Risk Bulletin

MARSH RISK CONSULTING · TORONTO

MARSH
An MMC Company

December 2000

Loss Prevention Guidelines for Laptop Computers

The use of mobile computing tools, particularly laptop computers, but also notebook, palmtop, and pocket systems, while enhancing productivity also imposes new security concerns. A recent estimate put the street value of an average laptop at more than $5,000. A stolen laptop, containing sensitive and valuable data can be worth far more. This value combined with concealable sizes, make laptops tempting targets for thieves. In addition, laptops are subject to all the other loss and damage exposure of PCs such as electrical surge damage, inadvertent file deletion, viruses, etc. This Bulletin is intended to provide some suggestions on safeguarding laptops against damage or theft.

Physical Protection

Be aware of your surroundings when using the laptop. The less it is used in public areas the better, from both theft prevention and data confidentiality perspectives. The following basic physical and environmental security procedures will help protect your laptop from theft and damage:

- To prevent physical damage or theft, use a sturdy, weatherproof, padded, adequately sized conservative bag which doesn't necessarily look like a computer bag. Make the laptop as inconspicuous as possible when transporting it. When carrying a laptop in a case or luggage with a strap, walk with your hand on the strap.
- Do not leave laptops unattended, particularly overnight on desktops. If your desk is in a high traffic area or an area readily accessible to outsiders, secure your laptop anytime you' re away from your desk. After hours, laptops should be secured in a locked desk or cabinet.
- Label the laptop with property identification information, preferably with 'invisible ink' which is only visible by black light.
- Engrave the organization user name and/or ID on all laptops.
- Maintain a list of current assignees, assigned equipment serial numbers and software. Assignees should keep a separate record of the laptop's serial number.
- Use a surge protector when not operating on battery power.
- If a laptop must be left in a car, keep it locked and out of sight. While riding, place the case between the drivers seat and the car seat so it won't slide around. However, most, if not all laptops have flatscreen technology which, being liquid crystal, won't tolerate extreme cold. Therefore, don't leave them in the car overnight in freezing weather.
- Batteries tend to be either lithium ion or nickel metal hydride - both of which are capable of rapid disintegration. Assure the safety cap is kept on battery packs.

Anti-Theft Devices

There are numerous ways to physically tie down the computer. Many vendors provide cable lock solutions, which take advantage of cable lock mounts built into the laptop.

- Use compatible cable lock or docking station which will secure your laptop to a desk, table, etc or lock inside your desk at night. Cable locking not only keeps the laptop from "wandering", but it also provides an obvious visual deterrent to theft.
- Always lock or secure your laptop when it's unattended. Cable locks can also be used in public places like libraries, schools, conventions, trade shows and trading floors where site security may be limited.
- Other popular anti-theft devices include:
  - **Defcon 1** (Targus Inc. - www.targus.com) which combines a stainless steel cable with motion sensor technology to create a combination locking system that attaches to the laptop computer or carrying case. If someone tries to steal the laptop or cut the cable a 110db alarm will sound.
  - **Computrace** (Absolute Software - www.absolute.com) is software that regularly connects to a monitoring centre and gives its unique serial number. If a computer is stolen, Computrace flags their system and waits until the computer calls in. Once the computer makes contact with the Computrace monitoring centre, Computrace recovery specialists work with law enforcement officers to recover the stolen computer and apprehend the criminals.
  - **SAFtyLatch** (SAFLink Corp. (www.saftylatch.com) uses voice-verification software that is used to create a password. Instead of typing a password, the user speaks the phrase (their SAFtyPIN). If it matches the approved pattern, they are in, anyone else gets rejected.

Data Security

Laptops are more vulnerable to disk crashes due to the reduced mechanical size of the drive and greater potential for dust and dirt inside cases. Consider keeping a back-up drive to allow you to back-up data, leave valuable data in your office, and reduce exposure to outside theft.

Security software should be used to prevent viruses and protect sensitive data. Highly sensitive data should be encrypted (scrambled) so that in the event the laptop is stolen, the data would not be compromised. Software security can also provide account/password access control to the laptop and to programs, directories, and files on the laptop.

The following additional precautions apply particularly to laptops because they are not only subject to data loss from viruses and human error, they are also stolen more frequently than desktop computers:

- If giving a presentation from your laptop in a public forum, ensure the infra-red port is disabled to prevent someone downloading information.
- Backup files and keep current copies readily accessible. Protect the backup disks in a secured location.
- Use password locking programs for power-on and access to confidential or sensitive files or directories.
- Use encryption programs, or file compression with encryption programs.
- Use anti-virus software.
- Limit software access. Use quality passwords (i.e. avoid passwords such as your name).
- Secure all PC related materials including disks, backups, etc.
- Report suspected intrusions and altered data.

- Do not rely on deletion commands. Format instead. Keep in mind that copy commands can move sensitive data inadvertently.
- Erase diskettes before disposal, or transfer to other use.
- Do not use unsolicited or borrowed software.
- Reformat hard drives before retiring old computers.
- Check with the manufacturer for their security suggestions and available security equipment.

Education and Awareness

The education of users is essential to minimize losses. Data theft and espionage aimed specifically at personal computers, laptop computers, networks and remote access ports is rampant. Anyone who keeps sensitive data in their computers should be informed why security precautions are necessary. Again, replacement cost is not your only loss. Consider the cost and value of:

- competitive and confidential data.
- the time it took to compile the data.
- the time it will take to reconstruct the data (or restore it from a backup, if available)
- modem telephone numbers, and mainframe passwords stored on the drive.

When this information is lost, the user and the organization are potentially vulnerable to wholesale theft, corruption of mainframe data, and sabotage via viruses, Trojan Horses, etc.

Policies & Procedures

Written policies and procedures should cover items such as:

- Responsibility and accountability for the safety and security of the assigned equipment (e.g. assignees made responsible in the event of loss of unattended or unsecured equipment).
- A signed-off copy of the policy statement should be required of all computer assignees.
- Audit annually, policies, procedures and assigned equipment and software lists.
- Loss investigations should be done for all stolen equipment.
- Reporting procedures clearly defined in the event of theft, where applicable.
- File a theft report with the local police agency where the loss occurred. As appropriate, also report the theft to management of the location of the incident (hotel, airline, bus, rental car agency, etc.).

Travel Alert: Theft Experience of Laptop Computers

Theft of laptops is common at airports. One method involves two persons who look for a victim carrying a laptop and approaching a metal detector. They position themselves in front of the unsuspecting passenger and stall until the mark puts the laptop on the conveyor belt. The first subject then moves through the metal detector easily. The second subject intentionally sets off the detector and begins a slow process of emptying pockets removing jewelry, etc. While this is happening, the first subject takes the laptop as soon as it appears on the conveyor belt and moves quickly away. When the mark finally gets through the metal detector, the laptop is gone. The subject that picks it up heads into the gate area and disappears into the crowd.

When traveling with a laptop computer, try to avoid lines to enter a metal detector, keep your eyes on the conveyor belt and watch for your luggage and laptop to come through as well as watching for what those in front of you are picking up. Other guidelines for protecting your laptop when traveling through airports:

- Never leave equipment unattended or out of your sight.
- Never check a laptop as baggage.
- Let your laptop go through x-ray, never ask for hand inspection and keep your eyes on it at all times.
- If security wants to see it operate, you handle it. Try to never let them touch the computer.
- Report any losses immediately to authorities.
- Keep serial numbers, make, and model information of your laptop computers, or of any items of value, separate from the item so you can give precise information to authorities if the items are stolen.

Another method of theft occurs while walking around in crowded areas. A traveler carrying a laptop computer on his rollbag is preceded by the first thief. Just as the traveler gets around a crowd of people, the first thief stops, causing the traveler to stop abruptly. As they stop momentarily, a second thief, following just behind them, quickly removes the traveler's laptop computer from his rollbag and disappears in the crowd.