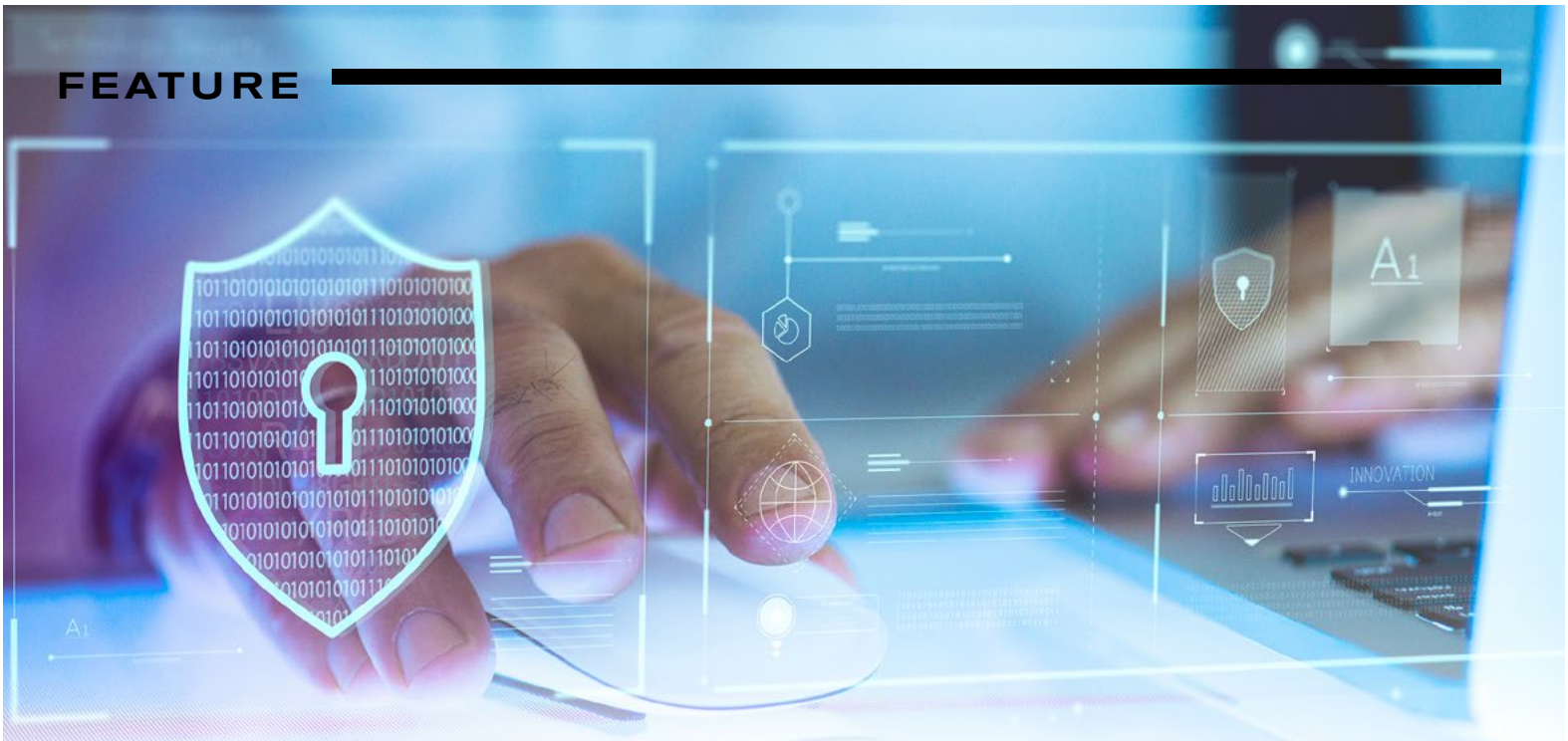


Emerging Trends: Captive Insurance and Cyber Risk

BUSINESS OWNERS AND LEADERS MUST TAKE THESE TRENDS INTO ACCOUNT WHEN DEVELOPING A ROBUST CYBER RISK-MANAGEMENT STRATEGY

Written By Laura Carabello

If the past two years have taught one thing, it's that the unexpected can and will happen: the onset and continuation of a global pandemic, the Russian invasion of Ukraine, and runaway inflation resulting from these and other market factors. Cybercrime is another factor to add to this list of unforeseen risks, with 2022 expected to be a record-breaking year for this type of nefarious activity, according to the Identity Theft Research Center (ITRC).

A cybersecurity breach can be decimating and costly for business, prompting more organizations to find ways to prevent business disruption. In this risk-laden environment, a growing number of companies will look to utilize their captives to cover cybercrime.

With the difficulty and unpredictable nature of mitigating against unexpected cybersecurity risks, captive insurance is positioned as a lifesaver, with its ability to write broad coverage and fill gaps in coverage.

Dana Sheppard, Associate Commissioner for Risk Finance, District of Columbia Department of Insurance, Securities and Banking gives some sage advice: "Captives are useful in insuring high severity, low frequency risks like cyber threats. Retaining a portion of this exposure in the organization's captive not only reduces the overall cost of this coverage, it also focuses management's attention on loss prevention and mitigation."

Mr. Sheppard states that ten captives in DC currently write cyber coverage and anticipates the number of captives that write this line of business will increase as organizations become more comfortable self-insuring these risks.
"DC captive law allows organizations to create unincorporated cells, which are ideal for this type of coverage because it allows captive owners to segregate cyber-related risks into a separate entity."

LARGE AND SMALL BUSINESSES ARE AT RISK

Industry experts advise that as cybercrime continues to become more sophisticated, attacks are forecasted to increase. Hackers appear to be getting more adept at their trade as they target even smaller businesses.

Ransomware and cyberattacks have seen a significant increase in frequency and severity in the last few years, fueled in part by the workforce moving to a largely remote model during the pandemic. There's also the possibility of political and diplomatic tensions with rogue nation states potentially increasing cyber-risk exposures.

Jeff Ellington, CIC, senior vice president, Capterra Risk Solutions, LLC says that cybersecurity is an ever-evolving risk. "Anyone who has attended an insurance industry conference or seminar in the last few years has most likely been given the opportunity to attend a session on cyber risks and how best to address them," explains Ellington. "And for those of us attending captive conferences, this theme has especially been true. One of the reasons for the predominance of concern with cyber risk is its unpredictable nature, which continues to expand in directions previously unseen or not anticipated."

Source: https://advisorsmith.com/data/small-business-cybersecurity-statistics/

As an example, in February of this year, a payment vendor was hit with a ransomware attack that may have exposed patient data from more than 600 healthcare providers and organizations. Professional Finance Company, an accounts receivable management company based in Greeley, Colorado, detected and stopped a sophisticated ransomware attack in which an unauthorized third party accessed and disabled some of PFC's computer systems.

The company said it immediately engaged third-party forensic specialists to secure the network environment and contacted law enforcement. During an ongoing investigation, it was determined that hackers accessed files containing certain individuals' personal information. The incident may have affected 657 of the company's healthcare provider clients.

The ransomware attack hit company computer systems that held data from clients such as Banner Health, Lifestance Health, Renown Health, DispatchHealth and hundreds of other provider customers.

The investigation uncovered no evidence of misuse of patient data, but data theft and the Company said that misuse could not be ruled out. The types of information potentially accessed in the attack included names, addresses, accounts receivable balances, information regarding payments made to accounts and, for some individuals, birth dates, Social Security numbers, health insurance information and medical treatment information.

MOST COMMON CYBERATTACKS

Companies and institutions need to be almost hyper-aware of this threat and devise effective methods and measures to prevent or mitigate it. The healthcare sector is especially vulnerable as organizations attempt to thwart portal cyberattacks which ripple through entire ecosystem.

A leading news magazine reported that the non-profit health care think tank ECRI recently listed cybersecurity attacks as the top health technology hazard for 2022. Many point to the proliferation of digital tools, such as member and provider portals, coupled with increasing consumerism in healthcare, translate in to exponentially more entry points for attackers to exploit.

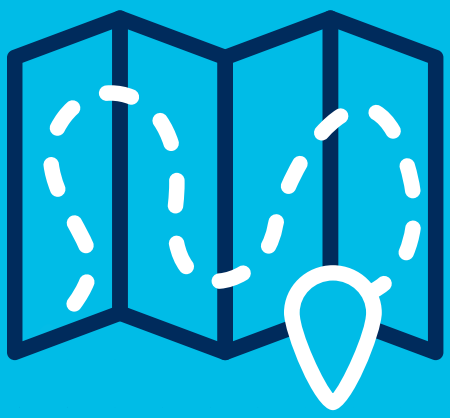
Cyberattacks may, in fact, be winging their way from as far as Russia. America's health care systems were put on the alert in March of 2022 when cybersecurity experts warned that attacks launched against Ukrainian institutions have the potential to spill over into America's health care systems, potentially endangering patients' lives.

According to reports, the cybersecurity program at the U.S. Department of Health and Human Services issued an analysis warning health care IT officials about two pieces of Russian malware that "could wipe out hospital data vital to patient care." This cautionary advice followed a previous warning from the American Hospital Association about increased risk related to Russian cyberattacks.

More recently – and equally alarming -- the Health Information Management Systems Society reported that North Korea-sponsored hackers have been targeting the healthcare and public health sector in the U.S. for more than a year.

AMWINS®
GROUP BENEFITS

amwins.com



The benefits landscape is broad and complex.

Skyrocketing prices. Administrative challenges. Shock claims. Aging workforces. At Amwins Group Benefits, we're here to answer the call. We provide solutions to help your clients manage costs and take care of their people. So whether you need a partner for the day-to-day or a problem solver for the complex, our goal is simple: whenever you think of group benefits, you think of us.

Bring on the future – we'll cover it.

An alert from the Cybersecurity and Infrastructure Security Agency (CISA), along with the FBI and the Department of the Treasury, included an advisory, "North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector."

The agencies allege that cyber actors have been using that novel strain of malware to target U.S. health systems since at least May 2021.

Furthermore, they urge healthcare organizations to "examine their current cybersecurity posture and apply the recommended mitigations," including training employees to recognize and report phishing attempts; enabling and enforcing multifactor authentication; and installing and updating antivirus/antimalware software on all hosts.

Additionally, COVID-19 has presented unprecedented challenges. To manage the pandemic and this extraordinary situation, the health sector has shifted its focus from the security of their systems and practices to their primary duty of delivering health care in order to save lives, placing themselves in a vulnerable situation.

Recent cyberattacks have impacted health care organizations, including the US Department of Health and Human Services, the World Health Organization (WHO), Gilead Sciences, Inc and numerous hospitals and health systems.

Captives are well positioned to help the health sector and the companies that access services on behalf of their employees. Being prepared to counteract cyberattacks is key to protecting the availability of essential health care services as well as the confidentiality and integrity of health care information.

Affirmative and stand-alone policies with clear and definitive language, as well as coverage and exclusions/inclusions that are detailed and clearly defined are expected to minimize or avoid disputes and litigations when a claim is presented.

The use of third-party technology and forensic cyber consultants to help with underwriting complement regular monitoring of the parent's cyber security policies, procedures and testing.

Kirsten Bay, CEO, Cysurance, explains, "Alternative risk financing programs for cyber are more frequently being contemplated by companies to broaden their risk financing capabilities at a reasonable cost while enhancing underwriting capacity."

She says that cyber captives are able to provide numerous options, including:

• Availability of Coverage – Cyber insurance is becoming harder for companies to find as markets have hardened and capital is scarce for this line of coverage and, it's likely going to get harder;

• Coverage Flexibility – Captives provide the ability to tailor coverages and limits to meet the needs of both large and small organizations where standardization in the traditional market is lacking; and

• Pricing Stability and Pricing Inequity – The crisis in the cyber insurance market, discussed above, saw the top 25% of companies cyber insurance rate increase an astounding 97.1% in the fourth quarter of 2021, while the median rate increase for all sizes of business was 50.2%. Captives can mitigate the extreme swings in the costs of coverages to support more consistent pricing.

COMMON TYPES OF CYBERATTACKS

To thoroughly understand the risks begins with awareness of the most common types of cyberattacks and how they impact the organization. Company leaders will want to become cybersecurity experts themselves. Advisor Smith points to these common attacks on small businesses:

Phishing attack. A phishing attack occurs when a cybercriminal poses as a trusted authority in order to gain personal information like passwords or credit card numbers. Businesses are increasingly seeing more phishing attempts, particularly spear phishing attacks, which target specific employees and generally see a higher success rate.

Data breach. A data breach occurs when your business's private or confidential data is accessed by an unauthorized party.

Malware attack. A malware attack is executed by malicious software.

Denial of service (DoS) attack. A denial of service attack is meant to take down a victim's network or system through a flood of malicious traffic.

Ransomware attack. A ransomware attack occurs when a cybercriminal gains access to your business device and locks down the system or blocks certain resources until your business pays a ransom. These attacks are becoming increasingly common, particularly as ransomware-as-a-service (RaaS) has emerged, allowing even those without technical expertise to execute ransomware attacks by paying for the service.

Source: https://advisorsmith.com/data/small-business-cybersecurity-statistics/

CAPTIVES TAKE CHARGE OF CYBERSECURITY

An A.M. Best report examining trends in the universe of Best-rated captives noted that cyber risk has become a profitable line of coverage for captive insurance companies.

Given the mounting risks, they predict that cyber-insurance coverage will continue to grow, citing a 75 per cent increase in direct premiums in 2021. Cyber risk represents one of the fastest-growing lines for captives that is generating "exceptional results" for the alternative-risk transfer vehicles.

According to the report cited above, "Given their flexibility, captive insurers can customize policies to mitigate the growing threat of ransomware attacks, aggregation risks and social engineering scams.

This allows parent companies to more quickly assess the damage and devise a plan of action toward recovery. Captives are being utilized as a strategic tool to provide cyber coverage, owing to proximity to the parent company — physically, culturally and enterprise-wide."

In its 2021 report, Aon noted that the frequency of ransomware attacks increased nearly 500 percent from the first quarter of 2018 to the fourth quarter of 2020. Along with the frequency have come growing costs and damages, with insured losses expected to reach $20 billion this year.

In response, they note that the number of captive insurance companies writing cyber coverage could grow by 34 percent by 2024, pointing out that captives still remain underutilized in addressing cyber risks, despite more than a six-fold increase in retained cyber premium.

There's other evidence of organizations increasingly looking to captive insurance companies as they try to address their cyber-risk exposures. Bermuda captives' gross written premiums for cyber risks increased 42% for the year ending 2020, according to the Bermuda Monetary Authority.

The number of captives writing affirmative coverage, meanwhile, was up from 20 in 2019 to 24 by the end of 2020, with more growth expected to come. Captives are continuing to "serve their purpose as a risk management tool for companies seeking to manage their own cyber risk exposures."

As cyber risks grow and securing affordable or adequate cyber coverage in the commercial markets becomes more difficult, captive insurance is playing a growing role in organizations' cyber-insurance programs. As organizations get a better understanding of the extent of their exposures and the need to protect against them, it appears the role of captive insurance in addressing the exposure will continue to grow as well.

As it has with other difficult-to-cover risks, captive insurance is being used more and more often to provide part of the cyber-risk financing solution. A captive insurance company provides an added risk-financing option to organizations that realize that cyber events can have a significant bottom-line impact. Among the many risks, ransomware attacks are one of the areas experiencing significant increases, drawing insurers' attention.

As cyber-insurance deductibles reach a point where they're more difficult for some organizations to manage, industry thought leaders say that captives are even funding deductibles. In this situation, the captive insurance company's surplus provides a deductible reimbursement program from the captive for the commercial cyber-insurance policy.

Jeff Ellington sums it up, pointing out that whereas most insurance companies now cover cyber exposure, any policies still contain significant exclusions or sub-limits which might not provide necessary protection.

"This is where a captive can prove itself to be the best solution to adequately cover a business's cyber exposure," says Ellington. "With the ability in most cases to offer broader coverage with less exclusions, and with the flexibility to complement policies through the standard market by providing coverage for a primary layer or excess layer, captives continue to be a viable alternative for business owners navigating the ever-evolving risks to their companies from cyberattacks." ■

Laura Carabello holds a degree in Journalism from the Newhouse School of Communications at Syracuse University, is a recognized expert in medical travel, and is a widely published writer on healthcare issues. She is a Principal at CPR Strategic Marketing Communications. www.cpronline.com

Sources:

https://www.usnews.com/news/health-news/articles/2022-03-11/could-russian-hackers-cripple-u-s-health-care-systems

https://www.healthcareitnews.com/news/feds-warn-north-korean-ransomware-threat-healthcare-organizations

https://www.captiveinternational.com/news/captives-still-learning-when-it-comes-to-cyber-says-aon-4866

https://www.forbes.com/sites/bernardmarr/2022/03/18/the-biggest-cyber-security-risks-in-2022/?sh=67556df87d7b

https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response

https://www.entrepreneur.com/article/416093

https://www.captiveinsurancetimes.com/captiveinsurancenews/industryarticle.php?article_id=8001&navigationaction=industrynews&newssection=industry

https://www.entrepreneur.com/article/415842

https://www.entrepreneur.com/article/281002

https://advisorsmith.com/data/small-business-cybersecurity-statistics/

https://www.nasdaq.com/articles/cybercrime-predictions-for-2022

https://www.captive.com/news/as-cyber-risks-grow-so-do-captive-insurance-cyber-risk-premiums