Are Cyber Limits Sufficient? It Depends

By: Kevin Kalinich | May 31, 2016

Kevin Kalinich is the global cyber risk practice leader for Aon Risk Solutions, focusing on identifying exposures and developing insurance solutions. He can be reached at riskletters@lrp.com.

Several cyber insurers recently announced new cyber facilities with up to $100 million limits per placement and additional new cyber capacity.

This has increased the generally available stand-alone cyber limits from traditional insurance carriers from approximately $200 million to approximately $300 million for most organizations in most industries.

Add in the potential reinsurance capacity for some large organizations seeking catastrophic coverage and we're looking at $500 million to $1 billion cyber insurance programs.

2016 studies indicate dramatic growth in cyber insurance purchases, including small, middle and large revenue organizations.

We are seeing small entities purchase $1 million, $3 million or $5 million as first-time buyers, and middle market and large organizations increase cyber limits from single layer $10 million and $20 million *limit* policies to multi-layer programs.

There are over 67 different cyber insurers with 67 different applications, submission processes, underwriting, policy forms and claims handling processes.

However, 92.5 percent of organizations that purchase cyber insurance buy less than $100 million limits and less than 5 percent are willing to consider paying the going premium rate excess of $300 million. Therefore, current capacity satisfies more than 95 percent of the current cyber insurance environment.

Is There Room for More Cyber Insurance Capacity?

There are more than 67 different cyber insurers with 67 different applications, submission processes, underwriting, policy forms and claims handling processes.

Most of the carriers target middle market accounts, where there is quite a bit of aggressive competition on price, coverage and limits. However, there are cyber capacity gaps in a few areas

• Large data aggregators with massive personally identifiable information, including personal health records, such as retail, health care, financial institutions and hospitality (hotels & restaurants, etc.);

• Organizations with the potential for bodily injury and/or tangible property damage from purely cyber perils (driverless cars, the Internet of Things-connected devices, etc.);

• Unauthorized transfer of funds via some combination of hacks (malware on a system) and social engineering (employee is tricked into sending a wire transfer at the request of an imposter CFO or CEO), such as the Bank of Bangladesh heist via the Federal Reserve of New York;

• Industries where business interruption is of greater concern than breach of personal information, such as transportation, agribusiness, energy, utilities, power, and manufacturing; and

• Industries where the **value** of the lost information is most critical, which is generally **excluded** from today's cyber insurance policies, such as law firms (think Mossack Fonseca breach), investment banks involved in mergers & acquisitions, defense contractors and research labs.

A few insurance carriers realize the future success of cyber insurance depends upon more creative solutions that combine the capacity and damage cover offered under property, general liability, crime, and kidnap and ransom policies, with the underwriting expertise of cyber insurance.

A number of entities are building actuarial models and cyber resiliency best practices rating assessments, which will facilitate the acceleration of the cyber insurance market.

However, it is important that insured organizations and cyber insurers understand a few important items prior to jumping in, including identification and quantification of the unique cyber exposures facing each specific organization; modeling, financial statement impact and priorities and risk appetite of the insured (i.e., smoothing of earnings, ERM).