JEFF HOLMES
Senior vice president and COO, SIAA

Cybersecurity is critical to business continuity

Business owners continue to struggle to grasp how cybersecurity—when paired with cyber security insurance—is vital to protecting their business continuity. Many small- and medium-sized enterprises continue to do nothing to protect themselves from a cyberattack, and most do not have standalone cyber insurance policies.

This lack of action poses a real risk to these businesses. Consider that 60% of small businesses fold within six months of a cyberattack, according to *Inc. Magazine*,[1] which stated: "The best defense is a good offense. Make it a priority to protect your data for the benefit of your employees, your customers and the long-term health of your business."

Business owners need to understand the critical nature of security and insurance for their own business continuity. Concerns are only growing, as states implement new laws to protect consumers' data.

This article will identify why cyber security protection is vital; why it is required for independent agents; and why businesses need to understand what can or will be impacted if they don't take cyber security vulnerability seriously.

Have a plan

No one wants their customer or company data breached, but if a business operates with technology, accepts payments online, and stores confidential data, it needs protection from top to bottom. That's why insurance carriers insist independent agents have cyber security coverage for themselves and their third-party vendors: It reduces liability all around. It also brings them into compliance with the October 2017 law enforced by the National Association of Insurance Commissioners. The NAIC's Insurance Data Security Model Law created rules for insurers, agents and other licensed entities covering data security, investigation and notification of breach. Obviously, independent agents need a cybersecurity and cyber insurance policy in place, and buying it for their own agencies helps them to become conversant about its necessity in general.

But, are independent agents asking their vendors if they are cyber-secure and have cyber security coverage? Is every one of the vendors compliant and meeting the rules and regulations for the carriers with which they work? No business—large or small—is immune to cyberattacks. Even if a business does have cyber security measures in place and has invested in a cyber insurance policy, it may be impacted by a third-party vendor being attacked, and a criminal gaining entry to one of its channels remotely.

Rather than targeting one company, cybercriminals often target vendors that work with many organizations (e.g., cloud services, email servers and payment platforms) in an effort to steal data from several companies. Businesses need to understand who their third-party vendors are and how much information is shared with each of them. This includes knowing what data and networks they're able to access and determining if they need the level of access they have.

You need to consider state and federal compliance requirements. Right now, it costs less to comply with cyber security regulations than it does not to be in compliance. A report by the Ponemon Institute and GlobalScape[2] found that noncompliance costs 2.71 times more than the cost of maintaining or meeting compliance requirements. The noncompliance costs come from the expenses associated with business disruption, productivity losses, fines, penalties, and settlement costs, among others.

Europe has implemented an extensive data protection law, which affects business owners working with cyberdata (General Data Protection Regulation) and any business with European clients. Currently, many U.S. states are adopting their own compliance regulations (e.g., Connecticut, New Hampshire and New York). California passed a plan

(California Consumer Privacy Act), which is the strictest data protection law in the U.S. The law took effect in January, and it is expected to compel companies that already buy cyber security insurance to reach out to their brokers to ensure their policies are compliant. This law applies not only to company data, but also to data kept by vendors and third-party groups.

Each state is working on these types of data privacy laws, which will affect small businesses and require greater cyber security, compliance and cyber insurance policies. According to NCSL.org, 31 states enacted cyber security-related legislation in 2019.

Are small businesses ready?

An estimated 43% of cyberattacks target small businesses, according to the Verizon 2019 Data Breach Investigations Report.[3] According to the 2018 Hiscox Small Business Cyber Risk Report,[4] only 16% of small businesses are very confident in their cybersecurity readiness. Areas in which businesses fall short are:

- **Willingness to respond.** Remarkably, 65% of small businesses have failed to act following a cyber security incident.
- **Training.** Less than one-third (32%) of small businesses have conducted phishing experiments to assess employee behavior and readiness in the event of an attack.
- **Insurance.** Less than a quarter (21%) of small businesses have a standalone cyber insurance policy, compared to more than half (58%) of large companies.

Best practices

These cyber security best practices should increase the security of all small businesses:

No. 1: Prevention. Involve and educate all levels of the organization about cyberthreats. Have a formal budgeting process and ensure cyber is a part of all decision-making. Implement cyber security training during the on-boarding process and in an ongoing manner.

No. 2: Detection. Include intrusion detection and ongoing monitoring on all critical networks. Track violations (both successful and thwarted) and generate alerts using both automated monitoring and a manual log. Record all incident response efforts and all relevant events.

No. 3: Mitigation. Create a plan for all incidents, from detection and containment to notification and assessment, with specific roles and responsibilities defined. Review response plans regularly for emerging threats and new best practices. Insure against financial risks with a standalone cyber insurance policy or endorsement.

Forty-eight percent of data breaches occur because of the negligence of employees or contractors.[5] Broaden awareness across your organization today. Individuals should know better than to share personally identifiable information with just anyone, so make sure everyone on your staff uses the same caution at work. It may seem obvious, but it's best to state in writing that all company data, sensitive information, or intellectual property is not to be shared. Create and implement a business policy that defines why cyber risk prevention is critical to your business, sets guidelines for prevention of cyberattacks, and identifies a lead person in charge of cyber risk issues in the event of suspicious activity or a cyberattack.

Make training mandatory for all staff so that everyone understands what cyberrisk is and what common attacks look like. Teach staff about phishing and malware, and the many ways these attacks can occur. Discuss different tactics cybercriminals use regularly, like creating fake emails and websites that look legitimate to make an employee more vulnerable. Quiz your staff on what they have learned after training so it is clear that cyber risk prevention is everyone's responsibility (it also will help evaluate its effectiveness).

Every staff member must be diligent to prevent cyberattacks. Execute a strategy for the entire business and assign responsibilities to prevent, detect, and mitigate immediately so that each staff member is proactive about prevention, detection and mitigation.

A growing market

On the upside, there is a growing cyber insurance market in commercial lines for independent agents, especially those who are educated on the risks associated with technology and systems, cyber security strategies and coverages available. *[EDITOR'S NOTE: PIA members can call the association to discuss cyber security policies that are available to them through PIA.]* Agents who help their clients to remove the mystery behind cyber—and provide simple solutions to move clients toward better security and cyber security insurance—

can improve their income and build a niche.

Clearly, cybersecurity must be prioritized with the urgency it deserves and within the limitations of a business's budget—and independent agents should be able to educate their small-business clients on how to purchase the best cyber security insurance, while meeting the list of state-specific compliance regulations and requirements. They need to be aware of the compliance requirements of each of their carriers and brokerage contracts due to their status as an affiliate of the carrier or brokerage as well.

With so many people working remotely because of COVID-19, and as small businesses everywhere make sure they are taking all necessary steps to protect their critical information and their clients' data, independent agents can proactively advise clients to implement these security measures, coupled with cyber security policies and standalone cyber insurance policies to ensure the safety of their businesses long-term.

Holmes is the senior vice president and chief operating officer of SIAA (Strategic Insurance Agency Alliance). Reach him at jeffh@siaa.net.

[1] Inc. Magazine, *2018 (bit.ly/34fItZF)*

[2] *Ponemon Institute and Globalscape, 2017 (bit.ly/38B4khL)*

[3] *Verizon, 2019 (vz.to/2PjGfnT)*

[4] *Hiscox, 2018 (bit.ly/36y8kh7)*

[5] Small Business Trends, 2019 (bit.ly/2thxsdN)