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

Insurance Buyers' News • January/February 2014 Volume 25 • Number 1

When Cupid Strikes in the Office

Valentine's Day is coming, and love is in the air—even in the office. In a CareerBuilder poll released in 2013, 39 percent of workers said they have dated a co-worker at least once over the course of their career; 30 percent of those who have dated a co-worker said their office romance led them to the altar. It's the ones that don't that more likely cause problems for employers.

A soured relationship can lead to claims of sexual harassment, particularly when it involves co-workers on different rungs of the corporate ladder. Sexual harassment in the office, pervasive a generation or two ago, has become less acceptable due to changing social norms and more employer awareness and training. However, that does not mean it is not a problem. A generation ago, the victim of sexual harassment probably would have quit her job. Now, she (or he) can sue.

In 2011, the last year for which complete figures are available, the U.S. Equal Economic Opportunity Commission (EEOC) reports that it received 11,364 sexual harassment complaints. Of these, 10.9 percent

continued on next page

This Just In

The Terrorism Risk Insurance Act (TRIA) will expire at the end of this year unless Congress reauthorizes it. An expiration could have repercussions throughout the insurance industry. TRIA encourages insurers to cover terrorism risk by creating a federal reinsurance program, which will kick in if claims paid by private insurers reach a certain maximum.

What could happen if TRIA expires? Without TRIA, many insurers would cease covering terrorism-related property damage. Lenders require terrorism coverage, so the lack of it could stall construction of commercial space, particularly in urban areas. Workers' compensation law requires employers to cover all

continued on next page

came to a settlement, 9.1 percent were withdrawn "with benefits," and 26.1 percent were resolved "with merit." Complainants won $52.3 million in monetary benefits, which does not include monetary benefits obtained through litigation.

In addition to the cost of settlements and litigation, employers facing a sexual harassment claim can suffer a hit to their reputation and staff morale. As the EEOC says, "Prevention is the best tool to eliminate sexual harassment in the workplace."

What Exactly Is Sexual Harassment?

The EEOC defines two types of sexual harassment: quid pro quo harassment and "hostile environment" harassment. In quid pro quo harassment, someone in power exchanges something (such as a raise or promotion) for sexual favors. This type of harassment is usually initiated by those in supervisory positions.

A "hostile work environment" can occur whenever unwelcome sexual conduct creates an environment that employees view as hostile or intimidating. Such conduct can include making unwelcome sexual advances or sexually offensive remarks, displaying sexually explicit pictures, or making crude jokes or obscene gestures.

Affairs between co-workers can sometimes lead to problems with other workers. Some courts have recognized "sexual favoritism" as sexual harassment because it creates a "hostile work environment" for the other workers.

What Action Steps Can Employers Take?

Until the 1970s and early 1980s, many companies banned employee dating outright. As of 2005, only 18 percent of human resource managers surveyed by the Society of Human Resource Management said their employer had written policies on workplace romances. Of those that did have written policies, 20 percent permitted romances among co-workers, 48 percent "permitted but discouraged" them, 31 percent forbade them, and 2 percent did not know.

Some companies take a proactive approach to dealing with interoffice romances. When an interoffice romance comes to light, some have the parties involved sign a "love contract," which stipulates that the relationship was entered into willingly and that, if it ends badly, neither party will hold the employer liable for sexual harassment.

If the relationship involves a subordinate and supervisor, some companies provide the parties a notice stating sexual harassment is a form of sex discrimination that violates Title VII of the Civil Rights Act of 1964. Other companies prohibit these relationships outright and require the transfer of one of the employees to another department when a relationship occurs or becomes public.

However, employers should be careful not to violate employees' privacy. Even if you suspect an interoffice romance, do not overstep. You probably will not want to make inquiries unless the relationship is between a supervisor and subordinate, has triggered complaints from one of the parties or other employees, or has affected work performance.

If you're interested in developing a written workplace romance policy, see the website of the Society for Human Resource Management (SHRM)'s template at www.shrm.org/TemplatesTools/Samples/Policies/Pages/CMS_006713.aspx. If you have concerns over a particular situation, though, you might want to consult an attorney experienced in employment matters. Your commercial general liability policy does not cover sexual harassment and other employment-related lawsuits. For information on protecting your company from the financial risk of sexual harassment and other employment-related lawsuits with employment practices liability insurance, please contact us.

This Just In

work-related injuries, so insurers cannot exclude terrorism from workers' comp policies. That could affect the rates employers pay, particularly those in urban areas.

The TRIA Reauthorization Act of 2013, which was introduced by Representatives Michael G. Grimm (R-NY) and Carolyn Maloney (D-NY) in late 2013 would extend the Terrorism Risk Insurance Program for five years, through December 31, 2019.

Does your organization have, or need, terrorism coverage? Please contact us for more information.

10 Cyber Security Tips for Small Business

Hackers gained access to data from some 40 million debit and credit cards of people who shopped at Target during the busy Christmas season. If it can happen to the country's third-largest retailer, it can happen anywhere.

The Federal Communications Commission offers the following tips to help small businesses protect their networks and prevent security breaches.

1 Train employees in security principles.

Establish basic security practices and policies for employees, such as requiring strong passwords, and establish appropriate Internet use guidelines that detail penalties for violating company cybersecurity policies. Establish rules of behavior describing how to handle and protect customer information and other vital data.

2 Protect information, computers and networks from cyber attacks.

Keep clean machines: having the latest security software, web browser and operating system are the best defenses against viruses, malware and other online threats. Set antivirus software to run a scan after each update. Install other key software updates as soon as they are available.

3 Provide firewall security for your Internet connection.

A firewall is a set of related programs that prevent outsiders from accessing data on a private network. Make sure the operating system's firewall is enabled or install free firewall software available online. If employees work from home, ensure that their home system(s) are protected by a firewall.

4 Create a mobile device action plan.

Mobile devices can create significant security and management challenges, especially if they hold confidential information or can access the corporate network. Require users to password protect their devices, encrypt their data and install security apps to prevent criminals from stealing information while the phone is on public networks. Be sure to set reporting procedures for lost or stolen equipment.

5 Make backup copies of important business data and information.

Regularly backup the data on all computers. Critical data includes word processing documents, electronic spreadsheets, databases, financial files, human resources files and accounts receivable/payable files. Backup data automatically if possible, or at least weekly and store the copies either offsite or in the cloud.

6 Control physical access to your computers and create user accounts for each employee.

Prevent access or use of business computers by unauthorized individuals. Laptops can be particularly easy targets for theft or can be lost, so lock them up when unattended. Make sure a separate user account is created for each employee and require strong passwords. Administrative privileges should only be given to trusted IT staff and key personnel.

7 Secure your Wi-Fi networks.

If you have a Wi-Fi network for your workplace, make sure it is secure, encrypted and hidden. To hide your Wi-Fi network, set up your wireless access point or router so it does not broadcast the network name, known as the Service Set Identifier (SSID). Password protect access to the router.

8 Employ best practices on payment cards.

Work with banks or processors to ensure they use the most trusted and validated tools and anti-fraud services. You may also have additional security obligations pursuant to agreements with your bank or processor. Isolate payment systems from

continued on next page

other, less secure programs and don't use the same computer to process payments and surf the Internet.

9 **Limit employee access to data and information; limit authority to install software.**

Do not provide any one employee with access to all data systems. Employees should only be given access to the specific data systems that they need for their jobs, and should not be able to install any software without permission.

10 **Have password protection and authentication procedures.**

Require employees to use unique passwords and change passwords every three months. Consider implementing multi-factor authentication that requires additional information beyond a password to gain entry. Check with your vendors that handle sensitive data, especially financial institutions, to see if they offer multi-factor authentication for your account.

Standard business property and liability policies do not cover data losses. To ensure you have coverage when you want it, you need a specialized cyberinsurance policy. Look for a policy that provides coverage for both remediation and fines and penalties.

One of the most common reasons smaller businesses fail to buy cyber-insurance is that they think they are too small for hackers to bother. However, as larger companies do more to secure their technology systems (the Target incident notwithstanding), less-secure small businesses are becoming easier targets for cybercriminals. For more information on these nonstandard policies, please contact us.

When Cupid Strikes in the Office

Valentine's Day is coming, and love is in the air—even in the office. In a CareerBuilder poll released in 2013, 39 percent of workers said they have dated a co-worker at least once over the course of their career; 30 percent of those who have dated a co-worker said their office romance led them to the altar. It's the ones that don't that more likely cause problems for employers.

The commercial general liability policy does not cover professional liability, so your doctor and attorney have malpractice insurance (or we hope they do!) to protect themselves against lawsuit if they make a mistake in the course of offering professional services. While other professionals' work might not have the life and death import of a doctor's, they still can cause bodily, financial or reputational harm to others if they make a mistake. What type of insurance protects them from this risk exposure?

Historically, insurance for professionals such as lawyers was called professional liability (PL); policies for quasi-professionals were labeled E&O. However, insurance companies now tend to use the terms interchangeably.

Both PL and E&O policies cover economic losses suffered by third parties but not property damage—which is typically covered under your general liability policy. Most PL and E&O policies exclude coverage for bodily injury—with a key exception being professional liability/medical malpractice for doctors.

Who Needs Coverage?

In addition to lawyers, doctors and accountants, many businesses need PL insurance. You don't have to consider yourself a "professional" to need coverage for negligent acts. If you give advice and recommendations, if you create programs or products for your customers or if you provide a service, you need liability protection.

Take, for instance, an ice sculptor. A socially prominent couple contracts with an ice sculptor to provide a figure of two swans for their very expensive wedding. When the sculpture is unveiled, the bride gasps—the swans look like ducks. She claims this mistake ruined her wedding and threatens to sue, not just for the cost of the sculpture, but for the cost of the entire reception.

Defense Costs

One of the most important reasons to carry E&O coverage is for defense costs. Even if our ice sculptor can prove that the client signed off on the design before it was unveiled, and it did indeed look like swans, the cost to defend the lawsuit could put a

continued on next page

small small organization out of business.

You can find the most extreme examples of costly lawsuits in the medical field, where 65 percent of claims are withdrawn before trial and 90 percent of claims that go to trial are denied, according to the Physicians Insurance Association of America. Nonetheless, it costs an average of $120,000 to defend frivolous cases.

Tailored Coverage

Whether you buy a PL or E&O policy, it usually will be tailored to the specific needs of your business classification. For instance, a policy for real estate brokers typically includes coverage for failure to advise clients on the existence of fungus, asbestos or bacteria. Policies for accountants might provide coverage for acting as a trustee or administrator of an estate. Some policies also cover inadvertent transmission of computer viruses and corruption of customers' data.

Examples of other professionals who need protection include:

- Real estate agents
- Data processors
- Accountants
- Pest control services
- Appraisers

Many insurance companies offer group policies to members of trade associations. In other cases, insurance companies form buying pools that professionals can "join." Miscellaneous professional liability coverage is also available for a variety of businesses such as translators, meeting planners and collection agencies. If you need coverage, we can advise you on the best approach.

Sole proprietors may choose to protect their personal assets by forming a limited liability company, but their corporate assets are still at risk unless they buy E&O coverage.

Claims-Made Policy

It is important to understand that most PL and E&O policies are written as "claims-made," which means the policy only covers claims filed during the policy period. A few companies offer occurrence-based policies, which cover any qualifying claim arising from an incident that occurred during the policy period—no matter when filed. If you switch from a claims-made to an occurrence policy, you have to make sure you don't create a gap in coverage.

In specific situations, a claims-made policy may allow an extended period for reporting claims: when an insured dies, retires or becomes permanently disabled. This is an important feature, because new claims can be filed years after the policy period. To qualify as a retiree, the insured usually has to be at least 55 years old, and he/she has had to maintain coverage with the same insurance company for several years—something to plan for if retirement is in your near future.

If you have any concerns about the liability coverages for your business, please give us a call.

Don't Toss Those Old Liability Policies

Imagine the worst-case scenario: a customer sues you for injuries allegedly caused by one of your products. Then make it worse: you can't find the policy that might cover that claim.

Most liability policies today are written on a "claims-made" basis, meaning they cover claims reported during the policy term, as long as they result from incidents occurring after the policy's retroactive date. When you first buy a claims-made policy, your retroactive date will likely be the same as the policy's inception date. Ideally, when you renew or replace that policy, the insurer will use the same retroactive date. This gives you continuous coverage back to the retroactive date of your original policy.

Older liability policies are often written on an "occurrence" basis, which means they cover claims that arise from incidents that occur during the policy period, even if the claim is filed years later. These older policies often come into play in cases involving "long-tail" liability claims, such as environmental, product liability and other claims that can take years to develop.

When you make a claim that might be covered by an old insurance policy, it's your responsibility to prove the policy existed. Having the actual document in hand can prevent coverage disputes with your insurer. For this reason, risk management experts strongly recommend keeping all insurance policies, even expired ones, in a safe place, and maintaining a list of policy information (including insurer name, address, type of policy, policy number and inception/expiration dates) in a separate location.

Even if you can't locate an old policy, you might be able to document its existence. Your broker might have a copy (although brokerage firms have no legal obligation to keep copies of clients' expired policies); your accounting department might have records of premium payments; your risk manager might have notes or correspondence relating to the policy or other claims paid under it.

If your organization has long-tail liability exposures, including pollution liability or products liability exposures, you have special risk management needs. Please contact us for an analysis of your exposures and coverage needs. ■

Insurance Buyers' News