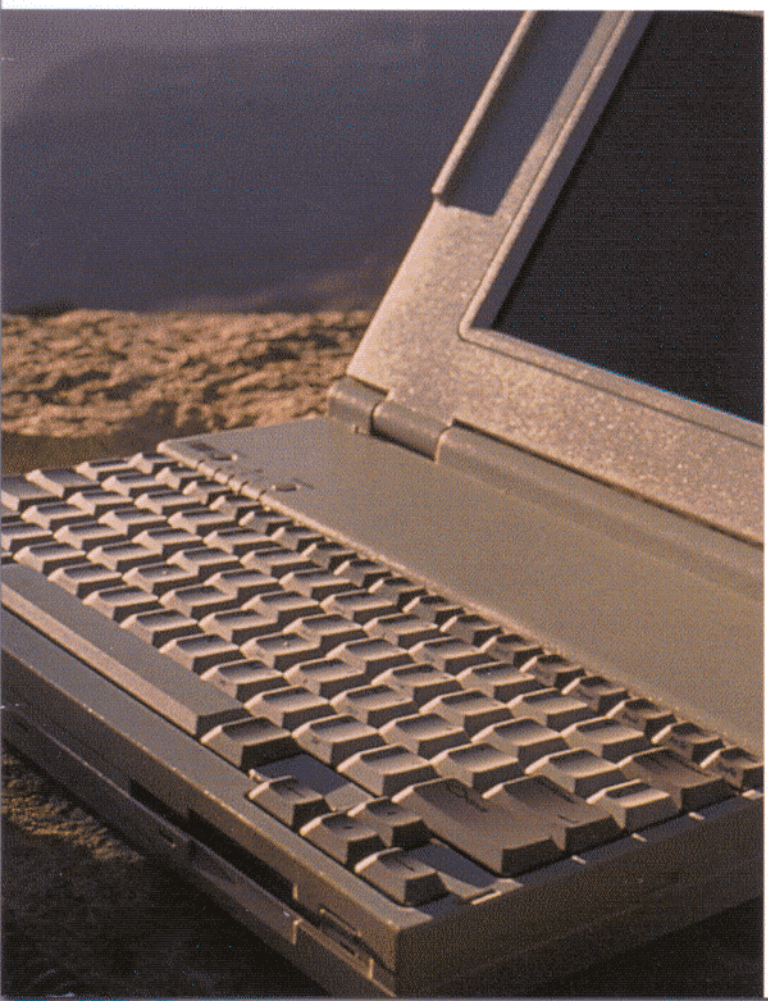
Laptop Computer Security

Loss Prevention Techniques for Companies and Employees



CHUBB

Laptop Computer Security

Loss Prevention Techniques for Companies and Employees

The rising popularity of laptop computers among business travelers has given rise to an equally popular form of high-tech crime: laptop theft.

Some thieves are opportunists, simply looking to sell a stolen laptop for a fraction of its value. Other thieves target certain companies or individuals for the valuable information typically stored in a laptop computer – including business plans, customer lists, pricing schedules and the like.

Laptop thefts are occurring with alarming regularity around the world. Anyone who owns, or travels with, a laptop computer can become a victim. The most popular targets? Offices, automobiles, airports and hotel rooms.

According to industry sources, approximately 318,000 laptops were reported stolen last year. 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.

The Internet has introduced a new potential for loss – the theft and unauthorized usage of information by cyber criminals. Technologies installed to protect information on your laptop can be compromised by cyber attacks. Information security breaches are widespread and diverse and can result in serious damages. The loss can be significant when it affects critical business information. A recent study conducted by the FBI found that 57% of computer crimes were linked to stolen laptops which were then used to break into corporate servers.

Don't become a statistic! Here are a variety of suggestions to help protect your laptop, and the information stored in it, from theft.

The bottom line: guard your laptop as you would guard you wallet.

For additional information, contact your local Chubb representative.

Physical Protection

- Use a weatherproof, padded, inconspicuous carrying case for storing and transporting laptops. Cases are now designed to look like backpacks, briefcases, even handbags, in which you can conceal your laptop.
- Store shipments of new or unassigned laptops in locked closets or rooms with controlled access and no false ceilings or partial walls.

Protective Software

The following software programs may be used to help protect and secure proprietary information and preserve data:

- Password locking programs
- Encryption programs
- Encryption programs with file compression abilities
- Anti-virus software

Locking Devices

- If your laptop can be connected to a docking station, always access the station's built-in locking device.
- Never leave your laptop unattended in the office, even for a few minutes!
- Do not place your laptop near exterior windows where it can be subjected to a "smash-and-grab" type of theft.

Airport Safety

- Keep your laptop in front of you and in sight at all times.
- Never check a laptop as baggage.
- Take extra care when passing through security checkpoints. Hold your laptop until you are ready to pass through the metal detector. Once you place it on the X-ray machine conveyer belt, do not let it out of your sight!
- If airport security asks to inspect your laptop, make sure you — and only you — handle it.

Traceability

- Engrave the company name/ID on all laptops.
- Record the laptop's identification number and keep it in a safe place.
- Check if the laptop manufacturer, or your local police department, offers an asset identification or registry program.

Storage in Cars

- If you must leave your laptop in a car, lock it in the trunk. In sport utility vehicles, station wagons and vans, safeguard it out of sight.
- While driving, store the laptop behind the driver's seat, not on the front passenger's seat!
- Avoid storing your laptop in vehicles during very cold or hot weather. If unavoidable, use an insulated case.

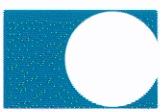
(continued)

In Addition . . .

Companies should demonstrate a serious attitude when educating employees about computer security to help control the expenses associated with such loss.

To encourage a positive loss prevention approach, companies can:

- Provide annual training and periodic reminders to maintain safety and security awareness.
- Communicate in writing its policies and procedures regarding employee accountability for the safety and security of laptops assigned to them.
- Require a signed copy of such a policy statement from all laptop users.
- Consider making loss of a laptop by gross negligence a performance issue.
- Encourage users to back up their files frequently.
- Guard proprietary information carefully — it is the lifeblood of the company!
- Maintain a current list of all laptop users, assigned equipment, serial numbers and software. Audit the list annually.
- Conduct both regularly scheduled and random inventory checks.
- Investigate all incidents of theft or accident and publicize the results.
- Make staff aware that all thefts will be reported to the police.



Chubb Group of Insurance Companies

Warren, New Jersey 07059

www.chubb.com

Form 36-01-0007 (Rev. 5/01)