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

Safety | September/October 2019 | Volume 30 • Number 5

Three Recent Efforts to Reduce Gun Violence

Businesses where a shooting occurs risk not only potential lawsuits from innocent customers and bystanders but they will also very likely suffer some business slowdown from loss of reputation.

Gun violence affects all aspects of society, especially businesses, such as the Walmart in El Paso, Texas and the merchants in the Oregon District of Dayton, Ohio, where mass shootings recently took place.

Whether or not federal legislation requiring more stringent background checks or red flag laws that allow guns to be taken away from people deemed suicidal or a threat are enacted, three recent developments will likely have an impact on the controversy.

continued on next page

This Just In…

People who cheat on their spouses are much more likely to engage in workplace misconduct, according to a study from the McCombs School of Business at The University of Texas.

The researchers examined the records of people who used the Ashley Madison marital infidelity website to develop its findings. Data from the website, which operates using the slogan "Life is short. Have an affair," became available in the public domain after a hack in 2015. The researchers, who had access to 36 million user accounts, found that the professionals they studied were more than twice as likely to engage in corporate misconduct than the rest of the population.

After matching misconduct

continued on next page

Families of Sandy Hook Children Can Sue Gun Manufacturer.

In March the Connecticut Supreme Court reinstated a wrongful death lawsuit brought against gun maker Remington Outdoor Co. for manufacturing the rifle used in the 2012 mass shooting at Sandy Hook Elementary School in Newtown, Conn.

Before the suit was reinstated it had been dismissed by a lower court because of a 2005 federal law, the Protection of Lawful Commerce in Arms Act (PLCAA), which shields gun manufacturers from liability when firearms they manufacture are used in crimes, except when the guns are wrongfully sold or marketed.

The families of the children killed at Sandy Hook argued that the gun used by the killer was a weapon of war wrongfully marketed to civilians and thus not protected by the PLCAA.

Remington has asked the U.S. Supreme Court to overturn the ruling, saying that the Connecticut Supreme Court interpreted the exemption too broadly.

Walmart Provides Mandatory Employee Training to Mitigate Casualties of Shootings

After the shooting of 58 people at a music festival in Las Vegas, Walmart began implementing its "Active Shooter" plan, which is said to be mandatory now at all Walmart stores. All employees are supposed to complete the program during orientation when they come on board and get reacquainted with it four times per year.

A few days before the mass shooting that killed 20 people at a Walmart in El Paso, employees at a Walmart in Southaven, Mississippi, acted in accordance with the "Active Shooter" plan and quickly sought to mitigate casualties when a disgruntled employee killed two co-workers and a policeman, by guiding associates and customers to the right exits and out of danger.

"I feel confident in saying that it did (help) in Southaven," said Walmart spokesman Randy Hargrove in a phone interview with Reuters News Service.

It's not clear whether Walmart's "Active Shooter" efforts reduced casualties in the El Paso incident.

Stricter Gun Laws Linked to Lower Risk of Gun Violence to Children.

According to a recent study that appeared in the September 2019 issue of the journal *Pediatrics*, children who live in states with stricter gun laws are less likely to die from gun violence.

The survey noted that states with strict gun control laws had four percent fewer pediatric deaths, and states with universal background checks for firearm purchases in place for at least five years had a 35 percent lower risk.

According to researchers quoted in the study, stricter gun laws have been shown to lower overall death rates in adults, as states with more laws have fewer homicides and suicides than those with fewer. A range of laws, including waiting periods to get firearms, universal background checks, restrictions on carrying guns in public and mandated gun locks have all been linked to lower suicide rates, according to statements made in the study.

"Firearm-related injuries are the second-leading cause of pediatric death in the U.S., yet there is significant variation in firearm legislation at the state level," said Monika Goyal, director of research in emergency medicine at Children's National in Washington. "In our study, we found that states with stricter firearm legislation, specifically legislation requiring universal background checks for firearm purchase, had lower firearm-related mortality rates in children." The National Rifle Association has disputed the methodology and conclusions of the study.

This Just In

professionals to misconduct-free individuals with similar ages, genders and experiences and controlling for a wide range of executive and cultural variables, the researchers found that people with histories of misconduct were significantly more likely to use the Ashley Madison website.

"This is the first study that's been able to look at whether there is a correlation between personal infidelity and professional conduct," said Samuel Kruger, a faculty member at the University of Texas who co-authored the report. "We find a strong correlation, which tells us that infidelity is informative about expected professional conduct."

The report goes on to make a strong connection between people's actions in their personal and professional lives and suggests that eliminating workplace sexual misconduct may also reduce fraudulent activity.

Remote Workers Pose Huge Cyber Liability Threat

There are benefits to working from home, but also risks to both employees and employers.

Working from home among non-self-employed people has grown by 140 percent since 2005 — ten times faster than growth of the workforce itself. There are plenty of benefits to both workers and employers when employees get online to work remotely. But there are also plenty of risks.

Especially when the gateways used to connect to company platforms are acquired via Wi-Fi in coffee shops and airport terminals.

83 percent of business owners give employees the option to work securely from remote locations when needed and appropriate, according to Nationwide Insurance's fifth annual Business Owner Survey. Among young business owners (ages 18-34), this number jumps up to 95 percent.

The potential damage from cyber threats requires businesses to be ever vigilant in implementing and constantly updating a comprehensive cyber security program. However, according to the Nationwide survey, only 50 percent of small business owners have updated their remote work security policy in the past year.

"What may seem like a harmless public Wi-Fi network could ultimately pose serious troubles for a business," says Catherine Rudow, vice president of cyber insurance at Nationwide. "Many employees may not realize the magnitude of risk associated with a cyberattack as they may not have engaged in a formal training process. The scary truth is that many small business owners, even if they are aware of these risks, have not implemented all the proper measures of protection."

Remote employees place businesses at risk, yet many small business owners are not properly mitigating potential cyberthreats, nor are they adequately protecting their employee platforms, says the Nationwide report. Failing to continually revise remote work policies in the growing digital workplace could put those business owners at higher risk of a cyber-attack.

The survey found that one in five small business owners have not committed their employees to formal cybersecurity training.

continued on next page

According to the survey:

- 65 percent of business owners admit they have been victim of a cyberattack; computer virus attacks are the top type of attack reported at 33 percent, phishing is number two at 29 percent.
- 86 percent of business owners believe that digital risk will continue to grow.
- 30 percent of companies with 11-50 employees do not provide any type of formal training on cybersecurity.
- Despite the simplicity of regularly updating software, seven percent of companies still fail to take that step.
- Reputational risk is among the top reasons (45 percent) why business owners would consider investing in or purchasing a cybersecurity policy.
- 35 percent of business owners who have never experienced a cyberattack are unaware of the financial cost to recover, highlighting a dangerous gap in knowledge from the implications.
- Only four percent of business owners have implemented all of the cybersecurity best practices and recommendations from the U.S. Small Business Administration.

How to Understand an Insurance Policy

Most people would rather go to the dentist than try to read an insurance policy. Like most things that seem intimidating at first, though, when you break it down, it makes a lot more sense.

There are four basic parts to every insurance policy:

- Declarations
- Insuring agreement
- Exclusions
- Conditions

Declarations: The declarations introduce your coverage. They identify the insurer, the insured and policy number. They also identify the properties or risks the policy covers, and for how long (the policy period). They outline the financial considerations of the contract, including premiums you will pay, limits and deductibles.

Here are some of the things you can find out about your coverage in the Declarations section. Check and make sure they are accurate:

- Check that the name of the insured matches the entity's legal name, spelled correctly.
- Check that the policy lists the addresses of all the business premises you want to cover (for a business property policy).
- For an auto policy, verify information on make, model and VIN numbers for covered vehicles.
- For a liability policy, verify the declarations accurately describe the type of coverage you want.
- Check the policy start (inception) and termination dates. This is your coverage period. If you are replacing an existing policy, will this create any coverage gaps? Some claims-made liability policies provide coverage for accidents that occur before the current policy term, the retroactive period. Check the retroactive date — the date on a renewal claims-made liability policy should match the date on your first policy, otherwise you will have a coverage gap.
- Policy limits are the most the insurer will pay under the policy. Some policies also have separate, lower sublimits for specific types of claims. Will these limits provide enough coverage?
- The declarations page will also list the premiums you pay, along with any deductibles you will have to pay before the insurer begins to pay on a claim. To lower your premiums, can you afford higher deductibles?
- Some policies include separate schedules, or itemized lists of covered property. They might also include endorsements, which are separate documents that modify terms of coverage under a policy. The declarations should list these — check that they are correct.

Insuring agreement: This section summarizes the insurer's agreement to pay covered claims. For a property policy, it will state the

continued on next page

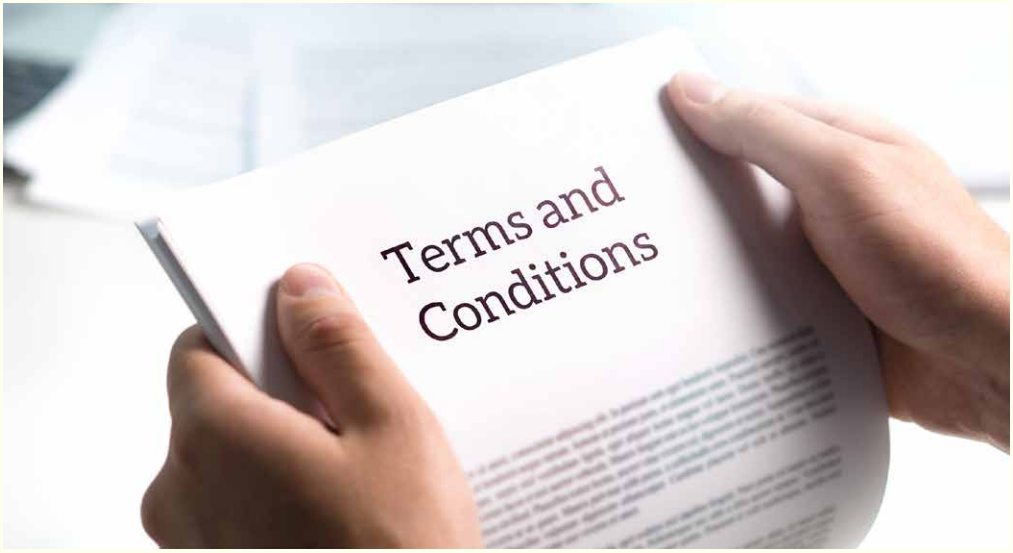
property covered and types of perils, or causes of loss, the policy covers. In a liability policy, the insuring agreement describes the types of activities covered. For a commercial general liability policy, the insurer agrees to any money the insured is legally obligated to pay for bodily injury or property damage claims covered by the policy. The insurer also agrees to provide the insured's legal defense for liability claims that might be covered by the policy.

Action item: For a property policy, determine whether you have a "named perils" or "all-risk" policy. A named perils policy will list the specific perils that the policy covers. Any peril not named is not covered. The so-called "all-risk" policy offers broader coverage, covering losses caused by any peril, except for those specifically excluded in the policy. If you have a named perils policy, do you have any significant risk exposures that are not covered?

Exclusions: Exclusions limit your coverage by stating the types of activities or losses the policy will not cover.

Action item: To avoid significant coverage gaps, list the exclusions included in all your liability policies. Most general liability policies exclude liability for pollution and design error, among other things. If you need coverage for these exposures, you will need to buy separate, specialized insurance.

Most businesses have a second layer of liability protection through an umbrella or excess policy. This pays claims that exceed the limits of the primary liability policies. Often an umbrella policy will provide broader coverage (that is, cover more perils) than your primary policies. If not, and you have significant risk exposures excluded in your primary policies, please contact us so we can tailor a coverage solution for you.



Conditions: The conditions describe the obligations of each party to the contract. Conditions can appear in the basic policy, the standard form and (if you have them) in your policy endorsements.

Conditions include the policy's cancellation provision. They also describe how the insurer will proceed if other coverage applies to a loss, and reserve the insurer's right to subrogate a claim, or seek recovery from another party after it has paid a claim on your behalf.

The conditions also outline your obligations to the insurer. They spell out when and how you must notify the insurer of an accident or claim that might be covered by a liability policy, your obligation to protect covered property after a loss, and your obligation to cooperate during the company's investigation or defense of a liability lawsuit.

Action items: Read policy conditions carefully, because failure to fulfill your obligations to the insurer could nullify your coverage!

To ensure you have time to find other coverage, look for a cancellation provision that requires the insurer to provide at least 30 days' notice before cancelling your policy for reasons other than non-payment. For difficult to place coverage, you may want as many as 90 days' notice.

If you need help reviewing a policy or understanding policy provisions, please contact us.

10 Tips for Reducing Cyber Liability Threats

1. Protect against viruses, spyware, and other malicious code. Make sure all computers are equipped with antivirus software and anti-spyware and updated regularly.
2. Secure your networks: Safeguard your Internet connection by using a firewall and encrypting information. Make sure your Wi-Fi network is secure and hidden.
3. Establish security practices and policies to protect sensitive information: Establish policies on how employees should handle and protect personally identifiable information and other sensitive data.
4. Educate employees about cyberthreats and hold them accountable : Deter employees from introducing competitors to sensitive details about your firm's internal business by informing them about how to post online in a way that does not reveal any trade secrets to the public or competing businesses.
5. Require employees to use strong passwords and to change them often: Consider implementing multifactor authentication that requires additional information beyond a password to gain entry.
6. Employ best practices on payment cards: Work with your banks or card processors to ensure the most trusted and validated tools and anti-fraud services are being used. Do not use the same computer to process payments and surf the Internet.
7. Make backup copies of important business data and information: Regularly backup critical data on all computers and store in the cloud or offsite.

8. Control physical access to computers and network components: Prevent access or use of business computers by unauthorized individuals. Make sure a separate user account is created for each employee and require strong passwords.
9. 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
10. Protect all pages on your public-facing websites, not just the checkout and sign-up pages.

Source U.S. Small Business Administration (for the complete description, see https://www.sba.gov/managing-business/cybersecurity/top-ten-cybersecurity-tips) As an additional precaution, you may also want to consider cyber liability insurance. ■

Insurance Buyers' News