Insurance Buyers' News

MOC Insurance Services
Maroevich, O'Shea & Coghlan Insurance

Divisions of MOC Insurance Services
Farallon Associates Insurance Brokers
San Francisco Insurance Center

44 Montgomery Street, 17th Floor, San Francisco, CA 94104
Toll Free (800) 951-0600 | Main (415) 957-0600 | License # 0589960

WWW.MOCINS.COM

Fraud | May/June 2019 | Volume 30 • Number 3

Don't Be the Victim of a Nigerian Prince

You wouldn't knowingly send money to a Nigerian Prince but ransomware and phishing attacks are becoming more sophisticated. Smaller companies are especially vulnerable.

By now, everyone who has heard of the Nigerian Prince emails knows they're a scam. You're told you just need to pay the so-called prince a small advance fee for helping him make a transfer of millions from his Nigerian bank account to yours and he'll reward you handsomely. Of course, after you pay the advance fee, there will either be more small fees to pay or you'll never hear from him again. Or he may even steal everything in your account!

continued on next page

This Just In…

Insurance industry analysts A.M. Best Co., forecasted "overall modest expectations" for U.S. property/casualty commercial price increases in 2019.

Other than automobile, commercial lines are expected to remain flat or decline modestly, says the report.

Price increases are expected to continue in commercial auto, where losses remain a drag on the industry's overall profitability. Otherwise the overall outlook for the industry remains stable, says the Oldwick, New Jersey-based firm in its report *2019 Review & Preview: U.S. Property/Casualty.*

"Workers compensation pricing has seen modest decreases overall in the most recent years, although much of the decline in

continued on next page

Believe it or not, variations of this, known as the "advance fee" scam, are still alive and well. According to Uzi Scheffer, CEO of cyber security firm SOSA, there are two reasons small business are especially vulnerable to this and similar "phishing" scams.

- Since large companies are usually better at protecting themselves against cybercrime, scammers see small firms as the path of least resistance.
- Small firms usually don't have a formal internet security policy, making them even easier targets.

Attacks are getting more sophisticated

Regardless of the type of phishing expedition involved, about two thousand cases of banking malware attacks take place every day in the U.S. alone, stealing financial data without the user even knowing. Using malicious software, called malware, embedded in e-mail attachments like documents, hackers nest themselves into their victim's financial data. Once they've settled in, they need only about 10 minutes to steal or, as with ransomware, cause financial mischief.

Ransomware results from downloading infected files that were attached to an email or obtained from suspicious websites. The ransomware then locks the device it was downloaded onto until a ransom is paid.

There are numerous kinds of sophisticated threats like these out there.

Scheffer recommends that every business, large or small, should take the following steps to lower its risk of falling victim to a cyberattack. General policies should be implemented first, followed up with a routine of taking certain simple precautionary actions on a regular basis.

General policies:

1. **Adopt a cyber security strategy.** Almost every business now makes sales online, even small brick and mortar operations. To ensure even the most modest platform is properly protected, there should be a clear set of directives regarding what should and should not be done online, how to make the devices secure, etc.
2. **Identify your system's vulnerabilities.** This is often part of the underwriting evaluation when purchasing cyber insurance. It's also often a good idea to bring in a professional to point out how best to reduce cyber risks. Unfortunately, only a small percent of small business owners bothers to hire a consultant for such an assessment, but doing so will most likely pay off big in the long run.
3. **Diversify security measures.** Since there are many different types and sources of threats, no one tool can provide a complete defense. You need to deploy a combination of tools, including firewalls, spam filters, automatic data encryption, backup and more.

Regularly scheduled action items:

1. **Make sure employees are trained in basic cybersecurity measures.** Studies show that 90 percent of all cyber security breaches are the result of human error, primarily from non-IT staff members. To minimize threats, staff members should know how to implement the firm's cyber security strategy, how to recognize online threats such as suspicious e-mails, how to identify if a device has been hacked, etc.

This Just In

rates has been offset by higher payrolls due to higher employment levels and some upward pressure on wages," says the report.

A.M. Best estimates the industry will report a 101.5% combined ratio for the industry in 2018 and an improvement to a 101.2% combined in 2019.

U.S. catastrophe losses reached a near-record high in 2017, while in 2018, the fourth quarter's Hurricane Michael and California wildfires drove a second year of catastrophe losses above the long-term average, according to the report.

A. M. Best estimates net catastrophe losses in 2018 totaled $37 billion, compared with $53 billion in 2017. Its projection for 2019 is a decrease to $31 billion.

The report also said that higher interest rates "should provide some tailwinds to the P/C industry given its substantial reliance on net investment income to boost profits," but the fourth-quarter's turmoil in the U.S. and global equity markets is expected to drive down overall investment returns for the year, according to the report.

continued on next page

2. **Ensure cybersecurity tools are updated on every device used in the business.** This should also apply to laptops and mobile devices that are often connected via external Wi-Fi networks.
3. **Download software updates for your operating system and applications.** OS and app providers regularly issue patches for newly discovered security threats which must be installed as soon as they are available.
4. **Back up important data in multiple locations.** With the rapid growth of cloud computing, this has become a relatively easy step to take to ensure that a breach in one site will not cause irreversible damage to the rest of your business.
5. **Enforce strict employee access procedures.** Employees might find some of these rules a nuisance, but you should stress how important they are for maintaining the integrity of what is, given all its vulnerabilities, a very fragile system. Make sure every staff member has their own user name and password. Passwords must be changed regularly and must be complex. Hackers have tools for discovering commonly used passwords (12345, abcde, etc.) in a matter of minutes. Physical access and authorization to download software needs to be limited as well.

"Even if you take all of these steps, there is, of course, no guarantee that your company or store won't fall victim to a cybercrime," says Scheffer. "Perhaps the most important element that needs to change is the false sense of security. Many business managers and owners are complacent, which is exactly what hackers are counting on."

Of course, even with a good cyber security plan in place, your business still needs a failsafe to protect it against cyber risk. So, please be sure to read our Cyber Liability Insurance Policies article.

Preparing for the Worst with Active Assailant Insurance

The coverage was introduced only a few years ago and more companies are now offering it.

Sadly, following incidents like the shootings in Las Vegas, Parkland, Fla., Christchurch, N.Z., as wells as numerous shootings in California and up and down the east coast and elsewhere in the U.S. this year and last year, there is now a growing demand for active shooter insurance.

Indeed, since the coverage was first introduced a couple of years ago, more insurance companies are now offering Terrorism coverage not only as a standalone policy, but as an endorsement to their property, liability and business interruption policies.

What's Covered in Active Assailant Insurance?

In general, these are the main features of a standalone policy, though it may be possible to add them to the appropriate property, liability, or package policy as well:

24/7 Crisis Consultancy: Experienced professionals are available (and promptly on-site) to guide management through the aftermath; this includes engaging with victims' families, liaising with authorities and handling media.

Extra Expenses: Policyholders are able to take a proactive role in assisting victims with medical costs, psychiatric

continued on next page

treatment and funeral expenses. Staffing, premises or security costs incurred following an attack also are covered.

Business Interruption: Active Assailant insurance recognizes that a premises may not be able to reopen promptly following an attack even if repairs have been completed, and indemnifies accordingly.

Loss of Attraction: Business owners may suffer a significant drop in patronage after a serious attack at their premises. The policy will cover the difference in net revenue.

Liability and Defense Costs: Some General Liability policies are silent on the issue of shootings or feature firearms/terrorism exclusions. The Active Assailant market offers clear protection against damages suits and the defense costs involved.

Property Damage: This policy element often acts as 'first dollar' protection. Further market innovation has created a policy that offers Demolition and Rebuild coverage for when a building must be razed following a tragedy.

"One of the most valuable aspects of an Active Assailant insurance program for policyholders is prevention training offered by the insurer," according to Pete Bransden, vice president of Crisis Management at Aspen Insurance Company. "This can range anywhere between providing an Active Shooter e-Learning training module for staff, to carrying out an intensive, on-site simulation exercise and a complete review of written safety policies. Insurers frequently offer significant stipends for such training, if not fund it completely."

Coverage limits may be available up to $25 million. Although originally designed for educational institutions like public and private schools and universities, other entities such as banks, hotels, restaurants, sports venues and amusement parks have been purchasing Active Assailant coverage as well. Some classes of business that may be appropriate include:

- Educational institutions
- Entertainment organizations
- Hotels
- Restaurants and clubs
- Healthcare providers
- Religious institutions
- Retail organizations
- Rodeos, fairs and trade shows.

If your organization or company feels it may be vulnerable to an active assailant risk, please contact us and let us help you assess your situation.

Two Essential Property Endorsements You Need if You Plan to Rebuild after a Loss

Your insurance may cover your losses, but will it be enough to meet new building code requirements if you rebuild?

A good insurance program will protect your business property from loss due to fire, theft, vandalism and more. But without certain important coverages, your property coverage could leave you short of the funds needed to rebuild and recover.

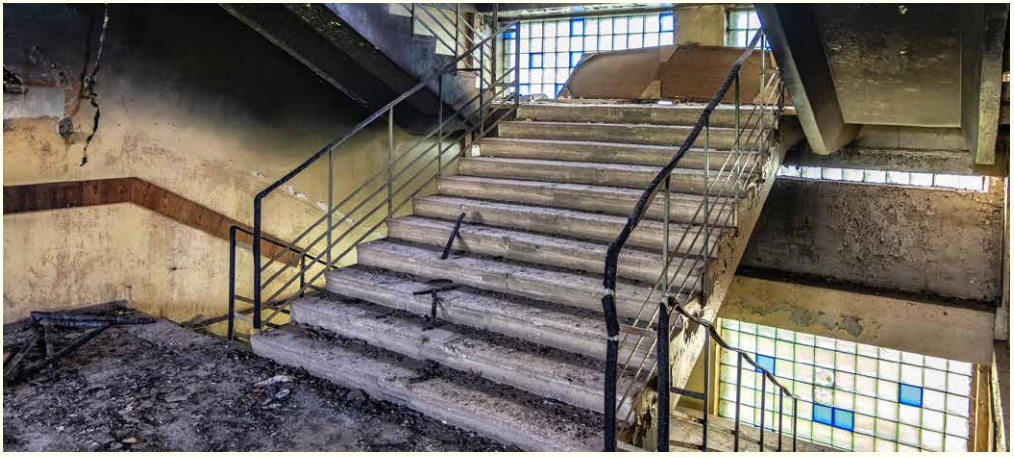
Do you own your business premises? Any building more than a few years old might not comply with current building codes, as well as additional regulations such as the Americans with Disabilities Act.

When property damage forces you to rebuild or remodel, you most likely will have to bring your construction up to current codes. Most property policies exclude coverage for loss due to complying with an ordinance or law regulating construction, repair or occupancy of any building.

So even if your building is properly insured to value, your policy will not cover the additional costs of bringing it up to current codes.

To make matters worse, after a portion of your building is damaged, local authorities will likely require you to repair undamaged portions of your building to bring them up to current codes. And since remodeling usually costs more on a square-foot basis than new construction, these repairs can be costly.

continued on next page



Debris Removal

If a covered peril damages your building, or any part of it, you'll probably have some trash and debris to remove before repairs can begin. Will your insurance policy cover these costs? The typical commercial property policy provides debris removal coverage as an "additional coverage" over and above your property policy's limits. It will "pay your expenses to remove debris of covered property caused by or resulting from a covered cause of loss" and usually limits coverage to 25 percent of "the insurer's liability for the direct property loss by a covered cause of loss, plus any applicable deductible (unless an additional debris removal limit is shown in the declarations)," according to Adjusting Today.

If the total of the direct physical loss costs and debris removal costs exceeds your policy limits, or if debris removal expenses exceed the debris removal "additional coverage" limits, most policies will provide an additional $10,000 in debris removal coverage per incident. In some instances, however, debris removal costs could greatly exceed the cost of the direct property damage. Debris removal can cost more than you might think. If your building is older, it could contain lead paint, asbestos and other contaminants that require special handling and disposal by law.

You might also have debris removal costs even without any covered property damage. For example, a flood or windstorm could deposit debris from another property onto yours. In that case, the debris does not come from "covered property" under the policy, which would not cover removal costs. Exceptions might exist when the debris itself is causing damage to covered property.

Increased Cost of Construction

A policy endorsement, or addition, called "ordinance or law coverage" or "increased cost of construction coverage" can help you cover some of the unexpected costs of disaster recovery.

This endorsement provides three types of coverage when laws or ordinances require you to spend more on reconstruction.

- **Coverage A** covers you for the cost of making required repairs to the undamaged portion of a building.
- **Coverage B** covers you for the costs of demolition and debris removal.
- **Coverage C** provides coverage for increased costs of construction, or your actual costs of bringing the damaged portions of the building up to current codes.

The standard property policy covers none of these costs, so without ordinance or law coverage, the building owners would have to pay these expenses. You can select the amount of additional coverage you need, which will vary with the age of your building, the stringency of applicable building codes, and your exposures to covered causes of loss, such as fire.

To obtain ordinance or law coverage, your property policy must be written on a replacement cost basis, rather than actual cash value basis. If you decide to relocate rather than rebuild after a total loss, your replacement cost coverage would pay the replacement cost of your building, but the increased cost of construction coverage would not apply, since no reconstruction actually occurred.

Does your property policy have these endorsements? If you're not sure, give us a call.

Cyber Liability Insurance Policies

Due to the lack of actuarial data, it's been difficult to price cyber liability insurance. This is one reason Insurers depend so much on evaluating each insured according to its risk management procedures and risk culture. As a result, cyber risk coverages are more customized and, therefore, can be more costly, depending on the vulnerabilities of the system and the environment.

The type and cost of cyber liability coverage offered by insurers is based on the type of business, its size and geographical scope, the number of customers it serves, its web presence, the type of data it collects and stores and other factors, including its risk management and disaster response plan.

Cyber liability policies might include one or more of the following types of coverage, according to the National Association of Insurance Commissioners:

- Liability for security or privacy breaches. This would include loss of confidential information by allowing, or failing to prevent, unauthorized access to computer systems.
- The costs associated with a privacy breach, such as consumer notification, customer support and costs of providing credit monitoring services to affected consumers.
- The costs associated with restoring, updating or replacing business assets stored electronically.

- Business interruption and extra expense related to a security or privacy breach.
- Liability associated with libel, slander, copyright infringement, product disparagement or reputational damage to others when the allegations involve a business website, social media or print media.
- Expenses related to cyber extortion or cyber terrorism.

For more information about cyber security insurance, please contact us.

Insurance Buyers' News