IN BRIEF

THIS ISSUE
October 2004
Issue No. 93

PROFESSIONAL LIABILITY FUND
www.osbplf.org

MALPRACTICE AVOIDANCE NEWSLETTER FOR OREGON LAWYERS

LAPTOP COMPUTERS: PROTECTING CONFIDENTIAL CLIENT INFORMATION

Laptop computers present special data security risks because they are designed for mobility and are frequently used outside the office. Some of the risks associated with laptop usage are:

- **Loss and Theft.** Laptops are vulnerable to both human error (loss) and to greed (theft). The portable nature of laptops makes them easy to leave in a hotel room, airport, or restaurant. They are also easily stolen and sold on the black market. National crime statistics report that roughly 150,000 laptops were stolen in 1994, 200,000 in 1995, and 275,000 in 1996. Theft is growing faster than the number of laptop computers in use. Theft from an office is the most common, and airport theft the second most common.

- **Unauthorized Access.** Laptop computers are frequently used in insecure locations – conference rooms, temporary offices, and airports, to name a few. In most cases, the laptop is used in a conference room or other public area where the laptop user is not well known to others in the area. This situation makes it easy for an unauthorized user to view or use the laptop without looking suspicious. Be especially careful if you are using a high-quality large screen, as this allows a much wider viewing angle.

- **Unauthorized Use of Data.** Unauthorized use of data usually results from: (a) loss or theft of the laptop; (b) unauthorized access to the laptop for long enough to view or copy data; (c) loss or theft of data copied to diskettes or other portable storage devices (e.g., memory sticks, USB drives) for printing, backup, or data transfer; or (d) interception or compromise of data transmitted over telephone lines or the Internet.

These security risks cannot be eliminated, but a combination of technology tools and user awareness can reduce laptop data security risks to a reasonable level.

PHYSICAL SECURITY

The risks of theft, unauthorized access, or unauthorized use of data can be significantly reduced by diligently observing the following physical security practices:

- Use a sturdy bag that doesn't look like a laptop bag to carry your laptop;
- Hang the bag from your shoulder or keep it on the floor between your feet;
- Use locking cables or burglar alarms;
- Never leave the laptop unattended or out of your sight in a public place;
- Don't check the laptop as luggage or in a coatroom;
- Don't store the laptop in airports, airplanes, trains, or subways;
- Keep the laptop with you when in taxis, cars, or other transportation;

- Watch the laptop as it goes through airport metal detectors ("snatch and grab" thefts are common); and
- Use locking or even unlocked drawers or cabinets to store laptop computers when you leave an office, conference room, or hotel room.

ACCESS SECURITY

The second line of defense against laptop theft or unauthorized use of data is access security. If a laptop computer is lost, stolen, or otherwise outside the control of its owner, data remains secure if an unauthorized person is prevented from turning the computer on and using it.

The simplest way to reduce access to your computer data is to log off of the computer when you are not able to stay near it, and to take the computer with you. Since this option is not always practical, you can also protect the data by using the lock computer function of the computer. Simply hit Ctrl-Alt-Delete while your computer is on, then select Lock Computer. Your laptop is now locked until an authorized user logs on.

Password security options include using password protection on screen savers (so a password is needed once the screensaver appears), using a password that guards against being easily guessed (often referred to as a "strong" password), changing passwords regularly, and following the other security suggestions that are available from the maker of your operating system. If you use Microsoft Windows, you can find a list of security tips by searching the Help menu.

DATA SECURITY

Access security alone is not sufficient protection for laptop computers. Power-on and screen-lock passwords can be eluded by removing a laptop's hard drive and reinstalling the hard drive in another laptop, and neither system protects data being transmitted by CD, memory sticks, portable hard drives, or e-mail. Using security software and hardware security devices provides additional data security. An example of security software that includes e-mail encryption is Steganos Security Suite, reviewed in the September 2003 issue of *PC World*. Examples of hardware security devices are DEFCON Authenticator (reviewed by David Hiersekorn for the June/July 2003 issue of *Law Office Computing*) and MemoPass. These devices create and store personal profiles for the authorized user through a USB port or by access card.

Creating a mobile system can backfire if the system is not secure. This is a very important consideration when using a wireless connection. Wireless laptops and computers have wireless adapters and wireless access ports that enable them to connect to your computer network. Unfortunately, these wireless access ports transmit radio signals continuously. Since only about one percent of wireless users change the vendor's default user name and configurations, 99 percent of these wireless access points are highly insecure. So if you are using a wireless network, don't rely on the default settings of your laptop to protect you. Check with your wireless vendor or consult with an expert about how to properly secure your wireless system.

Last, but not least, laptop users can secure data by being selective about what they store on the laptop. If possible, avoid storing personal information (such as birth dates and social security numbers) on a laptop. When working away from the office, use resources that the computer can link to via the Internet as the sources of confidential data. Intranets, extranets, and Web sites protected by private passwords are examples of such sources not located on a laptop's hard drive. If the laptop is lost or stolen, the client data will not be compromised. This is particularly true if you don't store the passwords to such resources on the laptop itself, or if the passwords are well encrypted to prevent unauthorized access.

Our thanks to Beverly Michaelis, PLF Practice Management Advisor; Dee Crocker, PLF Practice Management Advisor; and Steel Scharbach of Steel Scharbach Associates, LLC, for their assistance with this article. The original article, "Notebook Security: Protecting Confidential Client Information," October 1997, can be found at www.ssa-lawtech.com. Click on white papers, then on security issues.