Insurance Journal's Top 10 Cyber Risk Stories of 2019

By Elizabeth Blosfield | January 7, 2020

Cyber risks were cited as the top concern among businesses of all sizes in 2019, according to a Travelers report released in October.

Of the 1,200 business leaders who participated in an insurer-sponsored survey, 55% said they worry some or a great deal about cyber risks, ahead of medical cost inflation (54%), employee benefit costs (53%), the ability to attract and retain talent (46%) and legal liability (44%).

The Travelers Companies, which has been commissioning the Travelers Risk Index since 2014, said 2019 was the first year in its survey's history that cyber has been the top concern among businesses of all sizes.

As concerns about cyber threats have grown, a higher percentage of businesses reported taking proactive measures to safeguard against cyber risks. The steps taken by respondents included purchasing a cyber insurance policy – 51% of survey participants reported purchasing cyber insurance, up from 39% in 2018.

However, a sizable number of businesses reported they had not implemented such preventive best practices. Tim Francis, enterprise cyber lead at Travelers, said that while more businesses are taking steps to prevent a cyber event, “it’s still alarming that nearly half don’t have the proper insurance coverage.”

Hart Research conducted the national online survey of 1,200 business decision-makers for Travelers from July 8-19, 2019, and a report of the survey’s findings ranked among *Insurance Journal’s* top cyber risk news for 2019.

Check out *Insurance Journal’s* top 10 cyber risk stories for 2019 based on reader metrics below:

1. Iran Increases Cyber Attacks on U.S. Gov’t, Infrastructure: Cyber Security Firms

Readers were interested in an Associated Press report in June that Iran has increased its offensive cyber attacks against the U.S. government and critical infrastructure as tensions have

grown between the two nations, according to cyber-security firms.

Hackers believed to be working for the Iranian government have targeted U.S. government agencies, as well as sectors of the economy, including oil and gas, sending waves of spear-phishing emails, representatives of cyber-security companies CrowdStrike and FireEye, which regularly track such activity, told the AP.

The AP reported that tensions have escalated since the U.S. withdrew from the 2015 nuclear deal with Iran in 2018 and began a policy of “maximum pressure.” The National Security Agency would not address Iranian cyber actions specifically, but said in a statement to The Associated Press on June 21 that “there have been serious issues with malicious Iranian cyber actions in the past.”
“In these times of heightened tensions, it is appropriate for everyone to be alert to signs of Iranian aggression in cyber space and ensure appropriate defenses are in place,” the NSA said.

2. Norsk Hydro Cyber Attack Cost It Nearly $52M in First Quarter

Norsk Hydro said the March cyber attack that paralyzed its computer networks would cost the aluminum maker up to 450 million Norwegian crowns ($52 million) in the first quarter of 2019, Reuters reported in April.

The Oslo-based firm, one of the world's largest producers of the light-weight metal, was forced to halt some production on March 19 and switch other units to manual operation after hackers blocked its systems.

The Norwegian National Security Authority, the state agency in charge of cyber security, said the attack used a virus known as LockerGoga, a relatively new strain of so-called ransomware, which encrypts computer files and demands payment to unlock them, according to the Reuters report.

3. Capital One Breach Clouds Technology Strategy; Puts $400M Cyber Insurance in Play

After a hacker got into the cloud, siphoning off sensitive information for more than 100 million of Capital One's customers, Bloomberg reported in August that the third-largest U.S. credit-card lender was thrust into the center of a massive data breach.

According to U.S. prosecutors, a hacker began tapping into a vast trove of information from Amazon.com Inc. servers the bank was using. The breach has called into question the lender's strategy for reducing technology costs while taking advantage of the cloud's rapid scalability and burgeoning array of applications, Bloomberg reported.

Capital One's shares dropped as much as 7.9% after the breach, its biggest intraday decline in almost four years, the Bloomberg report added.

4. 'Sextortion' Is Emerging Cyber Risk for Businesses, Warns Beazley

Reports of a new form of online bribery where cyber criminals attempt to extort cryptocurrency by claiming to have potentially embarrassing evidence of people using adult websites on work computers topped Insurance Journal's most popular cyber risk news of 2019.

According to a report issued by Beazley Breach Response (BBR) Services in February, so-called “sextortion” is adding to the tide of cyber-related incidents hitting businesses. The report explained that the crime begins with an email from someone claiming to have accessed the recipient’s work computer. The sender says they have tracked the addresses of pornographic websites the recipient has viewed and to have simultaneously recorded footage of their activity while watching these sites using their webcam.

There is no sign yet that the targets of sextortion are anything other than hoaxes targeting random individuals, and it often turns out that no data has been compromised, said Beazley in the report.

“Don’t panic, delete the email, and perform a thorough scan of your computer using a recognised anti-virus solution,” recommended Helen Nuttall, international breach response manager at Beazley. “If the email comes from your business email domain, alert your IT department, who should take steps to lock down the domain.”

5. CIA Says China, Russia Pose Biggest Cyber Attack Threats to U.S.

Russia and China pose the biggest espionage and cyber attack threats to the United States and are more aligned than they have been in decades, Reuters reported at the beginning of the year that the leader of the U.S. intelligence community told U.S. senators.

While the two countries seek to expand their global reach, Director of National Intelligence Dan Coats said, some American allies are pulling away from Washington in reaction to changing U.S. policies on security and trade, the Reuters report said.

“China, Russia, Iran, and North Korea increasingly use cyber operations to threaten both minds and machines in an

expanding number of ways – to steal information, to influence our citizens, or to disrupt critical infrastructure," Coats said.

6. FBI Warns on Rise in Sophisticated Cyber Crimes

In 2015, $220 million was lost to wire fraud in the United States. In 2019, losses were projected to surpass $1.5 billion, according to WFG National Title Insurance Co., the Associated Press reported in November.

The AP report stated that in the past, attempts to trick people were often clumsy, FBI agents told journalists in November. Now they can be sophisticated. If people are asked via email to transfer money under a deadline, they should not rush and instead call a known number of the person the email is purportedly from and confirm the request, the agents said. "The emails have gotten well-crafted and quite detailed.

They’re highly tailored to that particular victim,” said Gabriel Gundersen, an FBI supervisory special agent with the Oregon Cyber Task Force. “It’s a social engineering piece, where they’re coercing a victim to do something based on an artificial agenda or an artificial timeline.”

7. The Cost of Cyber Attacks to U.S. Economy

Malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016, the White House said in February.

The estimate comes in a Council of Economic Advisers report on the impact of cyber attacks on U.S. government and industry, as reported in Bloomberg. The report details the range of threats that U.S. entities face from actors, including corporations and countries such as Russia, China, Iran and North Korea.

“Cyber threats are ever-evolving and may come from sophisticated adversaries,” the CEA said in its report. “Due to common vulnerabilities, instances of security breaches occur across firms and in patterns that are difficult to anticipate.”

8. Financial, Reputational Costs of Cyber Attacks Can Ruin Small, Medium Firms: Chubb

The average price tag for a business to recover after a cyber attack is $400,000, which can be fatal for small-and-medium-sized enterprises (SMEs), according to a February report published by Chubb. This hefty cost of repairing the business and its reputation is exacerbated by the frequency of cyber attacks, which are reaching 4,000 per day since Jan. 1, 2016, said Chubb, quoting FBI statistics. Despite these statistics, many SMEs may not believe they are at risk, Chubb warned.

“Cyber attacks against SMEs often go unreported by the media, so these quite-frequent crimes tend to fly under the radar, and smaller companies may subsequently fail to understand the true extent of the risk,” said the report titled

“Cyber Attack Inevitability: The Threat Small & Midsize Businesses Cannot Ignore.”

9. Businesses Believe Cyber Insurance Covers More Than It Does: Survey

Seven in 10 senior financial executives at the world’s largest companies believe their insurer would cover most or all of the losses their company would incur in a cyber attack. Many of the losses they foresee, however, are rarely covered by insurance.

In a study released in July of more than 100 chief financial officers (CFOs) and other senior financial executives, commissioned by commercial property insurer FM Global, 45 percent said they expected their insurer will cover “most” related losses from a cyber security event, and 26 percent said they expected their carrier will cover “all” related losses.

But, according to FM Global, most of the effects these financial executives expect to experience in a substantial cyber security event aren't typically covered by insurance policies.

10. Cybersecurity Awareness Month: Time to Close the Cyber Coverage Gaps

As October of 2019 served as Cybersecurity Awareness Month, Insurance Journal reported it may be time for businesses – especially small- or mid-sized firms – to assess their understanding of current cyber risks and whether they're adequately covered by a cyber insurance policy.

In fact, a Willis Towers Watson report on cyber insurance trends to watch in 2019 stated that mid-sized companies, which it defines as organizations with annual revenue of less than $1 billion, will continue to drive market growth in the cyber insurance space as they realize the threat and potential financial consequences of a cyber attack.

“Midsize companies can be prime targets for cyber attacks because they often lack the resources and protocols of larger firms to defend against them,” wrote Joe DePaul, National Cyber/E&O Practice leader for North America at Willis Towers Watson and author of the report. “For others, the menacing headlines alone are enough to drive them off the sideline and into the buying market.”

A new year is now underway and with it could come new cyber risks and trends, so be sure to check out *Insurance Journal’s* Research and Trends page for additional resources and information on all things cyber. Happy new year, and thanks for subscribing to Insuring Cyber.