LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Rising Cybercrime Drives Some Reinsurers Away

By **Daphne Zhang**

Law360 (October 26, 2021, 9:40 PM EDT) -- American companies are in desperate need of cyberinsurance coverage, but unpredictable cyber risks have scared some insurers and reinsurers away, leaving policyholders navigating skyrocketing insurance premiums, experts say.

The insurance industry is trying to be clear about what is covered and what is not in terms of fast-evolving cyber risks, sending out messages that systemic risks and cyberwars among nations are not covered under many insurance policies.

At the same time, more corporate policyholders are trying to get dedicated cyberinsurance. If they don't have any, they may risk shareholders asking why they did not adequately protect the company following a cyberattack.

But the supply hasn't caught up with the demand. There is not enough money supporting cyberinsurers in the reinsurance market, and cyber reinsurers are also having a hard time finding enough capital to protect themselves in the retrocession market. Retrocession, or "retro," refers to a reinsurer transferring some of its risks to another reinsurer.

"The primary cyberinsurance market right now for 2021 is around $11 billion, and around 30% to 50% of that $11 billion is reinsured," said Anjali Dharma-Wardana, a cyber reinsurance underwriter with Envelop Risk.

She said reinsurers want to take advantage of the "astronomical" cyber premium increases in the primary insurance market, but they are "constrained" by lack of retrocession support.

"The retro market isn't growing as much because we only have these few reinsurers to reinsure each other," Dharma-Wardana said. "We're slowly getting toward the capacity crunch."

However, the dominant players in the cyberinsurance and reinsurance space are benefiting from the hardening market and hefty premiums by tightening insurance contract language and adding sublimits. They face few hurdles in adding exclusions to cyber policies when they deem it necessary, reinsurance underwriters told Law360.

"Whenever we want to put an exclusion now on the reinsurance side, we get it," Dharma-Wardana said. "We are in a hard insurance market, so we're in a position to be really strict and add lots of exclusions to protect ourselves."

Michael Miguel, a principal in McKool Smith's insurance recovery group, said the "pressure on corporate America to secure the cyberinsurance is so great that the imposition of more restrictive exclusions is not going to lessen the market or the appetite to get it."

"What we're seeing here is there is less money available in the secondary [reinsurance] market," Miguel said, adding that insurers are saying they don't have the capacity to meet the demand when American companies need it the most.

"I have many clients that are having severe difficulty in getting policy renewals," the policyholder attorney said. "If you had $10 million last year in cyber coverage, you're going to be lucky to get $2 or $3 million with a more expensive price this year."

Miguel said insurers are replacing a traditional one-page renewal application with over 10 pages of difficult questions on policyholders' cybersecurity measures. But insured companies are desperate to maintain their cyber coverage, or else their shareholders will question whether they took the right steps to protect the company.

The cost of cyber events across the globe is projected to **surpass $10.5 trillion by 2025**, with the number of records compromised due to cybercrime being a top indicator of potential losses, according cyber risk analysis firm RiskLens.

Although the cyber reinsurance supply may not meet the growing demand, major players in the market still see huge opportunities.

"Only a small part of the global cyber risk is currently insured," said Maya Bundt, head of cyber and digital solutions at Swiss Re. "This is evident in the stark contrast of more than $1 trillion cost incurred due to cybercrime for the global economy, compared to approximately $8 billion of insurance premiums."

Bundt is optimistic about the long-term prospects of insurers continuing to be able to provide coverage for cyberattacks — so long as clients take more proactive steps to mitigate the risks of being victimized.

A Shortage of Cyber Reinsurance

Cyber risks are developing at a rapid pace, and insurers do not have enough historical models to predict how much capital to throw in without burning themselves out with unpredictable losses. While the existing big reinsurance players are trying to grow as much as possible, traditional reinsurers that do not have a cyber portfolio are waiting for the industry to gain a better understanding of cyber exposures.

"When you start looking at the book as a whole, there are all these cyber claims that are just eroding the policy limits and the risk is spread so thin," said Jennifer Rothstein, head of cyber insurance and legal at cybersecurity firm BlueVoyant.

Cyber reinsurance growth has slowed down and is not keeping pace with demand, experts say. Reinsurers are not comfortable increasing cyber exposures because acquiring cyber reinsurance requires a lot of work, and "it's just not returning as well as other classes of business," such as the more mature property coverage market, said Tom Johansmeyer, head of property claim services at ISO Claims Analytics.

Reinsurers are also well aware that cyberinsurers are shifting a significant amount of the risks to them, he said, and they ask the carriers "if you're not going to carry more risk on your own, why do you expect me to carry it for you?"

And the cyber retro market "is not the large, ongoing, robust market you can rely on," Johansmeyer continued. "If there were robust access to retro, reinsurers might be more comfortable allocating more capacity."

Clyde & Co. partner Marc Voses agreed, saying, "Reinsurers are reevaluating their contract to make sure that they are not overexposed."

The question is not whether cyber risks are insurable, but whether the individual companies are insurable, he said. Insurance and reinsurance companies want policyholders to take cybersecurity measures seriously, and rely on insurance as a backstop instead of a risk-management tool, he added.

Over the past two years, reinsurers have reined in their supply of capital to address their profitability, and when the reinsurance supply went down that affected the primary market, said Lori Bailey, chief insurance officer at Corvus Insurance.

"In the last 12 months, we've seen this huge increase in [reinsurance] rate activity and capacity restrictions in response to this claims environment," she said.

Bailey said reinsurers historically put 10% of their capital in the cyberinsurance market, but now they may cut it to 5% and move the other 5% to other lines that are more profitable and better understood. Some reinsurers have cut back their support and decided not to offer cyber reinsurance anymore because of the uncertainty, she said.

"It's really the first time where we've seen this type of market dynamic, and reinsurers are trying to make sure that the capital that is being deployed is being priced appropriately," Bailey said.

Cyber reinsurance rates have increased more than primary cyber premiums, Dharma-Wardana said, explaining, "There is less capacity as you move higher up the risk-transfer chain."

The industry has seen a more than 150% risk-adjusted reinsurance rate change in the past year, and the retro rate changes have been even higher, according to Dharma-Wardana.

"There are only a few really large dominant cyber reinsurers that can provide meaningful retro protection to one another," the reinsurance underwriter said. "We are all becoming less and less comfortable with the growing risk accumulation, so it's getting trickier and trickier in the retro market."

She said reinsurers welcome the fact that primary carriers are reevaluating cyber risks, adding ransomware sublimits for individual insurance contracts, and requiring coinsurance for higher policy limits.

"We ask primary insurers what technologies they're using and how they're using them," Dharma-Wardana said. "We want to make sure that those tools are being used properly, not just for a show."

For instance, a cybersecurity scanning technology can provide a score, but that is not as helpful as a

qualitative analysis of a customer's risks, she said.

Reinsurers want insurers to understand ransomware risks and loss development patterns, identify which industries are most impacted, and link different policy limits precisely with risks, said Erica Davis, global co-head of cyber at reinsurance broker Guy Carpenter, a subsidiary of insurance broker giant Marsh McLennan.

Huge Opportunities and Uninsurable Risks

The existing dominant cyber reinsurers, those with the largest standalone cyberinsurance portfolios, are recognizing the market opportunity and increasing their cyber reinsurance support as much as possible, industry experts say.

"If insurers and reinsurers shy away from the cyber market, they will not survive," Stefan Golling, a member of Munich Re's board of management, said during a virtual presentation at an industry conference last month.

While Munich Re wrote only about $150 million in cyberinsurance and reinsurance in 2014, Golling reported that the reinsurer's cyber premium volume is set to soar past the $1 billion mark in 2021. Last year, Munich Re wrote $850 million in cyber premiums, with roughly half of the total in primary insurance and half in reinsurance, Golling said.

Research from publisher Cybersecurity Ventures shows that global economic losses from cybercrime amounted to $6 trillion in 2021— double the $3 trillion figure registered in 2015. While only $20 billion of the $6 trillion is attributed to ransomware, ransomware losses actually increased by more than 50 times from 2015 to 2021.

The $20 billion in economic losses from ransomware is more than "the size of the cyberinsurance market for the next couple of years," according to Golling.

On the other hand, reinsurers like Munich Re have sent out clear messages that evolving cyber risks such as cyberwars and systemic risks are not insurable. Systemic risks are aggregated losses experienced by multiple institutions during one incident. That kind of exposure would require carriers to respond across many different industries at one time.

Dharma-Wardana said the insurance industry is paying close attention to the development of systemic risks and finding ways to contain and potentially exclude them. The reinsurance underwriter said the hard insurance market, increasing demand for cyber risk protection, and supply shortage have made it easy for reinsurers to tighten policy language and add in infrastructure, war, explosion, pollution and natural catastrophe exclusions.

"Historically, primary insurance wording tries to match that of reinsurance contracts and major exclusions actually came from the reinsurance side," she noted.

Golling said in September that "the topic of cyberwar is presumably not addressed enough," indicating that uninsurable cyberwar and cyberterrorism risks are not addressed by clear exclusionary language in cyber policies.

"Munich Re has engaged with clients and other industry working groups — such as the Geneva

Association and the London Market Association — to support the development of specific cyberwar exclusions," Ashleigh Lockhart, Munich Re's spokesperson for the Americas, told Law360.

Lockhart said the reinsurer is "taking an active role to ensure that any new clause addresses its areas of interest, notably impact and attribution, and is hoping that a market standard will emerge soon."

The current war exclusions in cyber policies preclude coverage for cyberattacks sponsored by nation-states. However, a commercially motivated cybercrime could also be state-influenced. Yet without showing a direct link, insurers may not be able to deny coverage, experts say.

The insurance industry is "evaluating the use of war exclusions that provide greater clarity to both sides, cyberinsurers and policyholders," Voses of Clyde & Co. said, adding that he anticipates an increase in disputes surrounding the current iteration of the war risk exclusion.

Dharma-Wardana agreed that there are a number of thorny questions regarding the war exclusion.

"With the war exclusion, attribution is a challenge because you have to prove that it was an act of war," she said.

--Additional reporting by Ben Kochman. Editing by Breda Lund.
