Courtesy of
Huckaby & Associates

CYBERRISKS&LIABILITIES_

Preventing Laptop Theft

Laptop computers are integral devices in the workforce today. As more and more companies issue laptops to employees, the chances of losing a laptop (and the data stored on it) to theft are much greater. Follow these guidelines to help keep your laptops safe.

Communicate Employee Responsibility

If your company issues laptops to employees, be sure to communicate that your employees have a responsibility to care for them.

Employees' work laptops may have their personal information on them (stored website sign-in information, name, address, work documents, etc.)—and they may not realize it. Making employees aware that the theft of a work laptop could personally affect them can be an incentive for them to protect the computer.

It may be beneficial for you to provide a security cable lock when you issue laptops to employees. A cable lock works similarly to a bike lock—one end of the cable has a lock that goes into the laptop's security slot and the other end is attached to a heavy stationary object, such as a desk. This type of lock works as a visual deterrent as well, making the laptop less appealing to a thief.

Give your employees frequent laptop safety reminders and updates on new scams or theft tactics. Laptop safety is not a one-time thing—making security a habit will keep your company's property and information safe.

Laptops That Don't Leave the Office Are at Risk, Too

A laptop that never leaves the office should not be considered safe from theft. If the laptop is not locked to a docking station or desk, it is vulnerable.

An employee who is planning to quit or who is feeling disgruntled may see stealing a laptop as an easy score. One way to protect your company laptops is to apply tamperproof metal labels with your company name and contact information to each laptop. There are many types of tamperproof labels available, such as labels that etch a permanent message or break into tiny pieces when removed. The labels can also be used to track inventory and software updates.

Deterring theft can also be achieved by engraving the company name on laptops. This will discourage employees from stealing them, because the permanent engraving decreases the resale value.

Use Encryption Software

The physical loss of a laptop may not be as devastating as the loss of the information and data stored on that laptop.

Encryption software uses mathematical algorithms and an encryption key to encode data so that only someone who has the encryption key can read it. There are three different encryption methods you can use, based on the sensitivity of your data. Make sure you choose the right level of protection for your company.

- **Full disk** encrypts an entire disk, including all its data. This method is used to encrypt laptops, desktops and mobile devices.
- **Individual file** encrypts a single file or creates an encrypted repository for file storage.
- **Data transit** encrypts during a transfer, but does not guarantee encryption once the data reaches its destination.

To protect the interests of your company and employees, all devices should be encrypted and require passwords for access.

Install Tracking Software

Tracking software is often called "anti-theft" software—it tracks your laptop to its current location using IP address

This Cyber Risks & Liabilities document is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice.

locations, GPS or Wi-Fi positioning. A stolen laptop can be easier to recover if you’ve installed tracking software before the theft.

Some software can take a photo of the thief if the thief turns on the computer, showing his or her identity. If the thief sells the laptop to someone, capturing the new user’s identity is helpful for finding the thief.

Tracking software can also take screenshots of what the thief is doing on your computer, which is helpful if the thief signs in to his or her own personal accounts. Some software can lock the thief out to prevent him or her from logging on to your computer at all, and some software can remotely delete sensitive data from the hard drive if you tell it to.

Keep in mind that tracking software alone does not prevent theft—your employees’ actions and habits play a major role, too. Contact Huckaby & Associates today to learn more about defending your company’s laptops against theft.