

Risk Monitor



Inside...

PAGE 1...

Don't Forget Insurance for Your Organization's Cyber Risks

PAGE 2...

Laptop Lockdown: Safeguard Your ompany's Laptops

PAGE 3...

Protecting Your Business from Natural Disasters with a Disaster Recovery Plan



Don't Forget Insurance for Your Organization's Cyber Risks

The federal Internet Crime Complaint Center received over 330,000 complaints in 2009, and more than a third of them ended up in the hands of law enforcement. The damages from those referred to the authorities totaled more than a half billion dollars. The Government Accountability Office estimated that cyber crime cost U.S. organizations \$67.2 billion in 2005; that number has likely increased since then. With so much of business today done electronically, organizations of all types are highly vulnerable to theft and corruption of their data. It is important for them to identify their loss exposures, possible loss scenarios, and prepare for them. Some of the questions they should ask include:

What types of property are vulnerable? The organization should consider property it owns, leases, or property of others it has in its custody. Some examples:

- Money, both the organization's own funds and those it holds as a fiduciary for someone else
- Customer or member lists containing personally identifiable information, account numbers, cell phone numbers, and other non-public information
- Personnel records
- Medical insurance records
- Bank account information
- Confidential memos and spreadsheets

- E-mail
- Software stored on web servers

Different types of property will be susceptible to various threats, such as embezzlement, extortion, viruses, and theft.



What loss scenarios could occur? The organization needs to prepare for events such as:

- A fire destroys large portions of the computer network, including the servers. Operations cease until the servers can be replaced and reloaded with data.
- A computer virus infects a workstation. The user of that computer unknowingly spreads it

continued on page 4

Welcome to The Chadler Group's Newsletter!

It is with great satisfaction that we bring our newsletter to you. In this issue and the coming quarterly newsletters, we will continue to discuss pertinent insurance topics which affect your business and personal insurance needs. This newsletter will deal with **Privacy and Disaster Preparedness**. We hope you find this information both informative and useful in your overall risk management practices.

The Chadler Group, Inc.
PO Box 11115
330 Passaic Ave, Ste. 200
Fairfield, NJ 07004



Phone: (973) 227-0025
Fax: (973) 227-4026



Laptop Lockdown: Safeguard Your Company's Laptops

According to the FBI, there were 221,009 laptops reported stolen from 2008 through 2009. As an increasing number of business men and women are traveling with laptops in tow each year, this already high number is likely to keep rising. Statistics show that the most popular targets for laptop thieves are office buildings, airports, hotel rooms and cars.

While some laptop snatchers are simply looking to make a quick buck by selling your computer, others are much more malicious. These higher-level laptop thieves are more interested in the valuable information stored within your computer—from business plans and customer contact information to Social Security numbers and passwords. Once they get a hold of your laptop, these cyber criminals may be able to gain access to your company's server. One FBI study found that 57 percent of computer crimes were linked to stolen laptops. Plus, research suggests that the theft of just one laptop can cost a company up to \$90,000 or more!

Unfortunately, many laptop owners forget just how much their computer and personal information is worth—and how much they stand to lose if their computer is stolen. That's precisely why experts say you should guard your laptop as closely as you would your wallet.

Here are a few steps you can take to protect your laptop from these spiteful computer crooks:

Travel incognito

Whether you're traveling by plane, train or automobile, be sure to carry your laptop in a protective, inconspicuous case. With thousands of laptop case styles available, you may be able to find one that looks more like a backpack, handbag or briefcase—which decreases your risk of being targeted by a laptop thief.

Use protective software

Take advantage of password protection programs, anti-virus software, encryption software and other robust programs that will protect the information stored on your laptop.

Keep unused laptops out-of-sight

If your company has extra, unassigned laptops, keep them locked safely away in fully enclosed, secure closets. Never leave them in a cubicle or unlocked cabinet.

Lock it up

Never leave your laptop out in your office, even if you're just leaving for a few minutes. Either lock it into your docking station

or lock it away in a secure desk drawer. Don't ever leave your laptop in plain view next to an office, house or car window.

Guard it in the airport

When traveling through an airport, be sure to keep your laptop within reach and in sight all the time. Never check a laptop with your baggage, and be extremely careful when you're passing through security checkpoints. Hold onto your laptop as you wait in the security line, and do not set it on the belt until you're getting ready to pass through the X-ray machine.



Protect it in the car

If you have to leave your laptop in the car, lock it up in the trunk where it's out of view. If you drive a truck or SUV with a window looking into the trunk, lock it in your glove box or conceal it under a seat. You should also keep your laptop in a weatherproof case. Avoid storing your laptop in the car in extremely hot or cold temperatures.

Keep track of it

Make sure your name or company's name and ID is engraved on your laptop. Also, be sure to write down your laptop's identification number and store it in a safe place. Ask the laptop manufacturer or your local police department if they offer an asset identification or registry program.

Protecting Your Business from Natural Disasters with a Disaster Recovery Plan



Of the U.S. companies that are victim to a man-made or natural disaster, the Contingency Planning Research Strategic Corporation says 43% never reopen their doors and 29% are out of business within the following two years. A study by Touche Ross found that companies without a disaster recovery plan only have a 10% or less survival rate. Business owners should be seriously asking themselves whether or not they have an adequate recovery plan for disasters.

There are three crucial areas that all disaster recovery plans should cover:

1. Physical Resources

Of course, the physical assets of a business, such as equipment, electronics, office furniture, and the building itself, are things that usually can't be quickly or easily replaced if they're damaged during a disaster. The following are questions that an adequate disaster recovery plan should answer:

- Are there at least three days worth of emergency supplies on hand to carry the business immediately following the disaster?
- What steps can you, should you, and will you take to protect physical assets?
- How would physical assets hold up against various disasters—flood, hurricane, tornado, fire, earthquake?
- Who will assess the damage to physical assets following a disaster?
- Has a list been made to prioritize the replacement of key physical assets and what suppliers or companies should be contacted for the replacement?
- Is access available from an off-site backup system if data and electronics are damaged and how often should backups take place?
- How will important documents and records be kept secure and protected?
- Is an alternative facility an option to resume operations if the primary location is unusable and what location and type of facility would be needed?

2. Human Resources

All employers know that their employees are one of their business's most vital assets. Therefore, employee safety and the resulting personnel issues that follow a disaster should be a top priority. The following are questions that an adequate disaster recovery plan should answer:

- Have all staff been adequately instructed on the disaster recovery plan?
- How will staff find safe shelter?
- How will contact be maintained with staff during and after the disaster?

- Are current contact numbers for all staff, vendors, suppliers, and clients available at an off-site location and how will this list be maintained and updated to stay current?
- Have staff members been identified to assume mandatory or key roles should other employees not be able to resume their roles?
- Are staff members assigned to form a crisis management team?

3. Operation Continuity

This component is about getting the business back up and running after the disaster. The following are questions that an adequate disaster recovery plan should answer:

- Does insurance, in particular business interruption insurance, provide adequate coverage?
- What amount of cash will be available for emergency contingency expenses?
- If the facility isn't usable, then where should an alternative command center be located to coordinate the recovery?
- Is there an alternative list of suppliers to use in the event regular suppliers aren't operational?
- What should be done for clients and customers during and after a disaster?



Employers might further assign specialized teams to be in charge of some of the tasks related to the above points. For example, a post disaster recovery team could manage recovery tasks like getting the business up and running quickly; an administration team could handle areas like logistics, transportation, and emergency and survival gear; a public relations team could make public announcements and field inquiries; a client/supplier communications team could advise vendors and clients of the business's status; and an IT team could be responsible for software and hardware issues.

Remember, disasters can strike with little, if any, warning. Business owners can keep themselves off the wrong side of the statistics by being prepared and being able to get themselves up and running as soon as possible.

continued from page 1...

Don't Forget Insurance for Your Organization's Cyber Risks

to everyone in his workgroup, crippling the department during one of the year's peak periods.

- The accounting department discovers a pattern of irregular small funds transfers to an account no one has ever heard of. The transfers, which have been occurring for almost three months, were small enough to avoid attracting attention. They total more than \$10,000.
- A vendor's employee strikes up a casual conversation at a worker's cubicle and stays long enough to memorize the worker's computer password, written on a post-it note stuck to her monitor. Two weeks later, technology staff discover that an offsite computer has accessed the human resources database and viewed Social Security numbers, driver's license numbers, and other personal information.

In addition to taking steps to prevent these things from happening, the organization should consider buying a cyber insurance policy. Several insurance companies now offer this coverage; while no standard policy exists yet, the policies share some common features. They usually cover property or data damage or destruction, data protection and recovery, loss of income when a business must suspend operations due to

data loss, extra expenses necessary to maintain operations following a data event, data theft, and extortion. However, each company may define these coverages differently, so reviewing the terms and conditions of a particular policy is crucial. Choosing an appropriate amount of insurance is difficult because there is no easy way to measure the exposure in advance. Consultation with the organization's technology department, insurance agent and insurance company may be helpful. Finally, all policies will carry a deductible; the organization should select a deductible level that it can afford to pay and that will provide it with a meaningful discount on the premium. Once management has a thorough understanding of the coverages various policies provide in relation to the organization's exposures, it can fairly compare the costs of the policies and make an informed choice.

Computer networks are a necessary part of any organization's environment today. Loss prevention and reduction techniques, coupled with sound insurance protection at a reasonable cost, will enable an organization to get through a cyber loss event.



The Chadler Group, Inc.
PO Box 11115
330 Passaic Ave, Ste. 200
Fairfield, NJ 07004

Phone: (800) 706-2478
Fax: (973) 227-4026

Risk Monitor