INSIGHTS
RISK & INSURANCE

Four Critical Questions Insurers Must Address before Writing Cyber Coverage

Milliman

The ever-evolving cyber insurance market creates both challenges and opportunities for risk managers and brokers.

Ask any broker or risk manager what risks concern them most, and "cyber" is bound to be in the top three. Insurers are rapidly responding with new products to provide the protection their clients' need, but the amorphous and ever-evolving nature of cyber exposure poses a constant challenge.

Despite the uncertainty, plenty of opportunity exists in the cyber market… as long as insurers stay aware of the hazards.

Below are four critical questions all insurers must answer before offering cyber coverage:

1. What is the current state of the cyber market?

Tom Ryan, principal and consulting actuary at Milliman, describes the cyber insurance market as both "crystalizing and diversifying."

"There are at least 40 different policy forms in use right now for cyber liability," he said. "It's like comparing apples to oranges to kumquats. However, Insurers are now in the process of smoothing out the wrinkles and developing some standardization of language and coverage."

Tom Ryan
Principal & Consulting Actuary

This "crystallization" phase will set expectations for both carriers and insureds for what should and should not be covered under a cyber policy and will build a foundation for future development of the coverage. Most of those decisions are playing out now in courtrooms and claims departments as disputes arise.

Ryan compared this process to the roots of a tree growing underground, while the "diversification" phase is analogous to its branches.

"Every industry has a unique cyber exposure, so specialized policies have to be created to meet those needs," he said.

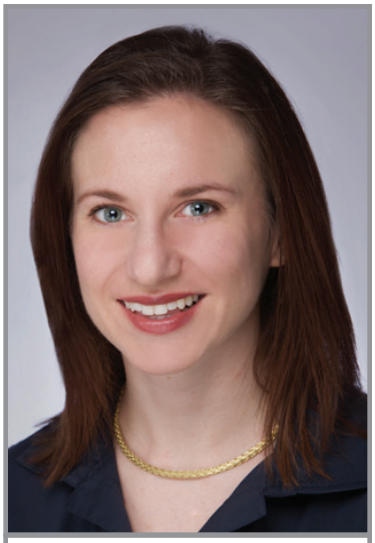
As policy wording becomes sharper and more standard across the industry, underwriters will adjust policy structure based on those unique needs, creating a "branch" for each industry.

2. What are the biggest challenges to writing cyber coverage?

Due to a lack of historical loss data, pricing proves the most difficult challenge for carriers.

"Actuaries describe pricing as more of an art than a science," said Elizabeth Bart, a consulting actuary with Milliman. "We like to see how losses develop over time, but cyber liability is so new and is changing so quickly that there hasn't been time for that to happen."

Additionally, most companies don't like to disclose when they've had a breach, so it's difficult to build aggregate cyber loss databases for insurers to reference.



Elizabeth Bart
Consulting Actuary

Without full disclosure, actuaries are hard-pressed to calculate the total cost of a loss because the estimates can come from multiple departments within the company and vary widely. IT specialists might see the costs associated with enhancing security of internal systems; the public relations team might think of the cost of launching a campaign to defend reputation after a breach; and the legal department might fear the potential of a lawsuit.

"The NAIC and ISO are starting to put together aggregate loss databases for cyber, but it won't be usable for some time," Ryan said. "The NAIC now asks insurers to disclose the number of cyber policies it writes, as well as premiums and losses, but it will take several years for all of that data to reveal meaningful trends."

Potentially massive aggregate risk also complicates efforts to accurately identify and quantify cyber exposure.

"You might be underwriting 30 different companies, but those are not 30 different risks," Ryan said. "If they are all using the same cloud service and it goes down, for example, you could be facing a claim from each insured relating to the same event, creating an astronomical loss."

Fitch Ratings and other agencies expressed concern that cyber insurers are biting off more than they can chew by not accounting for this aggregate risk.

Until more data becomes available, "pricing is based mostly on benchmarking against other carriers, or based on knee-jerk reactions to big breaches at major retailers and health care organizations," Bart said.

"We just looked at a company that was writing $1 billion in limits and collecting $2 million in premium," Ryan said. "Is that a good bet?"

Insurers should lean on their actuarial partners to find the best relevant data that most closely matches an insured's business to determine what their exposure is and what policy limits are appropriate.

3. How can insurers help to mitigate the risk of a catastrophic loss?

Insurers benefit by going beyond coverage and offering risk management tools and services to their insureds.

"Some carriers are getting really savvy about cyber. They want to avoid the losses as much as their insureds do," Bart said. "So they get the right people in the right place. The right lawyers, the right PR team, and the right IT vendors."

"We are seeing a lot of experts come into the insurance industry with knowledge of the hardware and software components of internal systems," Ryan said. "They have a better understanding of how hacking happens."

Aside from IT security, experts can also help insureds' train their workforce to spot and prevent less overt attacks, like phishing scams.

"This is increasingly the most common type of attack," Bart said. "Everyone should be trained to spot a fraudulent email."

Carriers can also provide professionals to thoroughly vet an insureds' vendors and determine whether they have too much access to a company's internal systems, and whether that access is secure.

4. What challenges lie ahead for the cyber market?

The burgeoning Internet of Things will complicate cyber risk and insurance as more and more devices become "smart" and connected.

"By 2020, estimates are that there will be 100 billion devices linked up to the internet, and each one is a possible attack target," Ryan said. This interconnectivity will also blur the lines between personal and commercial insurance.

If, for example, a smart home system that links everything from lights to the security system gets hacked, allowing robbers to shut down

security and break in undetected — is that a cyber issue or a product liability issue? Does the exposure fall on the consumer, or the manufacturer of the product?

"Additionally, the more devices I have and the more passwords I need to remember, the more likely I am to use the same password over and over," Bart said. "This increases my exposure and will challenge cyber insurers to come up with more innovative security solutions."

The threat of a cyber "Black Swan" event also looms. With more businesses relying on cloud computing to share information, the risk of a massive loss arising from a single breach grows larger, but the industry has not yet developed a solution.

"Right now, a cyber Black Swan could take a lot of insurers out of the business. It would be a huge disruption," Bart said. "It's a question of what will happen first: will underwriters collect enough data to master cyber coverage, or will a Black Swan force them to exit the cyber market?"

Commercial insurers could also face challenges in the future from cyber captives and pools, which many organization may turn to as a way to spread out their risk and better control their coverage.

For more information about Milliman's services for the insurance industry, visit http://us.milliman.com/us/solutions/insurance/.

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