Insurance Buyers' News

Barker Phillips Jackson
Insurance and Other Financial Services
www.bpj.com

Springfield
PO Box 4207, Springfield, MO 65808
Phone: 800-422-5275
417-887-3550 • Fax: 417-887-3252

St Robert
690 Missouri Ave, Suite 7
St Robert, MO 65583-4684
573-336-5016 • Fax: 573-336-3496

Rolla
PO Box 1258, Rolla, MO 65402-1258
Phone: 800-364-2212
573-364-8888 • Fax: 573-341-2257

West Plains
PO Box 964, West Plains, MO 65775
Phone: 800-400-3896
417-256-6162 • Fax: 417-256-6165

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

This Just In

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 Relations 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**

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 sublimits 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.

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

This Just In

the kinds of activity protected by federal labor law, such as the discussion of 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.

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

continued on next page

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:

- 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 you 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 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

continued on next page

- ✔ 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 packaged 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 Build Your Social Media Policy

Today, more than half of companies surveyed use social media in their marketing, and more than half plan to increase their involvement in social media this year. However, only 40 percent have a formal social media policy, reported the Society for Human Resource Management (SHRM). Social media involvement, if not handled properly, can expose your organization to charges of libel, harassment, trademark infringement, labor law violations and more.

A well-crafted social media policy can help protect your organization from these exposures by outlining whether social media posts must be cleared and by whom, what other employees can and cannot say, and consequences for violations. It should also spell out your organization's policies toward accessing social media during work hours, whether your organization monitors online activity and what employees can expect in terms of online privacy, if anything. In fact, your "social media policy" might not be one policy, but many, and incorporated into several existing policies and documents.

The following suggestions provide a starting point for crafting your own social media policy. Every company differs, however, and if you have extensive online activities, an IPO in the near future or pending litigation or complaints, you will probably want to have your policies reviewed by an attorney.

continued on next page

1. Protect company networks and data. Develop policies and procedures to restrict how your employees access the Internet in the office, while doing work at home, or while logged in to your business' network (i.e., accessing/downloading confidential information or accessing social networks such as LinkedIn, Facebook or YouTube). Work with IT staff to ensure technological protections are in place. These include firewalls, passwords, virus protections, etc.
2. Provide training for employees to understand what information and data is confidential, such as intellectual property, material non-public information, personnel information and financial records. Employees should also know the basics about copyright/trademark protections, and what they can and cannot post as "fair use."
3. Create policies outlining appropriate/inappropriate language, harassment and respecting colleagues and competitors in social media posts. (Your company's email policy should already contain similar requirements.)
4. Create policies outlining appropriate and inappropriate communications about your business in public and semi-private forums. If your company is publicly traded, remember that fair disclosure rules apply to social media posts as well. Some social media (such as Twitter) don't allow room for disclosures. Overly optimistic postings might constitute "forward-looking" communications. And using social media to disclose "material nonpublic information" to individuals who might trade on that information might not constitute "full and fair disclosure" under SEC rules.
5. Consider restricting "official" business communications to the public through social media to specific individuals with media training. Publicly traded companies will probably want to have an experienced investor relations professional handle social media communications to avoid potential problems.
6. Establish policies that govern whether your employees may discuss or endorse your business in public and rules about how to do so ethically. Employees should identify themselves as employees if discussing the business in a public forum. If they must post a personal opinion on a business matter, they should clearly state that it is a personal opinion and they are not speaking as a representative of the business.
7. Develop policies on monitoring social media activity. Ideally, you will have trained media professionals on staff or on retainer to monitor social media for mentions of your organization.
8. Inform employees of your communications privacy policy. If you reserve the right to monitor employees' online and social media activity during company time or when using company equipment or networks (as you probably should), notify your employees in writing that they cannot expect their activities to be private.
9. Train executives and managers responsible for policy enforcement to understand the laws that protect employee communications. This includes the National Labor Relations Act (NLRA), which protects workers' rights to discuss wages, working conditions or union organizing with co-workers or a union, and other labor activities.
10. Put your policy in writing and include it in your employee handbook. Have employees acknowledge, in writing, their receipt of the policy and their agreement to adhere to it.

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.)

Insurance Buyers' News