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

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

Liability Risks for Nonprofits

November is Nonprofit Awareness Month. If you manage or serve on the board of one of the estimated 1.58 million nonprofit organizations in the U.S., thank you for your service. To ensure your organization can continue its good work, you have an obligation to ensure it has taken steps to reduce its liability risks.

One liability lawsuit against a nonprofit can force it out of business, no matter how worthy its mission or works. The following article provides a very brief overview of some topics to discuss with your insurance agent.

Like for-profit organizations, nonprofits face the most common types of liability risks: personal injury lawsuits, contract disputes, and employment disputes. A general liability policy will protect your organization from many types of liability claims, but not all. If someone with your organization causes harm to another person while doing the organization's work, the policy will protect you in case of law-

continued on next page

This Just In

Discount retailer Dollar General faces fines of up to $4 mm for improperly using credit information to deny jobs to applicants. Dollar General's actions allegedly violated the federal Fair Credit Reporting Act (FCRA).

The FCRA allows employers to conduct a "consumer report," or employment background check. Consumer reports can contain information from a variety of sources, including credit reports and criminal records. When using this information, employers must comply with certain rules:

- **Tell the applicant or employee in writing that you might use the information in their consumer report for decisions related to their employment.**

continued on next page

suit or claim. They pay costs you become legally obligated to pay another person or entity, such as damages or settlements, along with related legal fees.

A business owner's policy will also provide liability coverage. Despite the name, nonprofits can buy these package policies. They combine into one policy insurance for general liability, property insurance and business interruption. Business interruption can pay a nonprofit's ongoing expenses for up to 12 months if a covered event forces a closure.

Bodily injury occurs when someone other than an employee is injured on your premises or is injured by an employee or volunteer while he/she is doing the work of your organization. Nonprofits dealing with vulnerable populations, such as children, elderly or disabled individuals, have higher chances of bodily injury and personal injury claims than other organizations. They should take special steps to screen and train employees and volunteers and to protect the people they serve.

Personal injury: A claim of personal injury involves non-bodily injury of an individual, such as humiliation, loss of reputation or misappropriation of a person's image. Complying with any applicable state or federal nondiscrimination laws and the latest professional standards for your field can help you avoid many potentially risky situations. To avoid claims of misappropriation of image, be sure to obtain photo and video releases before using a person's image in any advertising or promotional material, including social media.

Contract disputes: Any nonprofit should have procedures in place for signing contracts. First, be sure that staff and board members know who has authority to enter into a contractual agreement on behalf of the organization. Second, develop protocols for having contracts reviewed when necessary. Contracts involving employment, over a certain dollar amount or that involve any sensitive or potentially risky situations should require the review of more than one staff or board member, plus your insurance agent and/or attorney.

To avoid any personal obligation, directors and officers should verify that any contract they sign on behalf of the corporation clearly indicates that they are signing in their official capacity.

Employment disputes: Employment disputes can be some of the most costly and disruptive liability claims for any organization, whether for-profit or nonprofit. Employment disputes can include claims such as harassment or discrimination on the basis of age, race, gender and pregnancy or family status. Some states further protect individuals against discrimination on the basis of sexual orientation.

Unlike the other liability risks mentioned above, your general liability or business owner's policy will NOT cover employment-related claims. For these, you'll need a separate employment practices liability (EPL) policy.

Volunteers: When volunteers cause harm to other people in the course of their official duties, the law will likely consider them agents of the organization…making the organization liable. It therefore pays to give your volunteers adequate screening and training for the type of work they'll be doing.

What happens if a volunteer is injured while working? Unless you specifically cover volunteers as employees, your workers' compensation insurance won't apply. Unlike employees, a volunteer can sue your organization for injuries, so you might want to consider covering your volunteers with workers' compensation. Letting them know they have this coverage could help you avoid litigation and improve morale among volunteers, who know the organization will take care of them.

Errors and omissions/professional liability: Most general liability policies exclude coverage for professional liability, or injury caused in the rendering of professional services. If your organization provides professional services, such as health or mental health services, you might have no coverage if someone in your organization causes harm to a client. Errors and omissions or professional liability insurance will fill this gap.

continued on next page

This Just In

The notice cannot be in an employment application—it must be a standalone document.

- **Get the employee or applicant's written permission.**
- **Certify compliance to the company from which you are getting the employee or applicant's information. You must certify that you notified the individual, obtained their permission to get a consumer report, complied with FCRA requirements and will not discriminate against the individual or otherwise misuse the information in the consumer report.**

For a review of your hiring practices and suggestions on minimizing employment-related risks, please contact us.

Directors and officers: Liability claims against directors and officers might be one of the most overlooked risk exposures for smaller nonprofits. In some cases, third parties who are harmed by the nonprofit's activities will sue its directors and officers in addition to the organization itself. Employees can also sue directors and officers for discrimination and other "employment practice" wrongs.

Although many states have immunity laws to protect volunteers, they vary by state and might not always apply. For these cases, you'll want directors and officers liability (D&O) insurance. If your organization lacks specialized insurance coverage, your directors and officers could be held personally liable.

D&O policies are nonstandard, but most have two parts. Part A applies if someone brings legal action against individual directors and officers for alleged wrongful acts committed in the course of their duties. This coverage will pay benefits directly to the directors and officers for settlements or damages and related legal costs. Part B reimburses the organization itself when it indemnifies (covers) the directors and officers. Some policies also cover the organization itself (Part C).

Every nonprofit has different risk exposures. We can help you review your exposures and design an appropriate insurance program to cover them. Please contact us for more information.

Why You Need a Data Management Plan

Each record of sensitive personal information stolen or compromised costs companies an average of $201. That adds up to $5.9 million for every organization that had a data breach.*

When people trust you with their personal information, they expect you to protect it. When something goes wrong and their data gets lost, stolen or compromised, they get angry. According to the Ponemon Institute's 2014 Cost of Data Breach Study, companies suffering a material data breach in 2013 lost an average of $3.2 million in business. This comes in addition to the cost of remediating a data breach.

What Are Your Odds?

A survey by PricewaterhouseCoopers LLP found that information security breach incidents increased 48 percent this year, to 42.8 million, or the equivalent of 177,339 incoming attackers per day.

The Ponemon Institute's study found that malicious or criminal attacks caused 44 percent of data breaches, the highest cause. Human error caused 31 percent, while system glitches accounted for 24 percent. Security breach risks vary by industry and business size: calculate your organization's odds of experiencing a data breach at: http://databreachcalculator.com.

Both physical and electronic data can be compromised, but electronic breaches have higher loss potential. An electronic data breach can occur when:

- Unauthorized users gain access to electronic documents containing personal identifying information (PII) via sharing of passwords, leaving work station unlocked/unattended, etc
- PII is posted, in any format, onto the world wide web without authorization.
- A laptop or smartphone containing PII is lost or stolen.
- Someone steals data from a laptop or other device connected to an unsecured wireless network.

So…what can you do to protect your organization from data breaches?

continued on next page

Step 1: Protect

Ponemon found that organizations with a strong security plan lowered data breach costs by as much as $21 per record. To implement a data protection program, involve your IT team and data end users to identify specific risk exposures.

Consider the following: 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?

Organizations can control access to sensitive data by:

- 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.

Cloud computing creates new security exposures. Before entering into a cloud computing arrangement, check your vendor's security protocols. Will any ownership/access issues arise? Check your contract with any cloud computing vendors to ensure you retain ownership of your data and that the vendor will not mine it or use it for its own purposes.

Step 2: Plan

The Ponemon survey found businesses with a formal incident response plan lowered costs of responding to a data breach by $17 per record. Having procedures in place can help you quickly collect and preserve data and gather evidence about the incident as soon as it's reported.

You'll need to determine whose records have been compromised and how you are going to notify them. On the federal level, the Health Insurance Portability and Accountability Act (HIPAA) protects an individual's health information. No federal law at this point requires organizations to notify individuals when other personal information is breached, however.

Currently, 47 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have laws requiring private or government entities to notify individuals when their personally identifiable information is breached. These laws vary and may apply to different types of organizations. They may also have different definitions of "personal information" that trigger a notification requirement. For information on your state's requirements, see the website of the National Conference of State Legislatures, www.ncsl.org.

Involve your public relations staff or counsel as soon as you learn of the breach. Inform your customers and the public sooner rather than later to look proactive. Be honest in reporting how the breach occurred, what you are doing to prevent similar incidents, and what other security measures you are taking.

According to the California attorney general, nearly one in four recipients of breach notices in the U.S. became a victim of identity theft in 2012, more than four times the rate of the general population. For that reason, many organizations offer victims of a data breach a year's worth of identity theft protection.

Step 3: Insure

The standard general liability (GL) policy excludes coverage for loss or damage to electronic data. You can buy an endorsement that adds a separate sublimit of coverage for loss of electronic data only due to damage to tangible property.

To protect your organization from breach of data due to theft or negligence, you'll need cyber liability coverage. You can buy this coverage as a freestanding policy or as part of a professional liability policy. Policies vary by insurer, but may cover:

- Privacy claims: 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.
- Security losses: Losses due to a failure in network security, such as unauthorized access, virus transmission or destruction of software and data.
- Web or online liability: Losses caused by infringement, defamation, plagiarism or negligence arising from the organization's web site or social media. Policies might exclude this coverage for publishing or media-related businesses; you might have to obtain a separate publisher's or media liability policy.

To learn more, please give us a call.

**Source: 2014 Cost of Data Breach Study: United States. Ponemon Institute, May 2014. http://ponemon.org*

Additional Insured Coverage

Additional insured coverage can protect your organization from liability due to contractors' and subcontractors' operations

Liability insurance covers you from losses due to claims your company, its employees or products or services caused harm or wrong to a third party. Sometimes, however, your organization can be considered "vicariously liable" when another business, such as a subcontractor, causes harm when doing work on your behalf. In these cases, you would want the contractor or other business' policy to apply rather than yours.

***Black's Law Dictionary* defines "vicarious liability" as: The imposition of liability on one person for the actionable conduct of another, based solely upon a relationship between two persons.**

There are two ways to obtain coverage under another entity's policy. In the first, "contractual indemnity," your contract with the other party requires it to "indemnify," or cover you for any liability costs resulting from your joint operations. Alternatively, you can also require the other party to name your firm as an additional insured under its insurance policy.

Obtaining additional insured status often provides greater protection than contractual indemnity. Some states and courts look unfavorably on contractual indemnity, because subcontractors who want business sometimes have little bargaining power. Additional insured coverage, on the other hand, causes no such problems.

For your contractor to provide you with "additional insured" coverage, it must obtain an additional insured endorsement, which modifies its general liability policy. Unlike the policy owner (or "named insured"), the additional insured has no responsibility for keeping any records needed for determining premiums, paying premiums or reporting claims.

When you require additional insured coverage under another organization's policy, you'll probably ask for a certificate of insurance to provide proof of coverage. Be aware that the certificate provides proof that the coverage existed on the date the certificate was issued. The named insured can cancel coverage without providing notice to you. You can request the insurer to provide you thirty days' notice of cancellation or nonrenewal of the endorsement. However, the certificate is not part of the policy and not binding on the insurer. In the case of large or high-risk projects, you can request that the contractor modifies its policy with an endorsement that obliges the insurer to provide this notice.

Considerations for Subcontractors

If the shoe is on the other foot and you are a subcontractor, obtaining additional insured endorsements for contractors and providing the required certificates can be an administrative hassle. To solve this problem, you can buy a blanket additional insured endorsement. This provides additional insured coverage to any party with which you enterv a contractual agreement (typically a construction contract or equipment rental contract).

Blanket additional insured endorsements are not as desirable for the additional insured. Blanket endorsements do not name specific additional insureds, so the insurer cannot provide notice of cancellation or nonrenewal. They usually provide narrower coverage as well—for example, many of these endorsements state that coverage ends when operations are completed. This could be construed to eliminate coverage for claims that occur during operations but aren't filed until later.

For more information on covering additional insureds, please contact us.

Gun Rights vs. Employer's Property Rights

The debate over gun rights often pits the individual's right to bear arms and the rights of private property owners, such as employers, to prohibit firearms on their premises.

The Second Amendment is one of the most widely disputed provisions of the Bill of Rights. Two opposing interpretations dominate the debate: one that the amendment is intended to protect an individual's right to bear arms, and the other that its purpose is to protect the states' rights to maintain militias.

Forty-one states have "right to carry" laws, which allow individuals to carry weapons. Of these, 38 require individuals to apply for a permit; two have discretionary-issue carry permit systems. Vermont allows individuals to carry a weapon without permit, while Alaska, Arizona and Wyoming have a system whereby they will issue permits for permit reciprocity with other states. Currently, only the District of Columbia bans private individuals from carrying a concealed weapon.

What about Private Workplaces?

In most states, concealed weapons laws contain provisions that allow employers to prohibit possession of concealed weapons on their premises, and/or that prohibit carrying concealed weapons at certain "safety sensitive" sites, such as banks or schools.

Gun right advocates say that employer weapons bans violate their Second Amendment right to bear arms. At least 12 states, including Alaska, Arizona, Florida, Georgia, Kansas, Indiana, Louisiana, Kentucky, Minnesota, Mississippi , Oklahoma and Virginia, have laws that either expressly allow individuals with carry permits to keep weapons in their locked cars, or expressly prohibit employers from banning employees from keeping weapons in their locked cars while in the employer's parking lots. (Most of these laws do restrict the right to bring firearms into certain safety-sensitive areas, such as prisons, schools, etc.)

In most instances, employers can still exercise their private property rights and prohibit employees from bringing firearms into their buildings if they post notices conspicuously at all entrances. Many safety experts recommend banning weapons to protect employee safety and limit the employer's liability for weapons-related injuries and deaths. Before implementing a weapons ban, however, employers should know the concealed weapons laws that apply in their state or municipality. For information, contact an attorney. ■

Insurance Buyers' News