while you are traveling and then wipe out the account when you return home.
- Never use public Internet kiosks for any type of work, financial or sensitive information.
- While asleep or in the shower, engage both the dead bolt and the privacy latch or chain on the hotel room door.
- When leaving the room, make a mental or written note of how your suitcase or other personal property that would not normally be touched by the cleaning personnel was left. Any movement might suggest that others were in the room to examine your belongings.

While these helpful hints will increase your protection we must look at the opposite side of the equation. The following are things you should not do.

## DON'Ts

1. Do not rely on suitcase and attaché case locks. They may delay the trained professional for a few minutes but will not protect your sensitive information.
2. Don't leave anything of value in your hotel room.
3. Do not get distracted - be aware of your surroundings and where your computer is at all times.
4. Do not send anything you do not want to see on the front page of the paper.
5. Do not forget to use the anti-theft device.
6. Do not use internet cafés. Cyber spies have started to use keylogger software on public access terminals, such as internet cafes.
7. Do not forget about power adapters - use a small surge protector.
8. Do not forget the actual loss of a stolen computer is far greater than the cost of the computer itself. Some estimates say that it will cost at least \$6,000.

Traveling with computer equipment creates some additional risks and it is worth developing a plan to keep your information safe. Computers are a prime target for theft from your office, your home, or at airports, hotels, railroad terminals and on trains while you are traveling. They are an extremely attractive target for all types of thieves, as they are small, can be carried away without attracting attention, and are easily sold for a good price. Setting aside a few minutes before your trip to prepare your computer equipment and any other electronic equipment you will be bringing can save you countless hours and dollars later on.

You may want to consider having your security or IT team install Tracers that identify the location of a stolen laptop. When the stolen laptop is linked to the Internet, it transmits a signal to a monitoring station that identifies the user's telephone number or Internet account.



An ounce of prevention is worth a pound of cure! Laptop theft is rampant. Some reports even state you have a 1 in 10 chance your shiny new laptop will be stolen. And the real shocker: according to the FBI 97% are never recovered. Failure to be proactive and take these simple precautions will expose you and your organization to the risk of your computer equipment being compromised or stolen.

Place a personal proximity alarm in your laptop bag. If someone grabs your bag, within a few yards a loud audible alarm will go off.



## LAPTOP ALARMS

Use lanyards to secure your laptop whenever you will be moving around a business center or temporary office. It takes no time at all to steal a laptop. Turn your back to get a cup of coffee and it can be gone.



While suite case locks offer some minimal protection, they can be easily defeated, but that is not to say you should not use them. They can provide an indicator someone has tampered with your bags. Always make note of the placement of the number on the locks prior to letting them out of your con-

