FPN FRONT PAGE NEWS | CYBER EDITION

Advisen Cyber FPN - Friday, July 3, 2020



Advisen

# Cyber insurance has a ransomware problem. The solution may be 'old-fashioned loss control'

By Erin Ayers, Advisen

The cyber insurance market remains healthy, but increasing claim severity and frequency will lead to higher rates as well as an imperative for the industry to help insureds reduce risk and understand the value of their coverage, according to experts speaking during NetDiligence's Cyber Risk Summit this week.

While there have been both new entrants to and some exits of insurers from the cyber sector, the market is showing longevity and achieving stability, said Dan Trueman, global head of cyber for AXIS. Insurers are also paying claims, he added.

"We're certainly paying losses," Trueman said. "And it's certainly important to have a market that pays claims accurately and quickly."

Severity has been a fact for the market for some time, but claim frequency is now increasing too, he added.

Just a year ago, the cyber market was "going full guns" and very competitive, according to Nick Economidis, vice president with Crum and Forster. With ransomware claims rising and impacting the industry loss ratio, the market is changing, he said.

"I think the market may look a lot different in another year if losses continue to develop and I think we may see some people backing away from the market," he said.

John Coletti, chief underwriting officer for cyber and technology at AXA XL and moderator of the panel, noted when rates were set for cyber policies, "ransomware wasn't on anyone's mind." The substantial uptick in claims has underwriters and actuaries worried.

"When you have a ransomware event on a Friday and you've tendered your limit three days later, it's a pretty frightening phenomenon," he said.

Ransomware presents a significant challenge for cyber insurers, noted Shannon Groeber, executive vice president of CFC Underwriting. Ransomware doesn't differentiate by industry or size of business, resulting in a broad impact amid the proliferation of attacks.

“It’s very, very important we continue paying claims in this area,” she said. “We are going to continue to see the impact of this, and if we do intend for cyber insurance to be a sustainable market and to be a mainstream product, our business is in paying claims so we have to do so in a way that make sense for our insureds.”

The panel dismissed the idea that insurers promote bad behavior by paying ransoms or that legislation is needed to prevent payment of ransoms.

“There’s a little truth to it, but there’s also a little unfairness to it,” said Economidis. “It may be inflating the cost of ransomware, but I don’t think it would make the problem go away if the insurance wasn’t available. If anything, the bad actors might look for smaller amounts.”

“It’s just such a narrow view of what cyber insurance is doing in response to these claims,” said Groeber. “Look at the breakdown of losses. Sure, we might be paying a few thousand bitcoins reimbursement in some scenarios, but we are covering far more for our clients. To respond to that with a knee-jerk reaction ignores all the value that carriers are providing to their insureds when they’re faced with this very real threat.”

Trueman said complaints that insurance drives ransomware is part of the “fundamental PR problem” for cyber insurance, recalling the times when cyber insurance was accused of not paying claims.

“Now we’re in a situation where we’re paying claims, to actually then blame the market for causing those claims is at best ludicrous,” he said.

**Focus on loss control**

According to Trueman, the industry needs to ensure that it offers value as a market, not solely by paying claims, but by holding clients and the industry to higher cybersecurity standards.

“I don’t think frankly we’re asking the right questions often enough,” he said, adding that insurers need to engage more proactively with vendors and following up after claims. Insurers will also likely need to improve its pricing practices to provide better rates to insureds that take the right security steps.

“I don’t think this insurance class is ever going to be cheaper than it is today if we’re seeing both more frequency and severity,” said Trueman. “We’ve got to differentiate our pricing better …. We’re pricing on limit as opposed to security and capability.”

The panel discussed whether sublimiting ransomware would be a solution. Economidis said that wouldn’t be a good approach, since the vast majority of ransomware losses are under $2 million, with many under $1 million.

“The market will demand at least $1M sublimit, in which case, we’re largely already paying the claims already,” he said, adding that the solution is to instead help insured implement better loss control.

Economidis expressed frustration with municipalities – a market that had low cyber insurance premiums that has been hit with many ransomware claims.

“It’s been really difficult to find a way to communicate to the buyers the things they should be doing to prevent a loss,” he said. “I think good old-fashioned insurance loss control services could go a long way for us.”

According to Groeber, analyzing claims that occur and “providing relevant feedback and information, not just judgment” to insureds. While she explained that the idea of requiring the use of value-added services as a condition of coverage is a “very dangerous, slippery slope,” but the industry should highlight those services as a key feature.

“All of these additional services need to be explained and presented to an insured where they can see the value of embedding it into their daily activities, and not necessarily something that’s plastered on a marketing sheet and then just gets ignored,” she said. “The push is to make sure the insureds recognize how valuable that would be versus just relying on an insurance policy when something bad happens.”

*Editor Erin Ayers can be reached at eayers@advisen.com. Want to subscribe to Cyber Front Page News? Click here!*