Better When Working Together

Interviewee: **Randy Sadler, *CIC Services***
Published: **January 20, 2021, *captiveinsurancetimes***

As firms moved to a work-from-home environment in response to COVID19, cybersecurity has been highlighted as an increasing challenge. Industry experts suggest while captive coverage is tailored to the needs of the business, a commercial policy is just as important.

Since March 2020, there has been a huge increase in the number of people working from home due to the ongoing COVID-19 pandemic. However, due to how quickly government decisions were made, most businesses were left unprepared.

One of the biggest challenges for companies was cybersecurity and data breaches. A recent FBI's Cyber Division report found that the number of cyberattacks is up to 4,000 a day, representing a 400 per cent increase of pre-COVID-19 numbers. Elsewhere, a report from IBM and the Ponemon Institute showed that the average cost of a data breach has risen to $3.92 million.

It is not just an issue for large corporations, small businesses are also not immune to cybercrime. According to data from Accenture, 43 per cent of cyberattacks are aimed at small businesses and cost an average of $200,000.

When describing trends he has seen in cybercrimes since the shift to a working-from-home model, Oliver Delvos, global cyber underwriting manager, commercial insurance at Zurich Insurance Group, explains there has been a rise in more sophisticated phishing campaigns, "especially during a time when companies are rolling out new processes and procedures which are communicated via email".

Remote working requires seamless implementation of security protocols and processes, including multi-factor authentication, advanced password controls as well as properly configured and patched systems. Delvos highlights that if those measures are not implemented properly, this might lead to an increased vulnerability to cybercrime.

Although many firms use commercial cyber policies for coverage, there can be gaps, leaving firms exposed. Randy Sadler, principal with CIC Services, explains that some commercial policies will not cover losses that occur due to employee error.

Sadler explains this can be problematic as he quotes a study by IBM which stated that human error accounts for 95 per cent of data breaches. Another gap that is becoming common is social engineering fraud. Dustin Partlow, senior vice-president at Caitlin Morgan Captive Management, states: "I hear of more and more companies getting wire transfer or payment instructions from vendors and end up paying significant amounts to the wrong person."

Social engineering is one of those coverages that generally is part of the crime policy and not the cyber, but it seems there is an increase in the number of incidents occurring. Partlow explains: "Companies think they are covered only to find out that the cyber policy they purchase does not cover it."

The world has advanced so much over the last decade, especially in technology, but has the rise of new technologies has made it harder for firms to gain specific coverage against cyber-attacks?

Delvos notes that the rise of new technologies and processes is an integral part of the development of a company and the economy as a whole. He says: "As insurers, we need to respond to that and develop in parallel and find solutions. It is important to bear in mind that technology for protection also develops and improves."

Also weighing in, Sadler says the nature of cybercrimes, which is complex and rapidly changing,makes it difficult to insure against in the commercial market.

This is where captives come into play. Sadler explains that captives have the unique ability to write broader coverages with fewer exclusions that can be interpreted based on the 'spirit of the coverage' versus the specific 'letter of the coverage' resulting in better protection in the ever-shifting sands of the cybersecurity marketplace.

Loading.... captive coverage

In response to the hardening cyber risk insurance market, existing captive owners are looking to increase the use of their captives to include additional risks while others are exploring setting up new captives, according to Grant Maxwell, global head of alternative risk transfer at Allianz Global Corporate & Speciality (AGCS).

Maxwell reveals that cyber is one of the top risks that regulators see captives writing more frequently.

The use of a captive for cyber risk coverage can provide various benefits that generally come with self-insurance but also

(Continued)

additional ones. While a captive is a very valuable tool that can be utilised in coordination with a company's commercial cyber insurance policy to enhance coverage, fill in gaps in commercial coverage, and enhance limits afforded, Partlow suggests that a captive is not a better option than commercial insurance for cyber risk.

He explains: "The reason I believe a captive is not a better option than commercial insurance is that when a cyber incident does occur, the vast tools offered by the commercial insurance carrier are invaluable."

A significant portion of the claims costs for a cyber claim relate to the identification of files impacted, and notification of third parties whose data may have been compromised.

Access to the tools offered by the commercial carrier in regards to the identification of files impacted, notification of those parties affected, Partlow suggests will go "a very long way in terms of controlling the ultimate costs of the claim".

"A captive can definitely pay out a claim no problem, but when funding cyber risk through a captive, if a claim occurs and there is the need to notify third parties of a data breach my concern is that generally the parent company and captive do not have these tools in place that the commercial carrier does," Partlow adds.

Agreeing, Sadler says that CIC Services does recommend "an either-or approach when a bothand approach might suffice".

He adds: "We usually recommend our clients blend a commercial cyber policy with a captive policy. Captives can address losses associated with complex threats and insure any gaps or exclusions in commercial policies, so they're an ideal vehicle to protect businesses."

Although it's recommended to have both a captive and commercial policy in place, some firms still continue business without either. Sadler suggests one of the reasons for this is that many businesses and business owners struggle to pay insurance premiums for things they don't fully understand.

He notes: "Everyone knows what a car wreck looks like. We all know what a destroyed property looks like. Most know what an injured worker looks like. Many business owners don't fully appreciate what a cyber loss 'looks like' unless it has happened to them."

With the procurement of cyber insurance increasing over the last several years, Delvos suggests that many companies realised last year how their entire value-chain depends on smoothly running IT.

However, despite this, he explains that many companies are still in the process of understanding/quantifying their cyber exposure and reviewing scenarios that could impact them severely. "Risk transfer is only one part of the solution, and only comes at the end of the entire self-evaluation process," Delvos believes.

Writing cyber coverage

With businesses still reviewing how cyberattacks could affect their business, Sadler says it's "critical" for companies to recognise that the stakes are high and cyber risk is ever-evolving, so companies need a robust risk management strategy.

"This is not a place to cut corners. Businesses need to combine both active and passive measures and comprehensive insurance coverage that addresses all facets of risk. This creates an opportunity for captive insurance which can not only be written to fill exclusions and gaps, but the accumulated loss reserves provide financial aid to weather a future crisis," he adds.

It's not just about the business understanding the insurance coverage. Paul Wöhrmann, head of captive services for Europe, the Middle East and Africa, Asia Pacific and Latin America, commercial insurance at Zurich Insurance Group, suggests it is important for a risk manager and captive owner to select a professional fronting partner who is experienced with the complex captive reinsurance world and can provide access to a large international insurance network.

Wöhrmann adds: "In particular for cyber captive involvements, we have experienced that the pricing of appropriate captive premiums requires a lot of expertise on the part of the fronting insurer. Finally, professional insurance claims management expertise is key for captive involvements."

RANDY SADLER started his career in risk management as an officer in the U.S. Army, where he was responsible for the training and safety of hundreds of soldiers and over 150 wheeled and tracked vehicles. He graduated from the U.S. Military Academy at West Point with a Bachelor of Science degree in International and Strategic History with a focus on U.S. – Chinese Relations in the 20th century. He has been a Principal with CIC Services, LLC for 7 years and consults directly with business owners, CEOs and CFOs in the formation of captive insurance programs for their respective businesses.

CIC Services, LLC manages over 100 captives.