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

Risk Management January/February 2017 Volume 28 • Number 1

2017: The Year of the Cyber Attack

Cyber security problems will increase in 2017, warns Experian Data Breach Resolution, a branch of the credit reporting giant.

In its 2017 Data Breach Industry Report, Experian noted it expects to see several new—and frightening—trends:

- "Aftershock" password breaches becoming more common,
- Nation-state cyber-attacks moving from espionage to war,
- Healthcare organizations becoming the most frequently targeted sector,
- Criminals focusing on payment-based attacks, and
- International data breaches causing "big headaches" for multinational companies.

"Aftershock password breaches" can affect organizations that have not experienced a breach of their own data. They occur when

continued on next page

This Just In

In 2016, the EEOC resolved 97,443 employment discrimination charges. It secured more than $482 million for victims of discrimination in private, state and local government, and federal workplaces. This included:

- **$347.9 million for victims of employment discrimination in private sector and state and local government workplaces,**
- **$52.2 million for workers harmed by discriminatory practices, and**
- **$82 million for federal employees and applicants.**

This included 273 resolutions of systemic investigations and 21 resolutions of systemic lawsuits totaling more than $58.3 million in remedies for workers harmed by discriminatory practices and policies.

Through mediations and concilia-

continued on next page

a data breach and passwords from first-hand data breaches become available to criminals and hackers, who then use them to try to break into other networks. Organizations that see repeated unauthorized log-ins need to notify their customers that their data might have been misused.

Action step: Strengthen data protection and make unauthorized log-ins more difficult by using two-part or multi-part authentication protocols. As the name implies, two-part authentication requires more than a password. The user must provide something additional, such as a physical object like a bank card or USB stick with a code; provide secret information, such as a PIN or code from a text message; or match a biometric marker on file, such as a fingerprint, voice, eye iris, etc. Of course, these actions should be part of your comprehensive cyber security plan.

What Is Cyber Security?

Cyber security involves protecting your organization's digital information by preventing, detecting and responding to cyber attacks. Cyber attack dangers include viruses erasing your entire system, someone breaking into your system and altering files or someone using your computers to attack others. However, the biggest cyber security problem that businesses and nonprofits face is protecting the personal identifying information, or PII, of their clients and prospects.

Many organizations today use or store PII. PII is information that can be used to uniquely identify, contact or locate a single person. PII includes but is not limited to:

- Full name
- Social Security number
- Address
- Date of birth
- Place of birth
- Driver's license number
- Vehicle registration plate number
- Credit card numbers
- Physical appearance
- Gender or race

When someone's PII you have stored is stolen or compromised, you are responsible for notifying them of the breach. That costs time, money and reputation. If criminals use PII for identity theft, you could be liable for helping victims resolve the problem, a costly and time-consuming process.

The National Cyber Security Alliance (NCSA), a public/private consortium, reports that 69 percent of small businesses have "… sensitive information, including customer data." Hackers are increasingly focusing on small businesses, knowing that they have fewer resources to protect their data. The NCSA also points out that only half of small businesses (52 percent) "have a plan or strategic approach in place for keeping their business cyber secure."

What Can You Do?

All organizations particularly organizations that use or store others' PII, need a comprehensive data protection plan. Lack of a plan and systems in place can create serious liability exposures.

At a minimum, you should be doing the following to protect your data:

This Just In

tions, EEOC worked with employers to resolve charges voluntarily. Ninety-seven percent of mediation participants reported that they would mediate future charges with the agency. EEOC also maintained a 44 percent success rate for the past two fiscal years for conciliation of charges after a finding of discrimination.

EEOC offers services for employers that want to be sure their policies comply with applicable law—contact your local office for more information. It could save you a discrimination claim!

1. Make sure all company computers have the latest security software, web browsers and operating systems to protect against viruses, malware and other online threats.
2. Turn on automatic software updates, if that's an option. Many updates specifically address known security risks.
3. Scan all new devices, including USB devices, before they are attached to the network.
4. Use a firewall to keep criminals out and sensitive data in.
5. Use spam filters. Spam can carry malicious software and phishing scams, some aimed directly at businesses.
6. Adopt a privacy policy and post it on your website and other online sites. Your policy tells customers what information you collect and how you use it.
7. Know what PII you're storing on your customers, including where you store it, how you use it, who can access it, and how you protect it. Delete any unneeded information.

continued on next page

No matter what firewalls, software and authentication protocols you've installed, your cyber security system is vulnerable if you're not educating your employees on avoiding risky behavior online. The Workplace Security Risk Calculator, available free at https://staysafeonline.org/stay-safe-online/resources/workplace-security-risk-calculator, lets your employees gauge the level of risk their online behaviors pose.

If you don't have the time or resources to create your own cyber security audit and plan, your ISP may offer specialized services for small businesses. The NCSA has a list of other resources available at https://staysafeonline.org/business-safe-online/implement-a-cybersecurity-plan.

No cyber security program is complete without insurance. Cyber insurance can protect your organization from the cost of correcting a security breach, notifying victims and even help protect them from identity theft. For more information, please contact us.

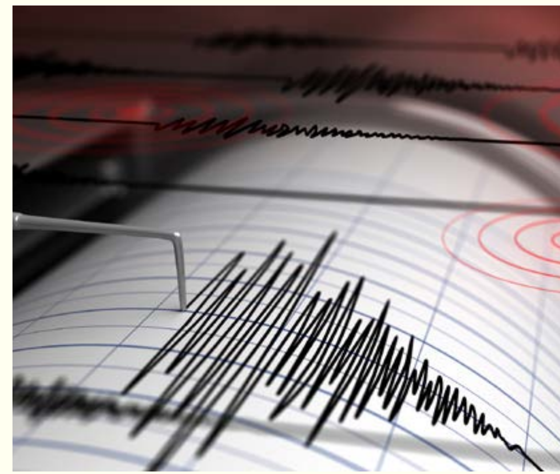
Don't Get Shaken by Lack of Earthquake Coverage

When you think of earthquakes, you probably think of California, or maybe coastal areas of the Pacific Northwest. But 90 percent of the U.S. population lives in earthquake-prone areas. And a recent study by the U.S. Geological Survey found that 7 million people now face the risk of human-caused earthquakes.

"By including human-induced events, our assessment of earthquake hazards has significantly increased in parts of the U.S.," said Mark Petersen, chief of the USGS National Seismic Hazard Mapping Project. "This research also shows that much more of the nation faces a significant chance of having damaging earthquakes over the next year, whether natural or human-induced."

Induced earthquakes are triggered by human activities, particularly the disposal of wastewater from oil and gas production. Wastewater can be disposed of by injecting it into deep underground wells, below aquifers that provide drinking water. Injecting fluid underground can induce earthquakes, a fact that was established decades ago by USGS scientists. This process increases the fluid pressure within fault zones, essentially loosening them and making them more likely to fail in an earthquake. When injected with fluids, even faults that have not moved in historical times can be made to slip and cause an earthquake if conditions underground are appropriate.

Six states face the most significant hazards from induced seismicity. In order from highest to lowest potential hazard, they are: Oklahoma, Kansas, Texas, Colorado, New Mexico and Arkansas. Oklahoma and Texas have the largest populations exposed to induced earthquakes.



How much of an earthquake risk does your business have? To find out, go to the U.S. Geological Survey's page at https://earthquake.usgs.gov/earthquakes/byregion/ and click on your state to find an earthquake hazard map. Please note that these maps are based on 2014 data and do not include the most recent information on induced earthquakes. For information on induced earthquakes, see the map at https://www2.usgs.gov/blogs/features/usgs_top_story/induced-earthquakes-raise-chances-of-damaging-shaking-in-2016.

continued on next page

What Should You Do if You're Located in a Higher-Risk Area?

Standard business property policies exclude coverage for "earth movement," which includes earthquakes. You can add earthquake coverage to your insurance program in one of the following ways:

Standalone policies: Many insurers write commercial earthquake insurance policies. Most will cover buildings, business personal property, loss of business income, sprinkler leakage due to quake, and "ordinance or law coverage," which protects you from increased costs of construction when you must bring existing structures up to current codes. You can find a list of insurance carriers admitted to do business in the state through the state insurance department, or simply contact us.

Policy endorsements: You can buy an endorsement to add coverage to an underlying commercial property policy. ISO form CP 10 40 will add earthquake and volcanic eruption to the causes of loss your commercial property policy covers. It also covers sprinkler leakage due to earthquake, but excludes coverage for fire, explosion (except for volcanic explosions), landslide, mudslide or mudflow, flood or tidal wave, even if caused by an earthquake or volcanic eruption.

As with your property policy, this endorsement has a coinsurance provision. This requires you to carry insurance on a specified percentage of the property's value. Most policies have a coinsurance percentage of 80, 90 or 100 percent. If your insurance limits are less than the coinsurance amount when a loss occurs, the insurer will penalize you proportionately when it pays covered claims.

ISO form CP 10 45 covers the same causes of loss as the CP 10 40, but places a sub-limit on coverage. This means it will cap claim payments for covered earthquake and volcanic eruption losses with a lower limit than other hazards covered by the policy, such as fire. Coverage under this type of endorsement usually costs less.

DIC policies: Some larger companies use DIC policies to insure earthquake exposures. DIC, or difference in conditions, policies are non-standard policies an underwriter can tailor to fill coverage gaps left by exclusions in other property policies. They generally exclude coverage for perils covered by standard property forms, such as fire, windstorm, hail, smoke, explosion, riot, civil commotion, vehicle and aircraft collision, vandalism and malicious mischief and sprinkler leakage. They also usually exclude damage from war and nuclear perils, which are considered too catastrophic to be underwritten.

DIC policies are usually written for a specific limit, such as $5 million or $10 million. Unlike most property policies, most DIC policies have no coinsurance provision, which means you do not have to purchase coverage for a specified percentage of the property's full value.

Because DIC policies fill coverage gaps, your broker should coordinate your DIC policy with your other policies. Most DIC policies require the insured to keep the "underlying" property policies in effect for the entire term of the DIC policy.

We can help you evaluate your earthquake and volcanic eruption risks and recommend appropriate coverage. For more information, please contact us.

Service Animals, Assistance Animals, Therapy Animals—What's the Law?

Guide dogs and service dogs have helped individuals with disabilities navigate life for decades. Now you also see assistance animals, therapy animals and emotional support animals. What's the difference and what's the law?

Many people legitimately need service, support or therapy animals, while others use the "therapy animal" name and even fake vests and registries to sneak their pets into public places. So what rights do users of service animals have?

Employment discrimination: Title I of the Americans with Disabilities Act (ADA) prohibits disability discrimination in employment. If employees or prospective hires need a service animal, you cannot prohibit them from having the animal at the worksite. You can ask the nature of the services the animal performs, but you cannot ask about the nature of the person's disability.

continued on next page

Discrimination in public accommodations: Title II and Title III of the Americans with Disabilities Act (ADA) prohibits privately owned businesses that serve the public, such as restaurants, hotels, retail stores, taxicabs, theaters, concert halls, and sports facilities, from discriminating against individuals with disabilities. The ADA requires these businesses to allow service animals onto business premises in whatever areas customers are generally allowed. As with employers, owners or managers of public accommodations can ask about the nature of the services performed by the animal, but not the nature of the person's disability.

The ADA defines a service animal as any guide dog, signal dog, or other animal individually trained to provide assistance to an individual with a disability. Service animals perform some of the functions and tasks that the individual with a disability cannot perform for him or herself. Guide dogs are one type of service animal, used by some individuals who are blind. Service animals also assist persons with other kinds of disabilities in their day-to-day activities. Examples include:

- Alerting persons with hearing impairments to sounds.
- Pulling wheelchairs or carrying and picking up things for persons with mobility impairments.
- Assisting persons with mobility impairments with balance.

The ADA does not limit its definition of disabilities to physical disabilities—psychiatric, intellectual, or other mental disabilities also qualify. The ADA National Network says, "Tasks performed by psychiatric service animals may include reminding the handler to take medicine, providing safety checks or room searches, or turning on lights for persons with post-traumatic stress disorder (PTSD), interrupting self-mutilation by persons with dissociative identity disorders, and keeping disoriented individuals from danger."

To qualify as a service animal, two conditions must apply: the person must have a disabling condition and the animal must be trained to perform a specific task or tasks. If they meet the definition, the ADA considers animals service animals regardless of whether they have been licensed or certified by a state or local government.

Service Animals vs. Assistance Animals and Therapy Animals vs. Pets

Some people use therapy dogs or emotional support dogs. These animals may provide therapeutic or emotional support to a person with a mental health disability, such as PTSD. They are not trained to perform specific tasks; instead, their mere presence has a calming effect on their owner.

The FHA, Fair Housing Amendments Act of 1988, allows therapy or emotional support dogs to be kept in housing with pet restrictions. If the owner has a verifiable disability, the animal is a "reasonable accommodation." HUD specifically states that "[w]hile dogs are the most common type of assistance animal, other animals can also be assistance animals." Title II and Title III of the ADA do not view emotional support animals, therapy animals and comfort animals as service animals. This means that, outside of housing and air travel, owners of therapy or emotional support animals have no legal right to bring their animals into places where animals are prohibited, even with a doctor's letter.

The ADA and other anti-discrimination laws are complex. Running afoul of them can lead to discrimination claims, fines and negative publicity. A good liability insurance policy can help protect your business from the cost of defending discrimination claims and paying damages, if any—please contact us for a policy review.

more on next page

Climate-Change Disclosures Recommended

Publicly traded companies should disclose their climate-change risks and what they're doing about them, says the Financial Stability Board. The Board, an international body that monitors and makes recommendations about the global financial system, includes members of the G20, government ministers and central bank governors of 20 leading economies.

In 2015, nearly 200 countries agreed to reduce greenhouse gas emissions and accelerate the transition to a lower-carbon economy in the so-called Paris Agreement. "Because this transition to a lower-carbon economy requires significant and, in some cases, disruptive changes across economic sectors and industries in the near term, financial policymakers are interested in the implications for the global financial system, especially in terms of avoiding severe financial shocks and sudden losses in asset values," said the Financial Stability Board's Task Force on Climate Change in a December 2016 report.

In its report, the Task Force urged publicly traded companies to disclose their climate-change risks. According to the report, "One of the most significant, and perhaps most misunderstood, risks that organizations face today relates to climate change. The potential impacts of climate change on organizations, however, are not only physical and do not manifest only in the long term."

Climate-Related Financial Disclosures

The Task Force notes that, "In most G20 jurisdictions, companies with public debt or equity have a legal obligation to disclose material risks in their financial filings—including material climate-related risks. The Task Force believes climate-related risks are material risks for many organizations..." It recommends that these companies include climate-related financial disclosures in their public financial filings. These filings should include information on governance, strategy, risk management, and metrics and targets related to the effects of climate change on the organization.

Failure to disclose information that could affect investors can lead to lawsuits against directors and officers. We can help you mitigate your directors and officers liability risks—please contact us for more information.