BLOG

Cybersecurity Exclusions in a Hardening Insurance Market

By Robert H. Rosenzweig, RPLU, National Cyber Risk Practice Leader

Jul 17, 2020

Back in February, when the DOJ announced that the Chinese government was behind two of the largest data security breaches of American companies in history — the Equifax breach of 2017 and the Marriott breach of 2018, it rattled the cyber insurance market.

In a cyber insurance market that was already beginning to see movement toward restricted coverage and narrower scopes of exclusions, this development gives carriers ammunition to tighten restrictions even further by limiting coverage if a cyber breach is determined to be state-sponsored or declared an act of war. Companies should prepare for cyber policies to become less favorable than we've seen in recent years.

To this day, the Equifax breach was one of the most expensive security breaches in US history. It's estimated to have cost the company close to $700 million in settlements and fines as well as an additional $449 million in remediation efforts. The attack exposed personal information, including Social Security numbers, of 147 million people. The Marriott data breach came a year later in 2018. In it, hackers exfiltrated personal data from over 500 million customers. Together, these breaches represent a staggering number of individuals whose data was compromised, having a catastrophic impact to both the insured and the insurers.

The DOJ indictment isn't the first time the US has charged members of a foreign government with cybercrimes — 12 Russian intelligence agents were charged for hacking into the DNC and Clinton campaigns as a result of the Mueller investigation. Indeed, there's been a rise in the number of private entities cyber-attacked by foreign governments around the world. But Equifax and Marriott are the largest state-sponsored attacks targeting private, commercial enterprises in the US to steal data and IP.

So, what does this mean for policy holders?

- **Focus on exclusionary language.** Over the last few years, the exclusions around an attack perpetrated by a state-sponsored actor have been written to be fairly broad and favorable to the policy holder. For example, there's currently no provision in these policies that gives the carrier the ability to claw back money paid after the fact if the breach is considered an act of war. That could

change as reinsurers grow more worried about what a massive state-sponsored attack could mean for their risk portfolios.

- **Insurers taking on less risk.** Large cyber policies are built on towers with multiple insurance companies putting up tiers of coverage (usually around $10M per tier). The first tier of coverage dictates the terms and conditions for the whole tower. But, as insurers are taking on less risk, we've already seen instances where it has become more difficult to buy excess insurance that sits above broader, more policy-holder friendly language.

Cyber insurance has been a growth market for long time and policies have generally been written very broadly. But the pendulum has swung back. Cyber insurers are starting to take on less risk and narrow the scope of their coverage.

Cyber policy holders should really focus on how insurers are crafting the wording around their war exclusion to make sure there's no restriction in coverage or claw-back if an attack is deemed state-sponsored. As the market continues to harden, it will become more important to work with risk advisors who have both the technical subject matter expertise and the market relationships to exert the necessary leverage to get results.

Find me on LinkedIn, here.

Connect with the Risk Strategies Cyber Risk team at cyber@risk-strategies.com.

Email me directly at rrosenzweig@risk-strategies.com.

TAGS:
Cyber Liability