RISK & INSURANCE
Affiliated with THE INSTITUTES
Sponsored Content by Pinnacle Actuarial Resources, Inc.

Cyber Insurance or Cyber Captive?

Pinnacle Actuarial Resources' Aaron Hillebrandt advises caution for those engaged in managing cyber risk—even those seeking a captive solution, given the unknowns and volatility associated with the cyber insurance market.

By: Pinnacle Actuarial Resources, Inc. | July 2022

Insurers and risk managers expecting relief from escalating cyber insurance premium increases may want to temper their expectations.

According to Pinnacle Principal and Consulting Actuary Aaron Hillebrandt, the cyber risk landscape continues to be extremely complicated, even murky. It's difficult to know if the insurance industry is getting a full and complete picture of the number and severity of cyber breaches or ransomware attacks.

In addition, price increases for coverages are continuing to increase, so anyone seeking to purchase coverage, start a captive to manage cyber risk, or self-insure for cyber losses should tread carefully.

Not only are premiums continuing to spike, but research from organizations specializing in cyber are delivering divergent results on the details of losses, including number and scope of losses for companies in a variety of industries.

Remote work became much more prevalent for a large section of the workforce during the COVID-19 pandemic. It stood to reason that less technologically secure remote work arrangements could, theoretically, increase cyber risk and attendant losses. According to IBM's Cost of a Data Breach Report 2021 featuring research from the Ponemon Institute, concerns about those arrangements appear to be well-founded.

According to the report, the average cost of a breach for companies with less than 10% of their workforce working remotely was $3.65 million. For companies with 81 to 100% of their workforces working remotely, that cost averaged $5.54 million.

Aaron Hillebrandt, Pinnacle Principal and Consulting Actuary, Pinnacle Actuarial Resources, Inc.

That same report stated that companies with less than 50% of their workforce operating remotely reported requiring an average of 258 days to identify and contain a breach. Companies with more than 50% of their employees working remotely needed an average of 316 days to identify and contain a breach.

Could it be that the companies encouraging remote workers to return to the office in 2022 are most concerned with cyber security risk?

Hillebrandt confirmed that the frequency and severity of cyber incidents increased as the COVID-19 pandemic pushed so much of the workforce into work-from-home situations.

"The influence of remote work accelerated cyber claims trends and exacerbated conditions associated with greater cyber risk," Hillebrandt said.

The Pinnacle team has also documented what many underwriters have experienced, some more acutely than others. Cyber insurance premium rates have been inadequate for quite some time and are likely still inadequate.

"Several years ago, research indicated that pricing levels were lower than where they should have been. The industry seemed to be racing, competing to write more cyber policies, depressing pricing," he said.

"Subsequently, the claim situation reversed, with increasing frequency and severity. Consequently, there is much more ground needed to be made up to get premiums to an adequate level. I think we're still not there yet," he added.

"That's why pricing is accelerating so much now," he said.

Is It Time to Form a Captive?

With premium prices increasing, one might be tempted to form a captive to help manage the risk, but Hillebrandt again urged perspective. Seasoned underwriters are having difficulty mitigating cyber risk, so it should be expected that captive management teams would face similar and familiar challenges.

The overarching issue is that cyber is a sizable insurance market, and it is relatively new. There just isn't enough good data and loss experience to properly underwrite the risk.

"It's not every day a new, major insurance line emerges," said Hillebrandt.

"Cyber is, of course, still emerging and evolving. But whether or not it's a new insurance line, so much in cyber

is conditional — it is dynamic and changing, and that is driving the number and nature of the claims that insurers are seeing," he added.

If considering a captive, one should consider that major insurance companies, with assets far beyond the amounts held by most captives, are better able to absorb the volatility of losses in the cyber market.

"If preparing a captive feasibility study, it is important that managers understand fully the kinds of limits under consideration," Hillebrandt said.

A captive owner considering insuring cyber risk will need to make sure that they have an adequate amount of capital backing the effort, not just for year one, but for scenarios in which some years' losses could be significantly worse than others.

That being said, Hillebrandt said some companies are being practical in exploring the captive route, given the difficulty of the commercial cyber insurance premium and underwriting environment.

"Some people may not have a choice because they can't get their commercial cyber insurance policy renewed," he said.

"Others may get it renewed, but it's triple the price which makes a captive solution more attractive," Hillebrandt said.

"Our message is not to be casual or indeliberate about it," Hillebrandt continued.

Cyber is a volatile risk and risk managers and their risk management partners need to understand what a bad year might look like and ensure they have adequate surplus available in their captive should they experience, if not a worst-case scenario, a substantial loss.

A bright side is that the premium that would be paid to a carrier stays in-house.

"The silver lining is that if you put it into the captive and you do have a good year, and you don't have any cyber claims, then the profit remains in the captive," Hillebrandt said.

It may be difficult to predict where things are going from a loss perspective, but, again, the picture is cloudy and complicated.

Hillebrandt pointed to recent commercial rate filings from major carriers.

In 2017, one major cyber writer showed a trended ultimate loss and allocated loss adjustment expense (ALAE) ratio of 37.2% in its cyber insurance line. In 2020, that loss ratio had risen to 97.6%. The company

had a somewhat less difficult time in 2021 but its cyber insurance loss ratio still stood at a difficult 88%.

The cyber security firm NetDiligence calculated the average cost of a breach in 2018 for companies with more than $2 billion in revenue at $2.9 million. In 2019 that average incident cost grew to $5.9 million and in 2020, stood at $10.4 million.

Looking at steadily rising premiums and steadily rising losses, Hillebrandt said, "It's similar to bailing water out of a leaky boat. The boat will continue to fill up until the hole is fixed. Assuming or thinking things may improve doesn't necessarily make it so. That seems to be the immediate future for the cyber market.

"If you're considering different avenues to manage the risk – say, forming a captive, waiting may be an unaffordable luxury. It may be a while."

For more information, please visit Pinnacle Actuarial Resources at www.pinnacleactuaries.com.

&BrandStudio

This article was produced by the R&I Brand Studio, a unit of the advertising department of Risk & Insurance, in collaboration with Pinnacle Actuarial Resources, Inc. The editorial staff of Risk & Insurance had no role in its preparation.