INSURANCE JOURNAL

Cyber Insurance Underwriting Moves from 'Toddler' to 'Teen' As Insurers Learn from Claims

By Stephanie K. Jones | December 8, 2015

Given the fact that the insurance industry paid out more than $400 million in highly publicized cyber liability insurance claims in 2014 alone, one might think that insurers would be shying away from the line.

But one would be wrong, according to insurance professionals who specialize in cyber-related risks.

"The interest in cyber is phenomenal right now. It's never been hotter. This is a product line that's been around for only 15 years. It feels like now it's reached that stage of maturity where we're seeing more and more buyers, we're seeing more and more market participants, and everybody's talking about cyber right now," said Graeme Newman, a director at CFC Underwriting in London.

In an interview at the PLUS Cyber Liability Symposium in Chicago in September, Newman said the cyber liability line has moved from the "toddler stage" to its "teenage years." The difference between now and, say, five years ago, claims are starting to come in and they are being paid, he said.

The year 2014 with its headline generating claims was extraordinary, Newman said, because the market "at that stage was probably less than a billion dollars in net premium."

> The thing about claims, though, is that the market is learning from them, and reevaluating their products and pricing models.
>
> "We're seeing how the insurance market is reacting … how coverage is changing. We're seeing new entrants come in. We're seeing some people leave. The interesting thing is going to be how it develops over the next 12 to 24 months," Newman said.

Going forward, insurers will necessarily have to make underwriting and pricing adjustments for the cyber market to remain viable, according to Sarah Stephens, partner and head of Cyber, Technology, and Media E&O at JLT Specialty Limited.

> The cyber line is "sustainable, but not if we continue to drive pricing down to the lowest common denominator, and not if we don't underwrite risks. There definitely was a point in the last few years, where you could get a cyber quote with no information," Stephens said.
>
> "It doesn't seem sustainable to me to do it that way. Insurers have swung the pendulum a little bit back, to actually asking for detailed information, and really trying to differentiate a good risk from a bad risk. They'll continue to do that."

Carriers expect this area to grow, said Manny Cho, regional underwriting manager at Axis Pro in San Francisco, but they need to be profitable in order for that to happen.

> He said in the marketplace today there are a "few very good primary underwriters for large accounts that really have the expertise and the experience to know what to ask for, and look for."
>
> Carriers are "picking and choosing the different areas that we feel most comfortable with," Cho said.

Growth Areas, New Markets

Historically, the cyber market has focused on healthcare companies, financial industries and more recently, retailers, Newman said. Now, "the market has started to develop and mature in those industry verticals," he added.

But Cho, Newman and Stephens all agree there is a lot of room for market growth both among tradition types of buyers and in new market sectors.

"I would say right now, there's a massive amount of growth in the U.S., even in industries that are traditional buyers. If you think about retailers and healthcare and financial institutions, still not 100 percent of them buy [cyber] insurance," Stephens said.

"And then there are the non-traditional industries, such as heavy industry, mining, manufacturing, transportation, energy," she said.

Newman said he also expects to see new buyers seeking the coverage — "everything from manufacturing, professional services companies, logistic companies, aviation, marine. I think we're going to see a huge number of new buyers entering the market, because the product is changing, and it's adapting."

Five years ago, the products being sold "were all about privacy breach response, and that's where the market started and it grew," he said. "Now we're seeing products develop around the business interruption components, the system damage elements, and that makes the product so much more appealing to a much, much wider spread of customers."

Another potential growth area — the global market — is virtually untapped, according to Stephens, who is based in London and works with many companies in the U.K. and in Europe.

"Probably only about 10 percent of the world's cyber premium is outside the U.S. There's a massive opportunity for growth there," she said. "Especially in Europe right now, because we've got a new EU data protection regulation that's going to be coming into effect at some point later this year. Then it will have about a two-year horizon before it really starts to affect companies."

A lot of companies are also starting to think about protection beyond data breach, as well. "You're now starting to see companies, in non-traditional classes and also in traditional classes think, 'Actually, I'm really dependent on technology. What if I didn't have email? What if my logistics system went down and I couldn't ship product?'" she said.

"They're thinking about that business interruption component, from either a cyber-attack, or the more broad system failure coverage. … That's going to drive even more growth," she said.

Cho said many carriers are also looking at small and midsize business as a robust area for growth. We are trying to "figure out if we can underwrite it effectively, if we can price it effectively and build our books on that segment," he said.

With the small to midsize company market there are some real inhibitors, Cho said. The main one is cost.

"If you're a small to midsize business owner with a limited budget, every dollar counts," he said. "When I was on the broker side … we would always try to talk about it in practical terms: 'If you have a PCI violation, what does that mean to you?'"

It may cost the client $10,000 to $25,000 for a forensic investigation. There could be an assessment charge, perhaps another $5,000 or $10,000. It may be a modest breach but it may cost the business $25,000 to resolve.

Can the potential insured afford to pay 25,000? Do they "have that kind of margin where that money is laying around? Most will say no. You just equate that to a $2,500 cyber insurance policy or $1,500 cyber insurance policy. Let them manage the risk or make the decision from there," Cho said.

He conceded it's very difficult.

"There's always the argument, 'That's not going to happen to me.' Then it happens and then [they] go, 'Oh my gosh! I should've done something,'" he said.

Cho said it's likely more insurers will start to offer "add-ons to just give someone a taste for what the cyber coverages is or give some critical first-party coverages, reimbursement coverages. Maybe if they want to buy more, they'll build on top of that. That may be another way small and midsize businesses can grow that segment and for carriers to grow the segment."

Related:

Cyber Insurance Rates Up, Unlike Other Commercial Rates

NAS' Palotay: Point-of-Sale, not Stored Data, Riskiest for Retailers

Just How Costly, Fast-Growing Is Cyber Risk?

Agent, Cyber–Educate Yourself — and Your Clients

Where Cyber Insurance Underwriting Stands Today

Target's Cyber Insurance Softens Blow of Massive Credit Breach

Note: This article originally appeared in Dec. 7, 2015, Insurance Journal Midwest and South Central editions. View video interviews with Cho, Newman and Stephens at the PLUS Cyber Liability Symposium at www.insurancejournal.tv.