Don't Get Your Wires Crossed

Interviewee: **Randy Sadler, *CIC Services***
Published: **April 2022 - Issue 243, *captiveinsurancetimes***

See original here: https://www.captiveinsurancetimes.com/editorspicks/editorspicks.php?editors_picks_id=199&navigationaction=editorspicks&newssection=editorspicks

Rebecca Delaney explores how the evolution of cyber risk has led to more companies considering captives to close coverage gaps left by the expensive commercial market.

Universally recognised as a rapidly-evolving risk, cyber has seen an exponential expansion over the last decade in the use of online platforms for communication, retail, financial transactions, and just about every other staple of modern life. Niel Harper, cybersecurity and digital policy expert at Octave Consulting Group, explains that cyber risks have evolved synchronously with this growing connectivity of companies, households and devices.

"Criminals have become more organised and professional as they seek to make money from stealing information and committing fraud, and we have seen noticeable increases in state-sponsored cyber attacks, including industrial espionage and critical infrastructure disruption," he notes.

Cybersecurity as an issue accelerated to the top of companies' agendas during the COVID-19 pandemic as entire work systems shifted online. This operational transition revealed cyber liability exposures and vulnerabilities within organisations, causing many firms to reassess their security protocols and processes. Randy Sadler, principal at CIC Services, contends: "Cyber risk is ever-evolving, since cyber criminals are becoming increasingly more advanced and have quickly adapted. The COVID-19 pandemic exacerbated the situation by fast-tracking digital change. An increase in cybercrime emerged as businesses moved to remote work models that pose vulnerabilities, weaken systems and create exposure to breaches."

In this current environment, characterised by accelerated implementation of digital transformation programmes — and as the velocity of digital change outpaces security — cyber threats are evolving into a form of disruption that organisations must learn to live with, rather than being able to eradicate entirely. The nature of cyber threats can range from supply chain attacks, data breaches and targeted malware attacks.

Ransomware in particular was named as the number two concern among risk professionals in Airmic's 2021 Annual Survey, while business interruption following a cyber event was identified as the top front-of-mind risk for risk professionals as a result of the exponential increases in cyber insurance rates. Harper describes how ransomware has become a commodified form of organised crime: "Fears around COVID-19 and the immediate rush to deliver contact-tracing applications created opportunities for threat actors. Additionally, online adversaries have ramped up their targeting of software supply chains since the start of the pandemic. Extending beyond the generally accepted damage to information assets, cyber risks now also include regulatory fines, non-physical business disruption, and directors' and officers' liability."

Timothy Powell, head of financial lines and cyber at Zurich, notes that heightened awareness of cyber exposures translates into a maturing market for cybersecurity services and providers. He explains: "This is a continuing evolution of what we have seen with businesses becoming far more interconnected electronically. People are becoming more aware of those risks as a result of this interconnectedness, and that awareness is driving insurance and risk management." Cybersecurity and cyber resilience protocols are essential, with Powell adding that the growing industry of cybersecurity consultants, such as Zurich's Cyber Resilience Services, can vastly help to improve the security profile of an organisation.

Sadler agrees that it is important for companies to follow best practices to mitigate the risk of a cybersecurity breach, including regular risk assessments, employee education, password protection, multi-factor authentication, and data encryption. However, he notes that commercial cyber policies are not always adequate when implemented alongside these best practices.

The commercial cyber insurance market has adopted somewhat inconsistent approaches to capturing and analysing data, creating a wide variety in the risk appetite for cyber cover, as well as challenges surrounding programme capacity, high premium rates, reduced insurer capacity, and more stringent underwriting criteria.

Common gaps in cyber coverage include a lack of proper asset inventory, weak identity and access management, and lack of segmentation.

For example, a commercial policy may not cover cyber risk arising from human error on the part of a company's employees, rather than 'bad actors'.require 24/7 vigilance for a risk that never sleeps. Developing a comprehensive and flexible protection and response plan will help protect your digital assets, avoid the costs associated with a cyber loss and provide your organization a potentially significant competitive advantage.

(Continued)

In this turbulent and fragmented cyber insurance market, organisations are increasingly turning to captive insurance to finance their cyber risk and address coverage gaps. This is affirmed by Alex Gedge, senior captive consultant at Hylant.

"Cyber insurance has evolved alongside cyber risk; with the hard market, pricing has increased and capacity has decreased. Many companies are struggling to adequately cover their cyber risk in the traditional market and thus are looking at alternatives," Gedge says.

Ctrl + Alt + Captives

A captive can provide a tailored alternative risk management solution to meet the specific exposures of an individual company. This means it can help cover vulnerabilities and key areas where traditional insurance coverage fails, as well as support operations through risk mitigation controls.

Paul Wöhrmann, head of captives at Zurich, elaborates: "In the European market, there is a growing interest among large corporates exploring the use of a captive because they often face capacity restrictions on the insurance side. Alternatively, they may want broader policy language to protect their local subsidiaries across an insurance programme and across various jurisdictions."

"Provided that captive owners use their captive effectively, they can bring more risk management interest and incentives within their own organisation to identify what kind of exposure they face in the business segment, what kind of claims have happened, and collect vital information from this."

CIC Services' Sadler notes: "On the front end, a captive insurance company is not inexpensive to create, as there are start-up and operational costs to consider. But in the long run, the captive insurance company serves as a lucrative financial strategy that goes beyond covering losses and provides a valuable profit centre that can enable businesses to survive during crises."

Hylant's Gedge adds that a captive should be considered as an alternative risk solution for cyber risk because it can offer additional coverage, both in traditional capacity and in difference in conditions or difference in limits. Captives offer other advantages for cyber risk in areas where the commercial market falters. As well as capacity,

Wöhrmann identifies that, currently, the insurance and reinsurance markets are confronted with a lack of historical data to model specific cyber risks, which in turn presents difficulties for actuaries looking to build professional modelling. Implementing a captive can help to close this gap over time.

Harper affirms: "Given the unavailability or prohibitively expensive nature of commercial insurance coverage in several markets, captives offer up great potential in terms of formulating a statistical base, which can make it easier to obtain excess coverage at favourable terms and pricing."

He adds that captives can be utilised for coverage that is not readily accessible in the traditional insurance market, or is not packaged into commercial offerings despite being a highly correlated risk. Prominent examples are cyber risk, technology failure, loss of value of intangible assets, and future lost revenue.

Published last month, Aon's 2022 E&O and Cyber Market Review found that financial institutions and healthcare organisations are the highest users (30 per cent) of captives for cyber, owing to the unique risk profiles and a typically higher level of risk maturity in these segments. This is a result of stricter regulation and the potentially disastrous consequences of a cyber attack or data breach in these industries. Powell identifies a connection between the cybersecurity of an organisation and the way that it transfers its risk, whether through a captive or on a direct basis.

He explains: "Large companies have the resources to invest in cybersecurity and may have a chief information security officer or a department focused on the security posture of the organisation. This will do them a world of good when it comes to considering a captive solution because they will have a better risk profile in the insurance and reinsurance market to place that cover — in particular, to place it via a captive."

Error_lack_of_data

But what about those companies that do not have the resources to form such comprehensive insights and make investments in cybersecurity? Wöhrmann acknowledges that there are challenges in ensuring a captive is sufficiently capitalised, particularly for cyber risks as a new market.

"If a captive has only covered property and casualty risks thus far, it is possible to provide a view of the economical capital required for the captive owner. This is more difficult with cyber because we do not have sufficient experience or historical data," he says.

Similarly, Powell explains that insurers traditionally rate and price their risks based on years of aggregated data so that actuaries can project future losses based on this history. "That situation does not exist to the same extent in cyber simply because the history is not there," he says.

This is affirmed by Gedge, who adds that this lack of data for both individuals and the wider market is indicative of any new or emerging risk. She explains that this results in companies taking more time to fully understand their business exposure to cyber insurance, as well as determining what portion of the risk they wish to retain, and the ultimate pricing and cost to the captive.

Gedge notes: "While data is improving across this line, it can still be a challenge to fully understand the implications of what is covered by your cyber policy. It is invaluable to speak to captive consultants, actuaries and brokers to understand exactly what the risk is to the business and how best to manage it through the captive."

Assessment and quantification of cyber risk requires a robust approach, rather than basing the underwriting on binary questions that do not take into account the broader context of the cyber landscape, warns Harper.

(Continued)

Aon's Cyber Market Review notes that, although on an upward trajectory, risk financing maturity is still in relatively early stages, with many organisations that place cyber risk into captives relying on management intuition or benchmarking to inform their approach rather than deterministic or qualitative analysis. The review notes: "Cyber, although no longer emerging, can still be considered in the 'incubation' phase for captives, mainly because the traditional risk management approach and the network security communities are not fully aligned. However, reframing the captive from a tactical, transactional play to something linked to the broader maturity development of risk will help accelerate this alignment." Cyber Risk 22 Zurich's Wöhrmann adds that another challenge lies in the future of cyber developments, and uncertainty over whether limited underwriting appetite on the traditional side will continue.

The reaction of the market to this is important, he notes, given how closely captive trends and their use in a transactional manner is correlated with market conditions.

This evolving environment will see the risk management and insurance community continue to develop its understanding of the underlying risks facing organisations, while exploring the role a captive can play in this dynamic.

Press any key to continue

Discussing how the landscape of cyber risk is likely to evolve over the next 18 months, Sadler says: "There is no doubt that cyber risk will grow and evolve as technology continues to advance and criminals become more sophisticated."

This includes even more refined phishing and ransomware attacks targeting new 5G networks. Sadler continues that it will be even more critical for organisations, regardless of size, to be aware of emerging cyber risks and trends, and to also adopt a proactive approach in cybersecurity assessment.

Harper agrees that ransomware attacks are likely to become more prevalent owing to the lucrative nature of Ransomwareasa-Service. He says: "Given that cyber physical systems (such as industrial control systems, water systems, robotics systems, and the smart grid) are not generally built with security by design, vulnerabilities in these systems will continue to be widely exploited in the coming months.

"There is also a growing interest by attackers in the use of deep fakes in facilitating business email compromise and in circumventing multi-factor authentication solutions and knowyourcustomer identity proofing."

With cyber risk set to only inflate in frequency and severity, risk professionals are urging organisations to reassess their cybersecurity posture and ensure they have sufficient insurance policies.

Harper adds that it is important for companies to complete an inventory of their digital assets and relevant threats, as well as identify cyber risk scenarios, and assess and quantify both the direct and indirect consequences.

"Businesses should then run the inputs and scenarios through a cyber cost framework that considers publicly and non-publicly available information about actual cyber losses, ultimately providing the organisation with an estimated maximum loss and most likely loss values for each chosen scenario," he adds.

This will then provide an estimate of coverage gaps or losses, which offers a more quantitative assessment of business impact from cyber.

Harper notes that companies should also take care to review their risk shifting and risk distribution practices, warning that regulators are increasingly scrutinising captives in particular. Both Sadler and Gedge anticipate that premiums in the global insurance market will continue to grow as the hard market persists across several lines of business.

In these market conditions, it is likely that cyber insurance premiums in captives will only increase.

With captives set to be implemented as the alternative risk financing vehicle for cyber risk, Powell identifies that insurers are increasingly considering the sustainability of their insurance programmes.

"As their cyber insurance portfolios grow, insurers are considering how to manage the accumulation of all these exposures from policies in their portfolio, particularly in the event of a catastrophetype cyber attack that affects multiple people at once. Insurers are very keen to understand what this accumulation risk poses to their portfolio," he explains.

"It will be interesting to look to the so-called alternative market in the future, as captives can learn and understand how the insurance-linked securities market may respond to the need for cyber protection behind a captive, as well as what terms and conditions need to be fulfilled to make them more interested," Wöhrmann concludes.

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.