FPN FRONT PAGE NEWS | CYBER EDITION

Advisen Cyber FPN - Friday, October 27, 2017

Greed is overtaking fear in the market': Has the cyber insurance market overextended itself?
By Erin Ayers, Advisen

The cyber insurance market has grown steadily in response to market demand and rising risk, but some question whether insurers underestimate potential losses when underwriting and pricing business.

A recent report from Cybersecurity Ventures predicted the global cost of cybercrime to rise to $6 trillion by 2021, up from a 2015 estimate of $3 trillion. Direct written premium in the cyber insurance market rose to $1.35 billion in 2016, according to an A.M. Best report, with a loss ratio of 46.9 percent.

While cyber insurance has proven profitable for insurers, broadening of coverage, changes in exposure, and some decreases in pricing for cyber.

“Greed is overtaking fear in the market,” said Brad Gow, global cyber product leader for Sompo International, in an interview with Advisen. “Everybody wants a piece of the hot line. We’re seeing a feeding frenzy of deals.”

Gow explained that the elimination of sublimits for coverages like business interruption and contingent business interruption, along with more interconnectedness and cloud-based exposures, have rapidly ramped up the exposure for the insurance industry. He estimated the industry has “well north of $100 billion in limits extended” through coverage grants.

“I see a lot of similarities to the property market of 25 years ago, when Hurricane Andrew blew through,” said Gow, noting that one storm wiped out all the cumulative profit amassed by the property insurance industry. “The possibility exists for the exact same thing to occur in cyber. I think as an industry, we’re opening ourselves up to some sort of cascading failure.”

He added, “The market is pricing for attritional losses like data breaches.”

Insurers acknowledge the risk they – and their clients – face. Underwriters are paying closer attention to interconnectedness in client risk assessments, hoping to manage aggregation. In recent conversations with Advisen, insurers expressed confidence in their market offerings, while hoping for a pricing upswing.

Nick Economidis, E&O underwriter for Beazley, likened the situation to the Great Chicago Fire of 1871, when raging flames destroyed much of the city over two days. A cyber version of the Chicago catastrophe affecting many insured organizations could have a chilling impact on the insurance market.

“We certainly all worry about the Chicago Fire situation. We haven’t seen it manifest itself,” said Economidis. “We all believe we’ve done the right thing to insulate our books.”

Cyber pricing has been dropping, “not dramatically, but not nominally,” John Coletti, chief underwriting officer for cyber and technology of XL Catlin, told Advisen. That approach may not be the best one for the industry.

“It doesn’t make a whole lot of sense to reduce pricing when the market is still pretty volatile,” said Coletti.

With cyber risks evolving every day, there is vast uninsured potential across the globe and the market could be bolstered with additional capacity. All capacity isn’t positive, however. Coletti commented, “The markets need to be in it for the long haul. They need to go into it with eyes wide open, with a view toward building a sustainable market. If it’s capacity that’s just going to come in and copy everyone and suppress pricing, no. Markets that come in need to be responsible, creative, and innovative.”

The cyber insurance market got a taste of the potential for rapidly escalating claims scenarios over the last few months, with the WannaCry ransomware attack in May and NotPetya in June. The latter shut down several high-profile organizations, creating extended operational delays.

The numbers associated with a “true zero-day exploit” would be “surprising,” according to Gow, who added that cyber underwriter “could stand to learn quite a bit from their property brethren” on business interruption. “They’re far more conservative than the cyber market is for the same risk,” he said. Waiting periods for cyber-related business interruption range from a few hours up to 48 hours – many of the organizations affected by NotPetya experienced downtime for weeks after the event.

Asked if he felt the market would correct any time soon, Gow responded, “If history is a guide, not until the market experiences a significant amount of pain. And that pain will be widespread through a number of the major and the minor carriers.”

Editor Erin Ayers can be reached at eayers@advisen.com.