Managing Risk

ZINN
Clear direction from a trusted source
www.zinn.com

Myerstown Office:
16 East Main Avenue
Myerstown, PA 17067
717-866-5717

Lebanon Office:
761 Poplar Street
Lebanon, PA 17042
717-272-6693

Property & Liability | Spring 2012 | Volume 21 • Number 2

Data Loss: Are You Covered?

Data. You store it on company computers and networks. Employees can access it at home or on the road. You might even have data "in the cloud," in facilities you don't own or control. And it's the lifeblood of your organization. How well is it protected?

As with most things, insurance should be your second priority — your first priority should be to take measures to protect your data from damage, loss or theft. When reviewing your organization's data protection program, involve your IT team and data end users to identify your company's specific risk exposures.

The questions you'll want to consider include: Where is data stored? Who has access? Who can make changes? How is it protected? Protections include both physical and intangible protections, such as software and procedures. When evaluating physical protections for your data, look at the setup of your data center. Can anyone access your servers, or is access limited to IT staff? Does your data center have appropriate fire protection/sprinkler devices?

Intangible protections include your procedures as well as software and systems. Organizations can control access to sensitive data through:

continued on next page

Risk Tip

How do labor laws affect your organization's social media policies? A U.S. Chamber of Commerce report examined cases involving social media brought before the National Labor Relation Board. Most of the cases reviewed involved complaints over employer policies that took an overly restrictive approach to allowing employee social media access/use or employer disciplinary actions "based on an employee's comments posted through social media channels."

To provide guidance to legal practitioners and human resource professionals, a report released in January 2012 by the National Labor Relation Board's (NLRB) Acting General Counsel Lafe Solomon underscores two main points:

- **Employer policies should not be so sweeping that they prohibit the kinds of activity protected by federal labor law, such as the discussion of**

continued on next page

- Requiring user permissions and separation of duties. Be sure to document each user's access to applications and files.
- Encrypting proprietary or personal data.
- Restricting access to data from outside the company's computer network.

The advent of "cloud computing" can also create questions of control and ownership. Are you sure your data is really yours? Check your contract with any cloud computing vendors to ensure you retain ownership rights to your data and that the vendor will not mine it or use it for its own purposes.

Your contract should also specify how the data will be returned to you if you end the relationship. The contract should spell out how long the vendor has to return data, and should also specify that it must provide data in a format you will be able to use, rather than holding you hostage by returning it in a proprietary format.

Insuring Your Data

The next step is to analyze your current insurance program to understand which risks are covered and which may need additional protection. Coverage for networks and data is sometimes called cyber insurance. It covers your own data and the data of customers, partners and clients that you interact with: in insurance terms, first-party and third-party coverages.

Most commercial property policies have coverage limits for computer hardware and exclude coverage for software and data. Many insurance companies offer optional endorsements that increase hardware limits and add coverage — usually with small sub-limits for:

1. Loss of software, programming and data caused by viruses.
2. Loss of income and extra expenses due to damaged hardware or software caused by viruses.
3. Loss of income due to viral attacks that overload computers and prevent normal business traffic.
4. Electronic fraud — reimbursement for money stolen through the computer.

wages or working conditions among employees.

- **An employee's comments on social media are generally not protected if they are mere gripes not made in relation to group activity among employees.**

For more information on devising a social media policy that will help keep your firm out of trouble, please see the article on P. 4.

If your first lines of defense are adequate, this coverage might be enough for you. If not, we can discuss specialized data coverages.

Third-Party Data

Many organizations today use, store or access data that belongs to third parties. Whether it's your customers' credit card information, a business partner's mailing list or any other data, you have a responsibility to protect it from theft, loss or breach while it's in your care.

The standard general liability (GL) policy excludes coverage for property damage to electronic data. You can buy an endorsement that adds a separate sublimit of coverage for loss of electronic data resulting from damage to tangible property. Your errors and omissions policy will probably not cover electronic data loss either, unless it includes specific cyber liability language.

Cyber liability is a big issue in the insurance industry. As the Internet, cloud computing and social media become more important to the way we do business, organizations need to review their liability coverage. The standard commercial general liability policy covers you for libel, slander and copyright infringement arising from your advertising. However, it typically excludes those coverages for companies in the publishing, broadcasting or media industries. Any company that has a website or uses social media could be considered a publisher. Does that mean you need a media liability policy, to protect you from claims of libel, copyright infringement and plagiarism? Many cyber liability policies cover this exposure and more.

Cyber liability coverage can be bought as a freestanding policy or as part of a professional liability policy. Policies vary by insurer, but may contain:

continued on next page

- Privacy liability: Covers losses from failing to protect personal information (i.e., Social Security numbers) and corporate information, as well as costs to repair identity theft and to respond to regulatory agencies.
- Network security liability: Covers losses due to a failure in network security such as unauthorized access, virus transmission or destruction of software and data. May also cover business interruption for third parties impacted by the network security failure.
- Internet media liability: Covers the company's Web content for infringement, defamation, plagiarism or negligence. May also include coverage for transmission of viruses to your Web visitors.

To learn more, please give us a call.

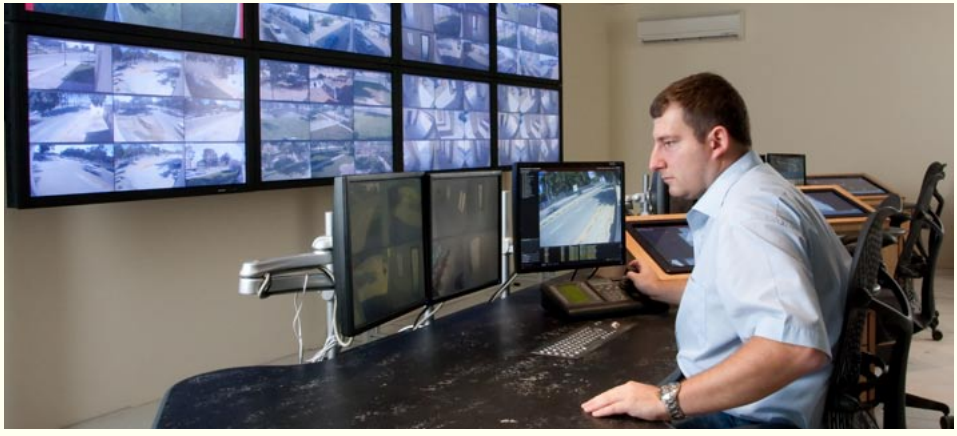
Protect Your Firm from Employee Theft

"2011 was another banner year for employee theft in the United States, continuing the frenetic pace set in 2010." So begins The 2011 Marquet Report on Embezzlement, an annual study of white collar fraud in the U.S.

The study also found that the average embezzlement scheme lasted nearly five years, cost an average of about $750,000 and a median of $340,000 and usually involved employees in finance, bookkeeping or accounting positions. Unfortunately, unless the victim organizations had separate commercial crime coverage, they were uninsured for these losses.

The typical commercial property policy covers you for theft committed by outsiders, but specifically excludes employee theft. You can buy commercial crime coverage, a type of fidelity bond, to protect your organization from employee theft.

Fidelity bonds indemnify employers for the loss of money or other property sustained through the dishonest acts of bonded individuals. Often called "honesty insurance," bonds provide coverage for intentional acts of fraud, larceny, misappropriation, forgery, embezzlement and other dishonest acts committed by a bonded employee. The acts must also be intended to cause a loss to the employer and financially benefit the bonded



continued on next page

person. The bonds are technically a form of surety, but are similar to an insurance policy in format and terminology.

Types of Crime Coverage

There are four major crime coverage forms available:

- ✔ Form A, employee dishonesty
- ✔ Form B, forgery or alteration of documents
- ✔ Form C, theft, disappearance and destruction, and
- ✔ Form D, robbery and safe burglary.

Most businesses buying crime coverage will need one or more of these forms. Forms to cover more specialized exposures, such as items in hotel/innkeepers' safe deposit boxes, also exist. The Insurance Services Office has combined these forms into crime packages for specific types of businesses. You can buy them as separate crime policies or attach them to your commercial package policy. Whatever you need coverage for, whether it's money and securities, the contents of safes and more, the property of guests and lodgers, there's probably a program that meets your needs.

Most crime programs exclude coverage for crime or dishonest acts committed by the insured or any partner, seizure or destruction of property by order of governmental authority, indirect or consequential loss, and legal expenses. Most plans cover only workers employed in the U.S., its territories and Canada.

What About Data Theft?

To be sure your crime coverage will protect you for data theft, read your policy carefully. A broadly drafted policy might provide coverage for electronic data, including data stolen by employees. Some insurance forms also extend coverage to certain computer contractors. We can help you review your operations and coverage to help you minimize exposures to employee theft. Please contact us for more information. ■

How to Keep Your Workplace Drug-Free… without Lawsuits

"My workplace doesn't have a drug problem," you might think. But among adults aged 18 or older, 8.4 percent of those employed full-time currently use illicit drugs, while 11.2 percent of those employed part-time do so. Legal drugs also have the potential for misuse: The National Institute on Drug Abuse estimates that about 7 million people currently use prescription and over-the-counter drugs "taken non-medically," or in a way other than as prescribed, without a prescription, or for the experience or feeling it causes.

The federal government does not require most private companies or individuals to have drug-free workplace policies. The exceptions: federal contractors, which must comply with the Drug-Free Workplace Act of 1988 and/or the U.S. Department of Defense's Rules and Regulations for Defense Contractors, and employers in "safety-sensitive industries," specified under the Omnibus Transportation Employee Testing Act of 1991.

However, drug-free workplace programs can protect employers from the negative effects of substance abuse. Studies show that when compared with non-abusers, substance-abusing employees are more likely to:

continued on next page

- change jobs frequently
- be late to or absent from work
- be less productive than other employees
- be involved in a workplace accident
- file a workers' compensation claim.

Research also indicates that between 10 and 20 percent of the nation's workers who die on the job test positive for alcohol or other drugs.

Some states offer employers with drug-free workplace programs a discount on workers' compensation premiums. And many states deny workers' compensation benefits to workers whose injuries are determined to be the result of substance abuse. Finally, almost 30 states have laws and rules that limit or deny unemployment benefits to individuals fired because of a positive drug test.

Should Your Program Include Drug Testing?

Employers can test for drugs at different points in the employment process — during the application process, during employment at random or regular intervals, or after an accident. It can be done for some or all workers — for example, for safety-sensitive positions only, or for all workers. Because drug testing costs money, you may choose not to use this method for assessment. However, many workers' compensation experts recommend testing all employees after an accident or near-miss to rule out the use of drugs.

If you decide to implement a drug-testing program, remember that laws designed to protect workers' civil rights could affect your workplace drug policies. These laws include the Civil Rights Act of 1964 and the Americans with Disabilities Act (ADA) of 1990. These statutes limit how far an employer can go in investigating and disciplining employee drug use. Under the ADA, for example, employers cannot fire a drug addict who is already seeking treatment for his/her condition.

Many states and U.S. territories have their own laws and regulations dictating when and how workplace drug testing should be carried out. Some also require state and local contractors to develop drug-free workplace policies similar to those under the federal Drug-Free Workplace Act. No one set of rules and regulations applies throughout the country. Some states, such as Louisiana, allow drug testing in virtually every type of business and in both the public and private sectors. Others, such as Maine, restrict who can be tested, how they can be tested, and what kinds of rehabilitation and disciplinary options can result from a positive test.

Employers can take several simple steps to avoid legal problems with their drug-free workplace policy:

- ✔ Consult an employment lawyer whenever you introduce a new drug-free workplace policy or change an existing policy.
- ✔ Make sure your drug-free workplace policy clearly stipulates penalties for violations. If your policy includes drug testing, spell out exactly who will be tested, when they will be tested, and what will happen to employees who test positive.
- ✔ Make sure every employee receives and signs a written copy of your drug-free workplace policy. Verbal agreements and unsigned agreements have little legal standing.
- ✔ Make sure that you, and all your supervisors, receive proper training in how to detect and respond to workplace drug and alcohol abuse.
- ✔ Maintain detailed and objective records documenting the performance problems of all your employees. Such records often provide a basis for referring workers to employee assistance programs.
- ✔ Never take disciplinary action against a worker or accuse a worker of a policy violation simply because that employee is acting impaired. Instead, try to clarify the reasons for the employee's impairment. If drug testing is a part of your workplace policy, obtain a positive test result before taking any action.
- ✔ Never accuse or confront an employee in front of coworkers. Instead, try to stage all discussions someplace private, with another manager present to serve as a witness.
- ✔ Never single out an individual employee or particular group of employees for special treatment — whether it is rehabilitation or punishment. Inconsistencies in policy enforcement may lead to discrimination charges.

continued on next page

- ✔ Try to get to know your employees as much as possible. This may help you more quickly identify workers who are in trouble or developing substance abuse problems.
- ✔ Most important, try to involve workers at all levels of your organization in developing and implementing your drug-free workplace policy. This will reduce misunderstandings about the reasons for a drug-free workplace program and help ensure that policies and procedures are fair to everyone.

The U.S. Department of Labor's (DOL) Working Partners for an Alcohol- and Drug-Free Workplace Web site provides employers with free resources and tools to help establish and maintain drug-free workplace policies. And we recommend having a local employment attorney review your policy before implementation. ■

Guidelines for Company Social Media Use

Share with communicators, managers and employees!

- ✹ The Internet is not anonymous, nor does it forget. Everything posted on the web can be traced back to its author.
- ✹ No clear line between your work life and your personal life exists. Always be honest and respectful in both capacities.
- ✹ Avoid posting or linking to any materials that are defamatory, harassing or indecent.
- ✹ Do not promote personal projects, or endorse other brands, causes or opinions.
- ✹ Respect third-party copyrights.
- ✹ If you must post a personal opinion, clearly state this does not represent the opinions of the business.
- ✹ Do not post confidential or proprietary information related to the business or its clients. Always adhere to your clients' policies and procedures for confidentiality and social media.
- ✹ Do not pad your own statistics. Do not create anonymous or pseudonym online profiles to pad link or page view statistics. Do not comment on your own or others' posts to create a false sense of support.
- ✹ Always trackback. When reposting or referencing a post on one of your business' online sites, provide a link to the original post or story.
- ✹ Identify yourself. When relevant, identify your affiliation with the business and your area of concentration.
- ✹ Do not pat yourself on the back. Do not post self-laudatory statements regarding your work or that of the business.
- ✹ Do not post statements regarding the quality of your work or of the business.
- ✹ Do not promote successes. Don't report business results or outcomes or use words like "successfully," "favorably," "won" or "prevailed" in describing your business representations.
- ✹ Do not return fire. If you find a negative post or comment about your business or yourself, do not counter with another negative post. Instead, publicly offer to remedy the situation through positive action.
- ✹ Do not offer or appear to offer legal advice, professional expertise or to form client relationships using social media. Formation of these relationships must be done only through your business' regular procedures to avoid conflicts and other ethical problems. ■

Source: FDIC's Office of Minority and Women Inclusion (OMWI). (Edited for space.)

Managing Risk