

MANAGING RISK

TWIIW

TWIIW INSURANCE SERVICES, LLC
TOLMAN AND WIKER INSURANCE • INWEST INSURANCE SERVICES
SINCE 1923

CDI LIC.
0E52073,
0357216,
0424313

Ventura • Santa Maria • Bakersfield • Monterey • www.twiiw.com

Property Insurance

Protecting Laptops on the Road

In 2003, more than 38 million Americans took at least one business trip of 50 miles or more (one-way), for a total of 210.5 million business trips during the year. Many of them took along high-tech gadgetry, such as laptops, PDAs and BlackBerries.

These items make business travelers vulnerable to theft in more than one way. First, these items are valuable, portable and easy to resell, making them an easy target for thieves. Second, they're easily visible, as business travelers often use them in public places, such as terminals and airplanes. And finally, using them requires the traveler's attention, which can make them less alert than they should be to their surroundings.

When a laptop is stolen or lost, you lose more than hardware. Losing trade secrets such as client lists, marketing plans, software code and other data can cost thousands of dollars in lost sales if a competitor gets the information. Rumor even has it that foreign governments are hiring spies to steal the laptops belonging to Fortune 500 employees to get the trade secrets stored within.

Favorite locations for thefts include security x-ray machines, phone booths and rest rooms, anywhere the traveler might let go of his or her laptop for a few minutes. Laptop thieves may work in pairs and use distractions to get their targets to relax their guard.

By taking some precautions, you can lessen the chances of having your laptop stolen:

- 1 Never let your computer out of your grasp. This may sound obvious, but many thefts are crimes of opportunity. If you hold on to your computer, a thief will probably look for an easier victim. To avoid losing your computer near the security x-ray machine, ask security personnel to scan your computer with a wand instead. And when using a phone, never place your laptop or briefcase beside or behind you — always place them in front of you, between your feet, if you must put them down at all.
- 2 Carry your laptop in a sturdy, well-labeled case. One that's not obviously a laptop case won't advertise that you're carrying a computer. To increase the odds of retrieving a lost or stolen computer, label the case and computer itself with your name, address and phone number. For personal security, use your business address rather than your home address. If you're in a highly competitive field such as software, or if you work for a well-known company, you might want to omit the company name and simply use its address.



- 3 Install a laptop alarm, an electronic device that will sound if the laptop is separated by more than 40 feet from a transmitter on your keychain.
- 4 Lock your laptop when you leave it in your hotel room. A locking cable, a lightweight six-foot-long cable with a small lock on one end, provides a lot of security for only about \$50. You use the cable to secure the computer to a solid object, then put the lock into your laptop's cable port. If a thief tries to pull the lock out, he'll destroy the computer. Kevin Coffey, a detective with the LAPD and business travel security expert, suggests wrapping the cable around the U-joint in your bathroom sink, since it's solid and difficult to dismantle.

LAPTOP — continued on Page 2

Avoid Evil Twin attacks

Illinois Attorney General Lisa Madigan gives the following suggestions:

- ✓ Disable your laptop's wireless card unless you plan to use it.
- ✓ Ask the provider of a public wireless network for its exact name (its "SSID"). Be cautious of networks with similar names, especially those offering free access when a nearby provider charges a service fee.
- ✓ Do not configure your computer to auto connect to a non-preferred wireless access point.
- ✓ Avoid sending sensitive information over a wireless network.
- ✓ Use a firewall, keep your software and operating system updated and turn off file sharing.
- ✓ Use hotspot providers that provide secure encrypted connections and a list of trusted hotspot locations. If you are not sure whether a wireless connection is secure, assume you are using an "open" hotspot and that your communications can be monitored.
- ✓ If you must use an open hotspot for sensitive communication, make sure the Web site you are using supports SSL or other types of secure connections. A padlock symbol appears in Web browsers when users communicate with a secure Web site.
- ✓ Be aware of your environment. Crowded public hotspots increase your risk of being a victim of a wireless attack. *Source:* Illinois attorney general, www.ag.state.il.us/pressroom/2006_01/20060117.html

Insuring Employees Who Drive Their Own Cars

In many companies, employees who drive during the course of their jobs—whether for making deliveries, calling on clients or picking up supplies—use their personal car rather than company cars. This has several advantages for the employer—it does not have to maintain a fleet, it does not have to worry about non-employees driving the car, and the employee’s personal auto liability policy provides the first layer of coverage. Accounting is also simpler—the employer does not have to account for an employee’s personal vs. business use of the car—all the employer has to do is reimburse employees for their mileage at the IRS rate (currently 44.5 cents per mile for business miles).

However, just because an employee uses a personal auto does not relieve the employer of liability if he or she injures someone while on the job. An employer could become “vicariously liable” for any injuries an employee caused to a third party during the course of work. (Time spent commuting to and from work is NOT considered work time; therefore, an employer has no liability for an accident that occurs during an employee’s commute.)

An employer can do a couple of things to protect itself from liability when employees drive their own vehicles for work:

- A** For all positions that require driving, check applicants’ motor vehicle records (MVR) before making a final job offer. This will show any tickets they’ve received or accidents they have been involved in. Avoid hiring someone with multiple moving violations, especially for speeding or failing to obey signals. Studies have shown that these habitually careless drivers are more likely to become involved in accidents.
- B** Require employees who drive for work to carry a personal auto policy with at least \$500,000 in liability coverage. This will serve as your first layer of liability coverage, so be sure to notify employees that if they’re involved in a work-related accident, their policy will respond first. Require employees to submit proof of insurance, and make continuing coverage a condition of the job.
- C** Consider buying a business auto policy to cover auto-related liability exposures. The BAP can be written to cover any of an insured’s auto-related liability exposures, indicated by “symbols” on the policy’s schedule of coverages. To see whether your policy covers employee-owned vehicles, check for either Symbol 1 (which covers “any auto”) or Symbol 9 (non-owned autos only) in the schedule of coverages.

The BAP covers only the liability of the named insured — that is, the employer. The business auto policy (and your other liability policies) will not cover the employee’s own liability.

The BAP and other commercial liability policies also will not cover any injuries an employee causes to a fellow employee. Workers’ compensation protects the employer from this type of claim.

In some states, employees can sue their co-workers for work-related injuries under certain circumstances. The employer’s workers’ compensation insurance will not provide coverage for this kind of claim, making the employee personally liable.



Time spent commuting to and from work is NOT considered work time; therefore, an employer has no liability for an accident that occurs during an employee’s commute.

If you want to provide employees with liability protection for suits by fellow employees and other situations, you can buy this additional coverage in an “employees as insureds” endorsement. The endorsement will provide employees with coverage under your BAP, secondary to the employee’s personal auto policy. Please note that if you have Symbol 9 coverage only (non-owned autos only), the BAP provides liability coverage only; it will not cover property damage to the employee’s car.

For more information on managing your firm’s auto-related risk exposures, please call us. □

LAPTOP — continued from Page 1

- 5** Install monitoring software. Several vendors offer security applications that can “report” to a server whenever they connect to the Internet. If you report your computer lost or stolen, the vendor can track the laptop’s exact physical location the next time it connects to the Internet.
- 6** Be careful in wireless hot spots. Free Internet hot spots offer travelers a great convenience. But unwary hotspot users can unknowingly connect to a nearby hacker’s computer (an “Evil Twin”) instead of the wireless network. The “Evil Twin” computer mimics the characteristics of a legitimate wireless network to gain access to others’ passwords, data and personal information.

Insuring Laptops

The standard commercial property policy and its extensions provide only limited coverage for laptops and their data. Specialized laptop computer policies may provide better coverage. These policies vary greatly from company to company; we can help you evaluate which one best meets your company’s needs. For more information, please call us. □

What does losing a laptop cost?

Hardware:	\$1,500-\$2,500
Software:	\$1,000+
Time lost to reinstalling/configuring software and recreating data:	4+ hours
Loss of sales if competitor gets your data:	priceless!

The Kensington Notebook Security Survey found that, as of 2001, medium and large companies lose more than 11 laptop computers every year through theft. Each laptop theft costs an average of \$89,000—mostly due to lost data, according to Computer Security Institute/FBI Computer Crime & Security Survey of 2002.