THE CYBER LIABILITY INSURANCE MARKETPLACE, CAPTIVES, AND THE GAO

Written By Karrie Hyatt

It comes as no surprise that cybercrimes are increasing and becoming increasingly more expensive. In fact, these crimes are becoming more sophisticated with cyber criminals capitalizing on multi-pronged methods of gaining access to computer networks and data.

According to a recent report from Cisco, "Cyber security threat trends: Phishing, Crypto Top the List," 86% of organizations surveyed had at least one user try to connect to a phishing site, 96% of organizations experienced some level of unsolicited crypto mining, and 50% experienced some type of ransomware activity. The report showed that multi-staged attacks were becoming more prevalent as cyber criminals become more advanced in their capabilities.

In Verizon's 2021 annual "Data Breach Investigations Report," they similarly found that 85% of security breaches involved a human element. The report also found that phishing scams were present in 36% of security violations in 2020, up from 25% in 2019. An increase that "correlates with our expectations given the initial rush in phishing and COVID-19-related phishing lures as the worldwide stay-at-home orders went into effect."

According to A.M. Best, the cyber liability insurance market in the U.S. is now worth $2.7 billion. Cyber insurance premiums grew by 28% in 2020, but cyber insurance claims grew by 38% between 2017 and 2020.

Yet, the traditional insurance market is not keeping up the pace to the desires of its customers. "Not only have commercial markets hardened, prices are increasing drastically and coverage is being limited while carriers are increasing deductibles," said John R. Capasso, president and CEO, Captive Planning Associates, LLC. "This is having a profound effect on our mid-sized clients."

According to Les Boughner, chairman of Business Insurance at Advantage Insurance Inc., "Commercial coverage is very expensive with numerous restrictive exclusions. Capacity is limited. Commercial underwriters are concerned with the significant increase in claims activity and respond accordingly. According to a recent Marsh study claims are up 55% and premiums have increased 86% YTD in 2021. The Wallstreet Journal reported [in August that] the ransomware payments in 2021 have doubled to 600 million."

"Right now, our clients—who I characterize as "main street American businesses"—largely are depending upon the standard commercial insurance marketplace to insure their potential third-party liability as a result of a cyber incident," said Harry Tipper, III, chief operating officer of insurance with CaptiveOne Advisors LLC. "Their bigger concern is the impact of such an event on their business operations and economics. Few if any have seen the standard insurance market address the business interruption/economic loss fallout from a cyber incident, especially if they are not the direct target. Instead, they universally have concerns over the business interruption/economic loss fallout from a cyber incident."

CAPTIVES INSURING CYBER RISK

Captives are helping to provide solutions for the gaps in cyber coverage offered by the commercial insurance marketplace. Either by adding cyber liability to their existing captive or a "difference in condition" option which covers losses that are denied by the commercial carrier and can be used to shore up gaps that are found in traditional policies.

“Captives provide a responsive vehicle for their owners to manage this environment. They can insure retentions and broaden coverage for their owners. Sophisticated captives can access the reinsurance market which is often more competitive than admitted insurers,” said Boughner. “In the commercial market cyber has evolved from a free add-on used to differentiate underwriters to a vital coverage that is individually underwritten. We are asked to routinely include cyber coverage to captives. 75% of our captives under management have some form of cyber coverage.”

For Capasso, more than 60% of captives managed by Captive Planning Associates have some type of cyber liability insurance. “In many respects, captives can offer similar coverage as a commercial carrier. However, it's usually not economical to do so. For a business to self-insure for cyber liability, it would have to capitalize the captive with an enormous amount cash (or letter of credit) in order to cover the policy limits. With that said, we see many businesses, especially mid-sized businesses utilize their captive to cover large deductible policies issued by commercial carriers as well as policy limitations and exclusions,” said Capasso.

“Among those captives that do offer cyber liability insurance, the principal motivation has been the degree to the standard—cyber liability insurance marketplace is in flux vis-à-vis coverage terms (i.e., exclusions), pricing, and limits,” said Tipper. “[Businesses] ask their captives to provide “difference in conditions” insurance that is designed to plug the holes and fill-in the gaps in coverage that the conditions and exclusions create. They also will ask their captives to provide additional capacity when the standard insurance marketplace wants to restrict risk-transfer capacity through such tools as sub-limits within the policy.”

TRIP AND THE GAO

Currently, the Government Accountability Office (GAO) is conducting research into cyber liability insurance coverage in both the traditional marketplace and through captives. Part of the investigation is looking at how captives insure cyber liability and how the Terrorism Risk Insurance Program (TRIP) has benefited captives.

TRIP is stop loss insurance provided by the federal government in the event of a terrorist event. After September 11, 2001, many insurers began excluding terrorism risk coverage from their regular policies. In 2002, seeing that the loss of coverage could have a heavy impact on businesses, Congress enabled the Terrorism Risk Insurance Act of 2002 (TRIA) which requires insurers to make available terrorism risk on certain lines of commercial property and casualty insurance, with a backstop provided by the federal government. The Act has been reauthorized four times and the most recent update, in 2019, extended TRIP to 2027.

As cybercrime events become more costly and have a larger impact on society, the federal government is looking into adding cybercrimes to TRIP or create a similar back stop of its own. As part of the research, representatives from the GAO spoke with a group of SIIA members, including John Capasso, Harry Tipper, and Les Boughner, who were interviewed for this article.

“Based on SIIA's meeting with them, the folks at the GAO are looking more broadly than the cyber liability insurance marketplace,” said Tipper. “Because the study that is being conducted is under the auspices of the reauthorization of TRIA, their focus is more broadly on the risk of cyber terrorism, the insurance industry's response to that risk, and the impact of TRIA on all the actors within the insurance marketplace. The captive insurance ecosystem is just one segment of a broader study whose focus is TRIA.”

UNSTOPPABLE

SPIRIT

See Our All-Star Speaker Lineup!
Live and **In Person!**

HCAA is bringing the glitz and glamour back to the self-funding industry in-person with Executive Forum 2022! Join us at the Bellagio in Las Vegas for impressive keynote headliners, powerful sessions on the topics most relevant in today's marketplace, and networking and connection-making galore! For those unable to attend in-person, we will also have a virtual registration offering.

Learn More and Register at hcaa.org/page/ExecutiveForum

HCAA's
EXECUTIVE
FORUM '22

REGISTER TODAY! FEBRUARY 21-23, 2022

BELLAGIO, LAS VEGAS | #HCAAEXECFORUM | HCAA.ORG

According to Boughner, in the interview, "The GAO was focused on cyber terrorism and the use of TRIP to provide catastrophe capacity to the insurance industry.... In spite of there not having been any significant terrorism events the program has been renewed with increasing attachment thresholds. While TRIP would be available for a significant terrorism event, the GAO is investigating if the need is there for TRIP to backstop cyber insurance without a terrorism event."

"The financial impact of cyber incidents is but one example of a catastrophic risk against which any individual insurance company, captive or otherwise, cannot assemble a large enough risk-sharing pool in order finance the potential monetary cost of an event in an economic manner. The risk of prediction error is just too great," said Tipper.

He went on to cite the Colonial Pipeline cyber hack in June and how the knock-on effect of the gas pipeline being shut down affected millions of people on the East Coast.

Both Tipper and Boughner said that cyber insurance requirements should not be legislated. Instead, the U.S. government should concentrate on intervention prior to cybercrime event and the mitigation and management of the risk of a devastating cyber-attack.

AMWINS™

amwins.com

Benefits are an endlessly evolving landscape.

Stop-loss. Skyrocketing prices. Administrative challenges. Shock claims. Amwins is your group benefits lifeline—whether you need help navigating the chaos, solving for the unique or simply looking for additional options. Our purpose is simple: Find and deliver the specialty products you want coupled with the administrative solutions you need.

Broker, consultant or carrier, let us make your life easier through custom programs and expanded capabilities. Amwins has the relationships and insights to tackle what comes next.

Bring on the future – we'll cover it.

"The government should be focused on cyber intervention not unlike military intervention," said Boughner. "Many cyber-attacks are initiated from countries such as Russia and North Korea who are unfriendly to the United States. The government and the military should treat this as a hostile act and respond accordingly. They should not legislate cyber coverage or force the insurance industry to provide coverage. TRIP could be broadened to include non-terrorism cyber events. TRIP could also be broadened for pandemic catastrophes although this was not an area that the GAO was investigating."

According to Capasso, "I think that government providing a backstop (reinsurance option) to include captives in a TRIA-like program would be an immensely good thing."

The SIIA members interviewed by the GAO were happy with the opportunity to talk about captives. "As an industry, we believe that any time a governmental agency takes the time to learn about how captive insurance companies provide an alternative risk management option for businesses as well as providing supplemental coverages, is a good thing," continued Capasso. "I thought the GAO asked some very good questions. I also think those of us interviewed did a commendable job answering the GAO questions and providing further insight into how the alternative risk market helps businesses manage risk."

According to Tipper, "The GAO interview presents SIIA with a great opportunity not only to showcase another instance where captives could provide solutions to American businesses' problems but do so to a governmental agency that historically has taken a dim view of captive insurance. My impressions was that the members of GAO staff came out with a favorable view of what captives are doing vis-à-vis the cyber risk specifically."

For Boughner, "It was a very encouraging experience. They were genuinely interested in learning about the role that captives could play for cyber and cyber terrorism events. Since purchasing terrorism insurance is voluntary, many companies elect to self-insure. Without a captive, the self-insurer has no recourse to the TRIP pool in the event of a major terrorism incident. Since TRIP is only available to insurance companies, a captive is necessary to access TRIP protection." ■

Karrie Hyatt is a freelance writer who has been involved in the captive industry for more than ten years. More information about her work can be found at: www.karriehyatt.com.