—Reprinted with permission from PIA Management Services Inc.—

MATT MASIELLO, AAI
Chief executive officer, SIAA and
President and chief executive officer, SAN Group

Cyberattacks

What every agency and small-business owner should know

I continue to beat the drum on this topic for two reasons: The cost of cyberattacks is increasing and the frequency with which they occur continues to increase as well. In other words, the potential harm to an independent insurance agency from a cyberattack or data breach could easily be catastrophic.

According to a recent *Harvard Business Review* article, "Cybercrime alone costs nations more than $1 trillion globally, far more than the record $300 billion of damage due to natural disasters in 2017." The article ranked cyberattacks as "the biggest threat facing the business world today—ahead of terrorism, asset bubbles and other risks."[1]

Although many who read about high-profile incidents think they are somehow immune from an attack—they aren't. In fact, their chances of falling victim to cyberattacks are growing, according to a July 2018 report from the Ponemon Institute LLC, sponsored by IBM. In the report, researchers found that the average global probability of a material breach in the next 24 months is 27.9 percent.[2]

The cost of a cyberattack

While you still may be thinking, "that only happens to big businesses," think again. Insurance agencies and their small-business clients certainly are susceptible to cyberattacks. In fact, the 2018 Data Breach Investigations Report, published by Verizon, found that more than half (58 percent) of cyberbreaches impacted small businesses. The financial and insurance industry accounted for 598 incidents alone in 2018, and 146 of those incidents involved a confirmed data disclosure.[3]

Now, consider the costs. Ponemon found that:

- The average total cost of a data breach in the U.S. was $7.91 million, the highest in the world.
- Companies worldwide that contained a breach within 30 days saved $1 million, but in the U.S., the mean time to contain a breach was 52 days.
- The average cost per record breached in the U.S. was $233, again the highest worldwide. So, an insurance agency with 2,000 records breached could spend nearly $466,000 in unbudgeted expenses.

Lastly, consider that approximately half of small businesses that have a cyberattack go out of business within six months.[4]

Cybercriminals use multiple tactics to commit wrongdoing. While the Verizon report estimates that nearly half of all 2018 attacks occurred through hacking, other common tactics include malware; errors such as causal events; social attacks (e.g., phishing scams); privilege misuse; or physical actions.

Reduce your cyberrisk

Professional insurance agents are business owners, and as such, should know how to reduce their own cyberrisk. Here are some suggestions:

Insure against cyberattacks. Look for a policy that provides coverage against cyberextortion and offers proper limits to cover the myriad of post-breach response expenses, including legal fees, notification costs and reputational repair.

According to RPS Executive Lines Producer Adam Connor, "a cyberpolicy is closest to a kidnap and ransom policy—the business has to immediately report the problem. Most speak with a lawyer, engage a cyberpolicies team including a breach response coach and IT firm, provide credit monitoring, and perhaps hire a public relations firm to mitigate any outside exposure." While Connor says the average policy cost is roughly $2,900 annually, the cost of a standard Personally Identifiable Information attack without any coverage can reach over $232,000 and will grow significantly higher if the company is caught up in a lawsuit as a result of the breach. Just tallying the cost of a forensics investigation, security remediation and a breach coach to give legal advice can total close to $170,000. Full disclosure: RPS is a strategic partner of SIAA and writes many cyberpolicies for and with SIAA member agencies.

Train employees to be proactive. More than one-quarter (28 percent) of last year's cyberattacks involved internal actors, according to the Verizon report. That is why independent insurance agents and their employees must know how to prevent cyberattacks and how to identify them.

Start by implementing some cybersecurity best practices, including updating your software; implementing complex passwords (and changing them monthly); using data encryption; and securing your Wi-Fi network. (Get additional tips from the U.S. Department of Homeland Security's Ready.gov website.)

Next, fortify the frontlines of cybersecurity: your email inbox. When an employee opens an attachment containing malware, it can compromise your system. And today's cybercriminals are increasingly clever when it comes to disguising malicious emails. That's why email tricks, such as phishing and pretexting, account for nearly all social cyberattacks, according to the Verizon report. Teach your employees to separate the phony from the authentic.

With the expansion of automation, denial of distribution or denial of services is common. In fact, Connor commented, "Everything has an IP address. These cyberattacks turn mundane devices, such as light bulbs or smart refrigerators, into bots that can send information to a specific network to overload and shut down a company. There is so much out there that makes a company vulnerable."

He also said agents need to be aware of trends and new exposures, such as the routine task of using thumb drives. "Don't put random thumb drives in your computer. Someone could drop a thumb drive in your office called 'vacation pictures'—and if you open it, you could download malicious code. It's about employee awareness, training, making others aware of what is out there and what is occurring. This is a fluid task, and what you do today may not include security measures you need to be taking tomorrow."

Appoint a cyber incident lead and test your response plan. All businesses should appoint an incident lead who can identify a cyberattack among the staff. With human resources, the incident lead can train staff and distribute communications to educate everyone on how to identify a cyberattack and the critical importance of reporting anything suspicious immediately.

Once an attack occurs, the incident lead must identify the type of attack; determine its severity; learn which information was accessed; compile an insurance report; and notify law enforcement as needed. He or she also should disable compromised accounts; compile all IP addresses involved; insist that all users change their passwords; and notify people who must access the compromised accounts. To start this process, contact your insurance company's breach response coach immediately.

Your incident lead should have a cyberbreach response plan in place and test it. If there is a breach, the person will know what takes priority and to whom to reach out to immediately. If an organization buys a cyber insurance policy, but never test the process on reporting a compromised event, it won't understand the

critical steps to take. This may be detrimental to the business or the ability of the insurer to contain the breach quickly.

Understand how and what data is being protected. According to a recent article by the technology company, Ciena, there are three pillars to protect your data: confidentiality; integrity; and availability.[5]

RPS's Connor agrees with this philosophy for data protection, with caution. "Don't make it so difficult to get through your computer that staff can't get to the documents they need," he said. "The bottom line is that not all information is created equal. For example, a patient record is much more important than a brochure on the latest medicine. By being more aware of what needs encryption and what doesn't, you could save your small business money."

Segregating just the important data and letting other files be accessible will drive down IT costs, which will enable small businesses to afford cyberinsurance.

Information valuable to attack

Some companies use data breach cost calculators to help small businesses to estimate costs of recovery from a cyberbreach. While data breach estimates are based on a limited claim history, as cyberattacks are relatively new, potential clients can at least understand the numerous areas of exposure that go into having a breach, the costs associated with each step of the process and how many steps are involved in recovering from a data breach.

There are four categories of information a cyberbreach can expose:

1. **Personally identifiable information.** This is information such as: mother's maiden name, Social Security number or birth date.
2. **Protected health-care information.** These are items protected by the Health Insurance Portability and Accountability Act of 1996. On the dark web, this data is being sold at four to six times the cost of PII information. Criminals can create credit cards on a person with PHI, and it's easier to create fraud accounts or uncover a person's insurance information with this.
3. **Payment card industry.** Most often, criminals try to get information to sell on the dark web. For instance, if they steal all of your clients' credit card numbers, they can resell the numbers immediately (before the credit card holder can cancel the stolen card).
4. **Cyberextortion.** This is when a criminal gets secure data from a network and tells the company it must pay to get the data back. Connor commented, "It's alarming how many companies pay ransoms to get their network back, rather than calling the police. How do they know the criminals aren't still skimming information off the returned network?"

Cyber criminals are casting a wider net with cyberattacks than ever before, so make sure your agency is insured; all of your employees are trained; and you are prepared for the very worst. Then make sure your small-business clients are doing the same.

Masiello is responsible for providing strategic leadership for SIAA and its related companies by working with the executive management team to establish long-range goals, strategies, plans and policies. To learn more about Masiello, visit siaa.net.

[1] Harvard Business Review, 2018 (bit.ly/2x7Ura8)

[2] Ponemon Institute, 2018 (ibm.co/2JWy0bF)

[3] Verizon, 2018 (vz.to/2USiMeb)

[4] U.S. Securities and Exchange Commission, 2015 (bit.ly/2enj0dc)

[5] Ciena, 2018 (bit.ly/2EAw0r5)