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 | September/October 2017 | Volume 28 • Number 5

Next Cyberattack Could Cost as Much as Superstorm Sandy

A major cyber attach could cost billions of dollars and, unlike extreme weather, comes without warning.

The total cost of a worldwide cyberattack could be as high as $53 billion, according to a report issued by Lloyd's of London in July 2017. That's almost as much as the cost of Superstorm Sandy ($50-$70 billion), the second costliest disaster in U.S. history. But worldwide cyberattacks aren't the only risk for small businesses. 43 percent of cyberattacks target small businesses, according to Small Business Trends.

Cyber-attacks can come from

continued on next page

This Just In

A strength test used by CSX Transportation to evaluate arm strength and endurance for applicants of certain jobs violates Title VII of the Civil Rights Act of 1964 because it discriminates against women, according to a lawsuit filed by the U.S. Equal Employment Opportunity Commission.

Scores for the test determine whether a person who passes belongs to the "heavy" or "medium heavy" group. The passing rate in the "heavy" group has been 87 percent men and 30 percent women. In the "Medium heavy" group it has been 94 percent men and 47 percent women.

In the complaint, the EEOC alleges the test is unfair because it is not related to the job appli-

continued on next page

anywhere: nation states, terrorists, criminals, activists, external opportunists and company insiders (both intentional and unintentional). Their motivation may be to gain political, military or economic advantage. Where businesses are concerned, though, they steal money or data they can turn into money, such as credit card numbers, health records, personal identification information and tax returns — or they set up a ransom situation that locks the company's access to its data until the ransom is paid.

The National Association of Insurance Commissioners (NAIC) has identified the main cyber risks as:

- Identity theft as a result of security breaches where sensitive information is stolen by a hacker or inadvertently disclosed, including such data as Social Security numbers, credit card numbers, employee identification numbers, drivers' license numbers, birth dates and PIN numbers.
- Business interruption from a hacker shutting down a network.
- Damage to the firm's reputation.
- Costs associated with damage to data records caused by a hacker.
- Theft of valuable digital assets, including customer lists, business trade secrets and other similar electronic business assets.
- Introduction of malware, worms and other malicious computer code.
- Human error leading to inadvertent disclosure of sensitive information, such as an email from an employee to unintended recipients containing sensitive business information or personal identifying information.
- The cost of credit monitoring services for people impacted by a security breach.
- Lawsuits alleging trademark or copyright infringement.

Cyber Risk Management

The primary defense against cyber security loss is a well-designed and conscientiously maintained risk management program. The first step in such a program is to identify the firm's vulnerabilities, including systems, procedures, programming and personnel. The next step is to control those vulnerabilities as much as possible. Here is a short, practical checklist:

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 Personally Identifiable Information (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.

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. You can get more good advice here: https://staysafeonline.org/business-safe-online/implement-a-cybersecurity-plan.

This Just In

cant's ability to do the job or if related to the job, it measures capability disproportionately.

"Companies must refrain from using a test causing adverse impact unless it is job-related and consistent with business necessity. Even if a test passes that standard, an employer must adopt any comparably effective alternative practices that have less adverse impact," said Philadelphia-based EEOC District Director Spencer H. Lewis Jr. in a statement.

continued on next page

Cyber Liability Insurance Policies

Even with a cyber security plan in place, your business still needs a fail-safe to protect it against cyber risk.

Currently most standard commercial lines policies do not provide insurance for cyber risks. You need a special cyber liability policy. Due to the lack of actuarial data, however, it's difficult to price. Insurers deal with this by evaluating each risk according its risk management procedures and risk culture. As a result, cyber risk coverages are more customized and, therefore, more costly.

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 NAIC:

- 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.
- Coverage for expenses related to regulatory compliance for billing errors, physician self-referral proceedings and Emergency Medical Treatment and Active Labor Act proceedings.

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

Is Distracted Driving Driving Up Your Auto Insurance Costs?

At least 17% of all highway crashes are the result of distracted driving, according to the National Highway Traffic Safety Administration.

That translates to approximately $148 billion a year — $47 billion in in physical damage plus $101 billion in "societal harm," such as traffic congestion and lost productivity,

Distracted driving can be visual — taking your eyes off the road; manual — taking your hands off the wheel; and cognitive — taking your mind off driving. Using the car's navigation system or talking with passengers or eating while driving are forms of distracted driving. But the most common and lethal form of distracted driving involves using hand-held devices while driving, namely using a cellphone.

Texting behind the wheel is illegal in 47 states and the District of Columbia and 14 states make using hand-held cellphones illegal.

Most people are aware of the hazards and illegality of using cellphones while driving, but laws, common sense and company policies often have little impact. "More training is probably one of the worst solutions for this problem," said Michael Davis Sr. VP and risk control leader for Lockton Companies, Houston, in an interview with *Business Insurance*.

"It's an easy thing to adopt (for companies) because (they)

continued on next page

can say, 'Hey, we sent out a memo,'" says Davis

He thinks technology offers the best solutions for reducing distracted driving. There are a growing number of firms starting to work on ways to keep people from using their cellphones, especially people who drive as part of the job.

Cell phone blocking: Blocking apps can be downloaded and activated to the cellphone or installed in vehicles as a "geofence" or virtual barrier around drivers, preventing them from sending or receiving transmissions. Many providers permit certain white-listed incoming phone numbers and will allow the driver to make an outgoing call in an emergency.

On board cameras or car "black boxes": Some units, called dash cams, record drivers ("cabin view") as well as the front view of the road ahead and can be useful in a variety of ways. The recorded video can be used to monitor driving habits, including ensuring that drivers refrain from cellphone use, as well as providing evidence in the event of a traffic accident.

Eye-tracking software: Car safety experts are studying how to mitigate driving without awareness (DWA). Tobii Pro, an eye-tracking technology company headquartered in Stockholm, defines DWA as "the sense of operating a vehicle with little or no conscious attention to the surrounding traffic, also known as subconscious driving."

Car manufacturer Audi and others have been working with the technology to study driver awareness by tracking their eye movements. With results from these studies, they hope to develop systems to provide feedback to drivers to help them maintain and improve their conscious attention to surrounding traffic.

Banned Cellphones and Productivity Concerns

The biggest obstacle to preventing distracted driving is often inertia on the part of companies. They either don't want to spend the money on funding technological solutions or they may be worried that doing more than paying lip service to banning cellphones would reduce productivity. A typical sales force may spend a bulk of their time on the phone, talking to customers, calling prospects, etc. while driving between appointments.

Yet, in a 2010 survey by the National Safety Council of Fortune 500 firms, only 7 percent of companies with cell phone bans in place reported productivity declines, while 19 percent thought productivity had increased.

David Teater, president and founder of FocusDriven LLC, and the father of a boy who was killed in a distracted driver accident, thinks productivity loss is a red herring.

"Being a former CEO myself and having probably spoken to hundreds of CEOs over the years and hundreds of companies that have put these policies in place, maybe thousands, I've never heard of, not only not heard directly, I've never even heard of a company saying 'we put this policy in place, and it hurt sales commissions; it hurt productivity; it hurt customer service; not even one comment on that anecdotally in the last 10 years, which I think is amazing," Teater told CNN.

Of course, in the long run, driverless cars could start making these concerns irrelevant. For help mitigating the problem of distracted driving in your company, please contact us.

Why Almost Every Business Needs Additional Insured Coverage

You have business liability insurance, but it may not provide coverage if you are considered "vicariously liable."

Do you work with outside contractors or partner with other businesses on ventures? What if they cause injury or property damage to others while doing work for you or representing your interests?

Additional insured coverage can protect your organization from liability due to contractors' and subcontractors' operations.

Liability insurance covers you from losses due to claims that your company, its employees or products or

Black's Law Dictionary **defines "vicarious liability" as: The imposition of liability on one person for the actionable conduct of another, based solely upon a relationship between two persons.**

continued on next page

services caused harm or wrong to a third party. Sometimes, however, your organization can be considered "vicariously liable" when another business, such as a subcontractor, causes harm when doing work on your behalf. In these cases, you would want the contractor or other business' policy to apply rather than yours.

There are two ways to obtain coverage under another entity's policy. In the first, "contractual indemnity," your contract with the other party requires it to "indemnify," or cover you for any liability costs resulting from your joint operations. Alternatively, you can also require the other party to name your firm as an additional insured under its insurance policy.

Obtaining additional insured status often provides greater protection than contractual indemnity. Some states and courts look unfavorably on contractual indemnity, because subcontractors who want business sometimes have little bargaining power. Additional insured coverage, on the other hand, causes no such problems.

For your contractor to provide you with "additional insured" coverage, it must obtain an additional insured endorsement, which modifies its general liability policy. Unlike the policy owner (or "named insured"), the additional insured has no responsibility for keeping any records needed for determining premiums, paying premiums or reporting claims.

When you require additional insured coverage under another organization's policy, you'll probably ask for a certificate of insurance to provide proof of coverage. Be aware

that the certificate provides proof that the coverage existed on the date the certificate was issued. The named insured can cancel coverage without providing notice to you. You can request the insurer to provide you thirty days' notice of cancellation or nonrenewal of the endorsement. However, the certificate is not part of the policy and not binding on the insurer. In the case of large or high-risk projects, you can request the contractor to modify its policy with an endorsement that obliges the insurer to provide this notice.

Considerations for Subcontractors

If the shoe is on the other foot and you are a subcontractor, obtaining additional insured endorsements for contractors and providing the required certificates can be an administrative hassle. To solve this problem, you can buy a blanket additional insured endorsement. This provides additional insured coverage to any party with which you enter a contractual agreement (typically a construction contract or equipment rental contract).

Blanket additional insured endorsements are not as desirable for the additional insured. Blanket endorsements do not name specific additional insureds, so the insurer cannot provide notice of cancellation or nonrenewal. They usually provide narrower coverage as well — for example, many of these endorsements state that coverage ends when operations are completed. This could be construed to eliminate coverage for claims that occur during operations but aren't filed until later.

For more information on covering additional insureds, please contact us.

more on next page

What Is Subrogation and How Does It Apply to Insurance?

Subrogation in the context of insurance is the right of an insurance company to "step into the shoes" of the insured after the company has paid the loss. Subrogation entitles the insurance company to assert any rights on its own behalf that the insured may have had to recover payment from the parties that caused the loss.

The topic of subrogation is loaded with nuance and there are too many fine points to cover here. But these short explanations of how subrogation works in various types of insurance policies should be helpful.

- In auto insurance, for example, if you have collision coverage, your insurer will pay to repair your car regardless of whether you were at fault. If you were not at fault, though, your insurer would subrogate against the party who hit your car for the damages it paid out.
- In workers' compensation, if a worker is injured operating a piece of machinery that malfunctions, the worker would be compensated for his injuries according the workers compensation laws of the state. But the insurance company that paid out the workers compensation would be subrogated to the worker's right to sue the manufacturer of the malfunctioning equipment and recover its payments.
- One of the most common appearances of subrogation is in property leases, which typically include mutual waivers of subrogation. In these clauses the landlord and tenant each agree to waive any rights of subrogation they may have against each other in the event a loss. Most insurance policies permit waivers of subrogation as long as the waiver has been agreed to before any loss occurs.

Insurance Buyers' News