Commercial Insurance Update

Topics Affecting Buyers of Commercial Insurance

MSP C 05/98 – "Laptop Computer Security" May, 1998

Laptop Computer Security

How good is your security program?

The rising popularity of laptop computers among business travelers has also given rise to a new and 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.

According to industry sources, approximately 208,000 laptops were reported stolen last year. That means there is a 1 in 14 chance that you could be next!

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

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

Physical Protection

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

Disk Drive Security

- Use a disk drive lock to prevent unauthorized access and operation.
- When possible, remove the hard disk and carry it separately while traveling.
- Check with the laptop manufacturer for other suggestions and available security equipment.

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! In addition, always

(Continued on page 2)

Published by

Cavignac & Associates

INSURANCE BROKERS

501 West Broadway, Suite 1340
San Diego, CA 92101-3505

Phone: 619-234-6848 ⋖✧⋗ Facsimile: 619-234-8601

License No. OA99520

(Continued from page 1)

use a locking cable to secure the laptop to your desk.

- 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 conveyor 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.

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.

Disclaimer: *This article is written from an insurance perspective and is meant to be used for informational purposes only. It is not the intent of this article to provide legal advice, or advice for any specific fact, situation or circumstance. Contact legal counsel for specific advice.*

Y2K: Are you ready for the Year 2000?

Our January 1998 issue of the ***Commercial Insurance Update*** addressed the "Year 2000" computer crisis. DPIC Companies has published an excellent pamphlet which deals with this important issue, and we have included a copy with this month's newsletter.