



COLBURN GROUP

I N S U R A N C E

NEWSLETTER

Welcome to Colburn Group's Newsletter!

This newsletter includes discussions of pertinent risk management topics that we hope you will find interesting and informative. Please do not hesitate to contact us if you would like more information about any of the topics discussed. Colburn Group provides a broad spectrum of insurance products including commercial insurance, personal insurance, life, disability and long term care.

Harry S. Colburn

Pamela Colburn Haron

Leslie E. Colburn

Third Party Coverage Is a Key Coverage of Employment Practices Liability Insurance

Employment Practices Liability policies respond to claims alleging sexual harassment, wrongful termination and discrimination. The purpose of third-party coverage in an Employment Practices Liability (EPLI) policy is to protect an organization and its employees from accusations of wrongful acts committed against customers, clients, vendors, and suppliers. Some EPLI policies also cover wrongful acts committed by third parties against the insured's employees.

Harassment and all forms of discrimination are covered under wrongful acts. Discrimination claims include discriminatory practices against a person based on their race, religion, age, sex, national origin, disability, pregnancy or sexual orientation. Harassment involves unwanted sexual advances or requests for sexual favors. Both verbal and physical conduct, as well as other forms of harassment that create a hostile or offensive work environment, are covered. Some policies also cover accusations of mental anguish, emotional distress, humiliation and assault.

If your organization has a lot of interaction with the public, it is especially vulnerable to third-party claims like those described above. In some cases, EPLI carriers may not provide third-party coverage to firms with a high potential for claims. What they might offer instead is limited coverage, such as covering accusations of discrimination, but not harassment claims.

In addition to purchasing coverage, you must also implement policies and procedures that address discrimination and harassment issues, both from the standpoint of an employee's actions and the actions of third parties. EPLI insurers are increasingly requiring employers to implement these practices before they will issue a policy.

Having policies in place will offer little help to stop third-party claims if employees aren't adequately trained. New employee orientation programs should include a presentation outlining the organization's harassment/discrimination policies. The training must also include how to report and handle



a third-party claim. However, hearing the information once is not enough to insure compliance. Employees must be periodically retrained through departmental meetings. To maintain the effectiveness of departmental training sessions, be sure that supervisors are provided with copies of all policy updates and procedural changes.

One important caveat to keep in mind is that most EPLI policies don't provide third-party coverage for accusations involving the violation of the Americans with Disabilities Act. Nevertheless, you should review your EPLI policy's definition of a claim to determine the policy's interpretation. Many policies define a claim as a "demand for monetary damages." This definition can present a problem in an ADA claim, because many of these claims are asking for reasonable accommodations, not monetary awards. That's why it is important to ensure that your policy's definition of a claim includes claims for non-monetary damages. A policy with this expanded definition will cover defense costs and indemnity connected with an ADA claim, but will not provide the funds to bring your organization into compliance with the provisions of the law.

When Disaster Strikes: Emergency Preparedness Helps Ensure Business Continuation

The events from 9/11, Katrina, Wilma, and the blackout of 2003 are wake-up calls to the kinds of dangers and challenges facing America, including American businesses. In the months following each event, companies across the country took steps to ratchet up security and emergency preparedness, in the event that they—their operations and employees—might someday be directly impacted by an attack or other major disaster.

A 2002 Hartford Financial Services Group survey found that security measures instituted or improved upon by companies after 9/11 drastically reduced the number of unauthorized visitors entering workplaces. As time passed, however, companies relaxed their post-disaster security consciousness. Unfortunately, emergency preparedness gaps are particularly apparent in smaller businesses.

As we know very well, natural disasters (hurricanes, tornadoes, blizzards), fires, and power outages all can endanger employee security and stymie business operations. The extent to which a company is prepared for such events can mean the difference between being able to continue operations and shutting down. The American Red Cross' statistics show as many as 40 percent of small businesses do not reopen after a major disaster.

According to the Hartford survey, the top workplace safety threat continues to be that posed by unauthorized entries into a business. Employers can take measures to reduce the number of unauthorized entries: check that all entry doors have working locks; reduce the number of entry points, and have all of them set up so that individuals coming in through them must pass by a receptionist or other staffed workstation; implement photo IDs for employees; require that visitors sign in and wear visitor badges; and establish a procedure that receptionists can use to inconspicuously signal that they need help (such as a call button).

The survey found that fewer than half of small businesses hold regular emergency evacuation drills. While such drills for all companies are valuable and necessary, they are suited only for situations in which safety is to be found outside of the business premises. Companies also must be prepared for emergencies that confine employees inside the building, such

as a blizzard, or a situation involving outside release of a chemical or biological agent. Businesses should have on site a supply of bottled water and nonperishable food; flashlights and batteries; a battery-powered radio; a landline phone that can operate without electricity; and first-aid supplies. Detailed lists of suggested "emergency" items for businesses can be found on the Web site of the American Red Cross (www.redcross.org).



Other basic steps businesses should take to prepare for disaster situations include—

- Establish emergency evacuation routes and conduct regular emergency evacuation drills.
- Copy or back up important, valuable, or irreplaceable documents, and store these off site.
- Keep an up-to-date list of contact information for employees, customers, suppliers, distributors, and professional service providers (e.g., insurance agent, accountant, lawyer), and store this list off site.
- Establish procedures for handling suspicious mail.
- If the nature of the business permits, formulate a plan for continuing operations from an alternate site.
- Make sure that the insurance coverages held by the business are appropriate and adequate, and store a copy of the policies off site.

Depending on a company's location and the nature of its business, it may be more or less susceptible to certain risks than others. Please call our office for help in evaluating your risk profile and for learning about business safety and emergency preparedness programs.

Is Your Cyber-Policy Really Covering Your Technology-Related Exposures?

As businesses become increasingly reliant on technology to store sensitive information, the incidences of security breaches are becoming more prevalent. Each security breach increases the risk that a lawsuit or regulatory action could financially ruin a company and permanently damage its reputation. The situation is so bad, that some retailers and financial institutions targeted by litigation and regulatory actions are trying to hold their technology vendors accountable so they can transfer some of the fallout.

A security breach can trigger the need for a number of coverages, including crime, errors and omissions, employment practices liability, general liability, property and directors and officers liability. The so-called "cyber" policies address only one aspect of the exposure, the theft of information, money and identities through the Internet. That's because these are major problems that are on the rise. According to Privacy Rights Clearinghouse, since February 2005, there have been more than 260 major security breaches involving nearly

continued on page 3

Home Care Equals One-Third of All Long-Term Care Claims Paid in 2006

A recent American Association for Long-Term Care Insurance study revealed that total long-term care insurance claims rose to \$3.3 billion for 2006.¹ This figure represents the highest amount of benefit payments to Americans for a one-year period ever.

Of the total, 34 percent of the insurance benefit payments made by eight of the nation's largest insurers covered home care expenses. Additionally, 30 percent of benefits paid were for assisted living costs and the remainder, 36 percent, was allocated toward nursing home care. The largest single claim paid to date was more than \$875,000. In fact, the largest claims paid by leading insurers ranged from well over \$350,000 to one approaching \$900,000.

The data also revealed that approximately eight million Americans now own long-term care insurance obtained individually or through their employer. The researchers concluded that the increasing amount of benefits paid to policyholders is proof of the growing need for long-term care insurance.

To encourage more consumers to buy long-term care insurance, The National Association of Insurance Commissioners has developed the following consumer guidelines to help you select the right policy:

- The policy should cover at least one year of nursing home or home health care, including intermediate and custodial care. Nursing home or home health care benefits should not be limited primarily to skilled care.
- The policy should also provide coverage for Alzheimer's disease if the policyholder develops it after purchasing the policy.
- Inflation protection is critically important. The policy should offer a choice between:
 - Automatically increasing the initial benefit level on an annual basis.
 - A guaranteed right to increase benefit levels periodically without providing evidence of insurability.
- Your insurer should offer you a coverage summary that describes the policy's benefits, limitations, and exclusions, and also allows you to compare it with others. They should also provide a long-term care insurance shopper's guide that helps you decide whether long-term care insurance is appropriate for you.
- There should be a guarantee that the policy cannot be canceled, non-renewed, or otherwise terminated because you get older or suffer deterioration in physical or mental health.
- The insurer should permit you to return the policy within 30 days of purchasing to receive a full premium refund.
- No requirements should exist that policyholders:
 - First be hospitalized in order to receive nursing home benefits or home health care benefits
 - First receive skilled nursing home care before receiving intermediate or custodial nursing home care
 - First receive nursing home care before receiving benefits for home health care

¹ 2007 LTCi Sourcebook published by the American Association for Long-Term Care Insurance

continued from page 2...Is Your Cyber-Policy Really Covering Your Technology-Related Exposures?

100 million personal records. But if a company has only this basic coverage, they may not be prepared if disaster strikes. They should consider a more company-wide approach that includes insurance coverage for all possible exposures associated with a breach.

At the very least, your cyber policy should provide coverage in the following general risk areas:

- Defense Coverage – Some policies limit the insurer's duty to defend to actual lawsuits. That means that the insurer isn't required to defend the insured against a claim, which may or may not result in a lawsuit. Others extend the duty to defend to all claims. You should look for the provision to defend against all claims in a cyber policy. You also need to review the policy in terms of who has the right to choose the attorney who will defend the claim. Many insurers can provide a choice of counsel provision that allows the company to make that choice. Talk to your insurer about having this provision incorporated into your policy.
- Business-to-Business Coverage vs. Business-to-Consumer Coverage – If you want coverage for either or both of these risks, you have to make this known to your insurer. You need to be sure that the various exclusions and/or conditions necessary to minimize gaps in either coverage are present in your policy. These include electric/mechanical breakdown exclusion; breach of security exclusion; bodily injury/property damage exclusion; and employee malicious conduct exclusion.
- Intellectual Property Infringement Coverage – All cyber insurance policies provide some level of intellectual property infringement coverage. However, some policies offer less coverage than others. Some even exclude coverage for software copyright infringement. Review the policy before you purchase to understand how much protection you have in this area. Most insurers are willing to insure software copyright infringement risk for an additional premium. Please call us to develop a plan that is right for you.

Loss Control Tips for Laptops

Have computer will travel. More and more businesses are learning that these four words make up one of the secrets of staying competitive. For meetings outside of the office, you have to take your show on the road and the best way to carry everything you need to make a presentation is on your laptop. But along with this freedom of mobility comes a Pandora's box of problems. The only way to keep the lid on the box is to practice some basic loss prevention techniques.

Whenever you travel, you should carry your laptop in a nondescript case. It should never look as though you're carrying a computer. Never let your laptop leave your sight and secure it in the hotel safe when it is not in use. Do not make the mistake of thinking it is safe locked up in your hotel room. Your room is open and vulnerable when the maid is cleaning it and there is the possibility that somebody can walk in unnoticed and take it.

When you are attending an off-site meeting, be sure that your laptop is secure during breaks. Be aware of your surroundings. Take notice of the various ways to enter your meeting room and make sure that all doors are locked during breaks. If they aren't, take your laptop with you.

Never leave a laptop in plain sight in a locked vehicle; and never put it in the trunk unless there is no other alternative. Thieves assume valuables are in a trunk and that's the first place they look. When you fly, never check a laptop as luggage. It can be stolen or, at the very least, damaged as a result of rough handling. When you go through airport security,

take the laptop out of the case and hand it to the guard before you walk through the metal detector.

Of course, a laptop's portability also makes it a security risk even when you are in your own office. You should always keep your laptop in a secure location when not in use. Lock it up or take it with you when you go out to lunch or to a meeting in another part of the building. Keep a record of the make, model, and serial number of your laptop in the event it is stolen.

Preventing loss applies to your data too. You should keep a regular data back-up schedule so that you will not lose valuable documents in the event of equipment failure. You should also minimize the amount of proprietary data or intellectual property that is stored on the hard drive. Develop a two-tiered password system or use data encryption to protect information that is stored on your hard drive.

Another way you can protect your laptop, which is well worth considering, is arming it with a tracking device. These operate using the same principle a LoJack system uses to protect your car from being stolen. You install software, which runs unobtrusively in the background, reporting in to the security company on a pre-set schedule. The software program tells the security company who logged in on the laptop, and the IP address that it's using. If a laptop is stolen, the security company will change the computer's reporting schedule to be more frequent. The thief is unaware that every time he/she goes online, the laptop's location can be tracked.



COLBURN GROUP
I N S U R A N C E

3001 W Big Beaver Road • Suite 302
Troy, Michigan 48084-3192

NEWSLETTER