Cyber Crime: A Silent Killer for Main Street America?

In years prior to the internet age, poor business planning, outdated product offerings, or lack of innovation were at the root of small business failure. Today, the reality for small to medium-sized businesses is that cyber crime may be the Achilles heel in their otherwise successful venture since a large percentage of attacks are not front-page news. As agents and brokers know, many business owners insist that they will not be the target for cyber crime and repeatedly resist purchasing even basic cyber insurance that could protect, and ultimately save, their business.

The past year has been one tarnished by continual cyber crime and major data losses inflicted upon global corporations. Early 2017 produced massive ransomware attacks in the form of the Trojan horse viruses and system worms that affected hundreds of thousands of computers. These attacks accompanied unprecedented data breaches, with millions of customers facing some form of sensitive data stolen.

According to the Ponemon Institute's "2017 State of Cyber Security in Small & Medium-Sized Businesses (SMB)" report, as of September 2017:

- Over 60% experienced a cyberattack in the last 12 months
- Only 38% regularly implement security patch
- Only 22% encrypt sensitive customer and employee data
- Only 25% of business had adequate cyber coverage in place

Costs related to cybercrime and remediation lead to 60% of businesses in this market sector going out of business within 6 months of a cyberattack.[1]

The category of business known as "Main Street America" is comprised of roughly 28 million small to medium sized companies with approximately 100 to 1,000 employees.[1] These smaller, typically privately owned businesses often characterize our communities and serve as neighborhood fixtures. These businesses, such as local food markets, restaurants, hardware stores and retail shops, serve as long-term employers to their towns and often define the economic foundation of the area. It is for these reasons that the statistics regarding cyberattacks on Main Street America are so concerning.

According to the Ponemon Institute's "2017 State of Cyber Security in Small & Medium-Sized Businesses (SMB)" report, as of September 2017, over 61% of businesses in this class had suffered a cyber -attack within the last 12 months, and over 54% had data breaches involving their employee or customer data.[2] What's more concerning is that these numbers are on the rise from 2016, and are showing no signs of slowing down. Even worse, only 25% of businesses in this category have cyber coverage in place to respond to these exposures.[3]

So why are maleficent hackers targeting Main Street America, and what do brokers and agents need to present to properly help their clients understand their exposures? Despite their relative size, these very businesses are rich with sensitive customer data. The client-facing aspects of small business dealings, such as direct-to-consumer marketing communications, weekly email flyers, and forward-facing customer service departments, make them easy targets for social engineering schemes and phishing attacks. These practices, along with a lack of budget for IT and adequate loss controls, leave customer data vulnerable. Ponemon's report showed that of the 28 million businesses represented in this demographic, 60% of them store their customers' email addresses, 64% store customers' phone numbers, and 54% store customers' billing addresses.[4] With an increased use of web and mobile applications as a means to conduct business in modern society, the numbers relating to data storage are expected to increase over

[1] 2017 State of Cybersecurity in Small & Medium-Sized Businesses (SMB). September 2017. Ponemon Institute LLC
[2] Ponemon Institute LLC
[3] Ponemon Institute LLC
[4] Ponemon Institute LLC

time. However, despite the statistics, only 38% of businesses in this category regularly implement security patches for their software. Even more shocking is that only 31% monitor their credit reports regularly, and a mere 22% encrypt their sensitive customer and employee data.[5]

It is not just ill-intentioned hackers and malicious coders attacking this market segment. As previously noted, over 50% of small to medium sized businesses have experienced data breaches. What may surprise many business owners is that negligent employee or contractor behavior caused 54% of these breaches, with 34% stemming from system and operating process errors.[6] These factors are frequently due to small business owners' failures to implement and facilitate necessary training and privacy policies to their employees. Only 43% of small to medium sized businesses institute a password policy, and of those only 68% strictly enforce them.[7] In many of these circumstances, standard procedures could have prevented the data breach.

No matter how well prepared a company may be, their data is always at risk. Even the United States Senate has taken notice of the increased risks to small and medium sized businesses. In April 2017, Senator Joe Thune of South Dakota introduced a new bill to create resources for small businesses under the "Main Street Cyber Security Act," updating the previously established "Cyber Security Enhancement Act of 2014." Recognizing the impact of this class of business on the U.S. economy, the Senate called upon the Director of the National Institute of Standards and Technology to develop additional resources tailored to this market segment under the prior Act. The resources as outlined in the Act require an overhaul of regulatory reviews, standards of procedures, and the development educational outlets for small business by numerous governmental agencies, including the Department of Commerce. With over 55% of U.S. jobs and 54% of all U.S. sales dependent on small business, the Act portrays the urgency felt by the legislative branch to respond to the growing cyber threat posed to Main Street America.[8]

In addition to cyberattack frequency being on the rise, the cost of remediating cyber incidents has also been increasing at a staggering rate. The aftermath of these incidents has averaged well over $1 million in remediation costs, including an average of $1.2 million in lost business income. It is not surprising that as a result, over 60% of businesses in this market sector go out of business within six months of a cyberattack.[9] Lack of adequate insurance coverage to respond to these incidents leaves many businesses by the wayside, realizing all too late the exposures they have in place.

There is, however, a light at the end of the tunnel. Cyber insurance coverages have been evolving to fit Main Street America companies with options tailored to meet the needs of small to medium sized businesses. Cyber insurance can provide these businesses an outlet to address the damages caused by cyber incidents, including the costs related to forensic investigation, notification requirements, call center services, lost business income, data restoration costs, regulatory fines and penalties, and so much more. As a result of these evolving coverages, Main Street businesses are no longer alone as they try to navigate their way through a cyberattack. Trends in the market have lead reputable carriers to engage "Breach Consultants" for their insureds at the time of a cyber-related incident, as a means to provide guidance to the insured throughout the remediation process.

With vast improvements to cyber insurance policies and the implementation of accessible solutions to cyber related attacks, every business should be considering the purchase of cyber insurance coverage. Agents and brokers need to continue to produce real and meaningful statistics and actual loss scenarios to clearly identify the risks and cost of being uninsured. Evolving technology and the ever-changing landscape of regulatory requirements have put all businesses at risk, with Main Street America being among the most susceptible. Cyber insurance can provide small business owners true peace of mind as they come to realize that the key question is not *if* their business will be a victim, but *when*.

To find out more about Great American's cyber capabilities, contact:

Alan Fiano
Production Underwriter
860-683-4743
afiano@gaig.com

[5] Ponemon Institute LLC
[6] Ponemon Institute LLC
[7] Ponemon Institute LLC
[8] S.770 - MAIN STREET Cybersecurity Act of 2017. 115h Congress (2017-18)
[9] Ponemon Institute LLC