1 in 4 Businesses Has Experienced Cyber Event, Travelers Survey Finds

By Elizabeth Blosfield | October 22, 2020 INSURANCE JOURNAL

Nearly one in four respondents (22%) out of more than 1,200 business leaders surveyed in 2020 Travelers' Cyber Risk Index said their firm was the victim of a cyber event – the highest percentage since the annual survey began in 2014.

Still, only a little more than half of those surveyed said they have purchased a cyber insurance policy.

What's more, many surveyed business leaders admitted to not implementing basic prevention strategies such as cybersecurity awareness training, using virtual private networks (VPNs) with multi-factor authentication, enhancing cybersecurity monitoring and early warning protocols and implementing endpoint detection and response (EDR) solutions.

“Obviously, it’s been a challenging year for individuals and businesses, and the reasons why not as many are implementing proper cyber safeguards might be due to other priorities,” said Tim Francis, vice president of Cyber Risk Management at Travelers Insurance.

“[The insurance industry] needs to continue providing awareness about the cyber threats companies face, make sure they know the potential consequences that come from suffering a cyber event, and offer services that help reduce the chance of becoming a victim.”

It is worth noting that the percentage of survey participants that reported having purchased a cyber policy has steadily climbed over the past few years, with 51% of Travelers survey participants saying they purchased a cyber policy last year, up 39% from the year before.

That said, Francis would like to see that number climb even higher.

“There are multiple reasons companies cite for why they haven’t purchased a cyber policy, and cost is among them,” he said. “We certainly would like the percentage of companies with a cyber policy to increase, because we think it’s a necessity.”

Remote Work

In fact, Travelers’ Index found that cyber threats are a top concern for large and medium-sized businesses, particularly as the ongoing COVID-19 pandemic has forced many businesses to transition quickly to a remote working environment. The percentage of survey participants whose companies have at least 40% of their workforce being remote has more than doubled during the pandemic, from 26% to 59%.

“Employees working remotely are often on routers that are less secure than corporate networks, so when workers return to the office, they’re potentially exposing their companies to greater risk if a corporate device has been compromised,” Francis said.

Given the widespread remote work environment due to the pandemic, Travelers’ Index found that the biggest cyber-related concerns among businesses surveyed include a

security breach, a hacker gaining access to company financial systems or employees putting sensitive information at risk.

While Francis said business email compromise, which occurs when a cyber criminal tricks an employee into transferring company funds to a fraudulent account, has increased over the last several years, the largest cyber incident companies face remains the threat of a ransomware attack.

“The cyber risk landscape is constantly evolving, with sophisticated mechanisms being used to inflict serious cyber damage,” Francis said. “Over the past two years, ransomware has become by far the biggest cyber threat facing companies of all sizes.”

Ransomware is a type of malicious software that is designed to block access to a computer system until a ransom is paid. It has been a top of mind concern among insurers and consumers alike over the past several years, with insurance broker Arthur J. Gallagher & Co. and its claims unit, Gallagher Bassett, recently reporting a ransomware incident that happened on Saturday, September 26, and limited some of its internal systems, Insurance Journal reported.

Ransom Demands

Francis said monetary ransom amount demands are increasing and so is the average length of time it takes for companies and organizations to resume operations after a computer network or system has been taken down.

Underscoring the risks created by pandemic-related work-from-home requirements in particular, ransomware attacks grew by nearly 50 percent in the 2020 second quarter compared to the first three months of the year, a September Coalition report determined.

With this in mind, Francis encouraged those businesses who feel behind on their cyber risk prevention strategies to start by working with an insurance agent or broker, taking a cyber risk assessment that identifies vulnerabilities and creating a mitigation program addressing those gaps.

“There are multiple insurance options, with features and services that insureds can select,” Francis said. “Ask questions and make decisions and choices that best fit the company’s needs.”

Francis added that it’s the job of insurers to continue to monitor the cyber landscape and make sure they’re providing customers with needed products and services.

“Nobody wants to become a cyber victim, and there are specific ways companies can reduce that risk,” he said. “The cyber insurance industry can be a valuable resource in assisting companies [to] deal with cyber risks.”