Privacy & Data Security Law

Cyber Insurance Policies Grow Pricey Amid Rising Hacks, Lawsuits

By Jake Holland

Deep Dive
May 31, 2022, 5:31 AM

- Insurance becomes costlier, harder to get for businesses
- Companies turn to courts to argue policies apply to them

An uptick in data breach litigation and skyrocketing costs tied to ransomware attacks and other cybercrime are making it more difficult—and more expensive—for companies to secure insurance policies that help them cover financial hits.

The changing insurance market and disagreements over policy exclusions are also driving legal uncertainty, leaving businesses and policy providers to duke it out in court over who's responsible to pay for what, attorneys say.

"Too often there's a disconnect between what companies think a policy may cover and what's actually covered," said Michael Phillips, chief claims officer at Resilience, which provides cyber insurance policies and integrated cybersecurity solutions.

Many businesses turn to insurance as a means of guarding against loss. But smaller entities might not even know such coverage exists or face difficulties in acquiring it, said Iliana Peters, an attorney at Polsinelli PC in Washington, D.C.

"Coverage isn't as easy to get as it used to be," Peters said. "Before they offer or renew a policy, insurers are requiring a lot more from businesses."

Changing Market

An April report from Fitch Ratings found that "cyber statutory direct written premiums" rose by 74% in 2021 to nearly $5 billion. The property and casualty insurance industry overall grew by 9% during that same period, according to the report.

That increase is being driven by "heightened policyholder risk" and a greater demand for coverage, the report noted.

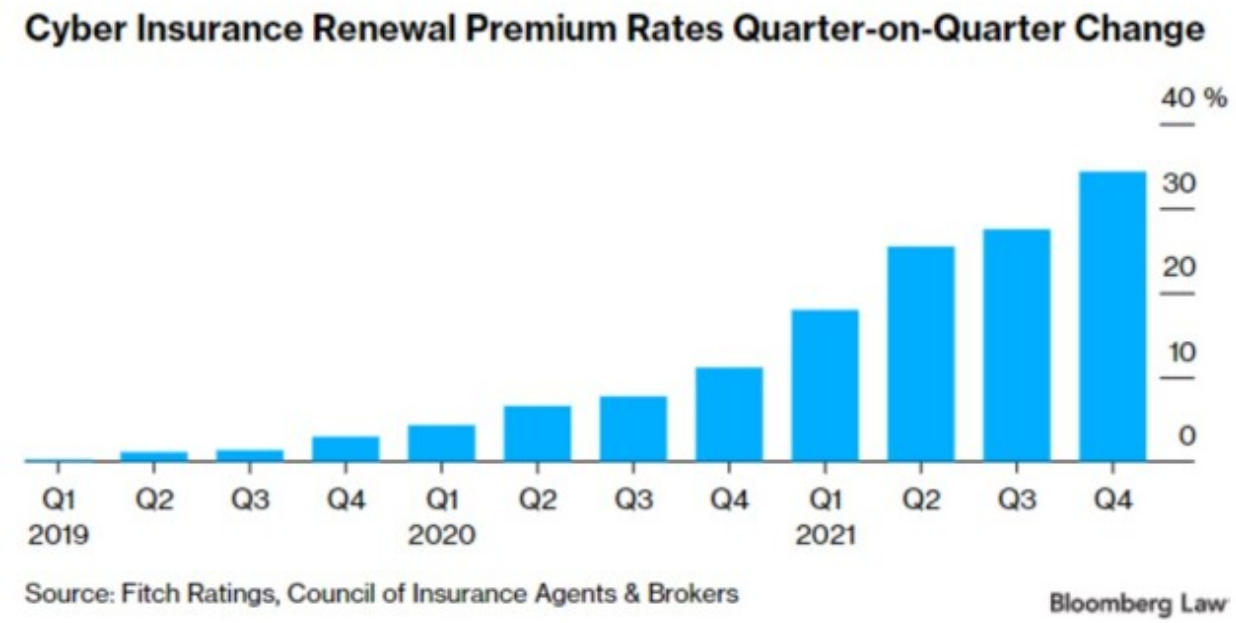
Rising “loss costs” and litigation stemming from cyberattacks are part of the reason why prices are going up, said Gerry Glombicki, senior director of insurance at Fitch Ratings.

“Cyber insurance is less than one percent of the overall market,” Glombicki said. “But it’s growing at a much higher rate than other types of insurance.”

Renewal premium rates in the space have been growing each quarter since 2019, he added.

In addition to raising prices, policy providers are also requiring companies to meet certain security standards.

“Insurers may now require from companies a broad application of multifactor authentication, endpoint detection, multiple backups, and disaster recovery plans,” said David Derigiotis, corporate senior vice president at Burns & Wilcox, an insurance wholesale broker and underwriting manager.



Coverage Disputes

Disagreements over insurance coverage have led some companies to sue their policy providers, asking courts to force them to cover the costs of remediating a hack or defending a related lawsuit. Likewise, insurers have brought litigation to absolve themselves of responsibility.

Court decisions have turned on policy types and policy language—plus exclusions.

In one instance, the US Court of Appeals for the Ninth Circuit ruled against the Insurance Company of the State of Pennsylvania, which argued it didn’t have to defend Landry’s Inc., a restaurant and casino conglomerate, in data breach litigation.

The Ninth Circuit found that the insurer had a duty to defend Landry's because the payment processor who sued it sought damages arising out of the "oral or written publication" of material violating someone's privacy.

That overruled the district court's holding that the data breach wasn't a "personal and advertising injury," as defined under the insurance policy, and that the damages in question weren't "privacy" damages.

There's often a misunderstanding among buyers, who may think that a general liability insurance policy covers something like biometric privacy litigation, Phillips said.

Even some cyber insurance policies only cover costs stemming from a cyberattack or data breach, Phillips said. An Illinois Biometric Information Privacy Act lawsuit focused on a company's failure to secure consent before collecting fingerprint scans, for example, wouldn't be included in that definition since it's not related to an attack or breach of security.

Wrongfully collecting biometric data or storing it improperly can lead to expensive litigation, but those lawsuits generally aren't covered by general liability insurance policies and cyber policies focused on cybersecurity, Phillips said.

Illinois courts have grappled with this type of issue in recent months, siding with both policy providers and businesses depending on the specific provisions of their insurance agreements.

Buying Policies

Securing a good broker who knows your company's priorities and needs is key to getting connected with the appropriate insurer, Peters said.

But businesses should also recognize that securing coverage isn't a one-size-fits-all approach, said Kamran Salour, a partner at Troutman Pepper Hamilton Sanders LLP in Irvine, Calif.

"Some cyber policies, based on premiums and coverage, might not make the most sense for a company," Salour said. "From a deductible standpoint you want something that's workable, and you want to make sure you're working with a carrier that you know and trust and have a good relationship with."

In some cases, deductibles are low, but so too is coverage. Finding that "sweet spot" is critical for companies as they seek to maximize coverage and minimize expenses, Salour said.

Companies need to keep a close eye on policy language, since insurers will often put exclusions for BIPA in employment practice insurance policies, Derigiotis said.

"At this point, given the number of lawsuits, companies need to be taking a closer look at potential biometric privacy risks and insurance policies that could help shield them from associated costs," Derigiotis said.

To contact the reporter on this story: Jake Holland in Washington at jholland@bloombergindustry.com

To contact the editors responsible for this story: Jay-Anne B. Casuga at jcasuga@bloomberglaw.com; Adam M. Taylor at ataylor@bloombergindustry.com