SPECTRUM
Asset Management

Small But Growing Cyber Insurance Market

August 19, 2021

Cyber security is a growing credit risk. It is also a key component of a company's social responsibility from an *ESG* perspective. In different jurisdictions, such as Europe's General Data Protection Regulation (GDPR), companies can face penalties for failing to comply with certain standards. Nevertheless, vulnerabilities from remote work have led to a rise in the incidence of costly cyber and ransomware attacks on organizations. Ransomware, which can block access to computer systems until payment is made, often in hard to trace cryptocurrencies, can be difficult to investigate. However, organizations are improving cyber security protocols including the purchase of cyber insurance. Cyber insurance can be used to cover cyber liability and defense, costs for ransomware and to replace/restore data, and to compensate for lost profits due to cyber-related business interruption. Cyber coverage can also provide other services to enhance a company's security protocols, such as monitoring of data and systems.

Re/insurance companies are poised to be part of the cyber security solution, but the industry remains cautious given new and evolving risks. And while cyber has been one of the fastest growing lines of insurance, it is small in the context of the broader industry. Also, given the growing prevalence of cyber risks and customer demand for the product, the price for cyber insurance has been rising rapidly and with conditional terms such as requiring policyholders to implement internal security procedures to improve preparedness. Also, insurers have made strong efforts to exclude cyber risks from their traditional policies to avoid unforeseen "silent cyber" exposures.

While the global economy has become increasingly digital, property and casualty (P&C) insurers have historically protected against losses tied to tangible assets. As such, the safeguarding against loss of data, information, and digital technology remains underserved, whereby a major cyber-attack could be highly disruptive to society. Despite the growing need for cyber protection, limited historical precedence could put a cap on the private insurance market's appetite to offer coverage. Cyber-crimes can be pervasive and random, making them more difficult to model than geographically isolated perils such as severe weather. Further, while terrorism and war exclusions can apply, it could be difficult to discern between a state and rogue (bad actor) attacker and thus lead to drawn out coverage disputes. A further challenge is the moral hazard tied to insurance companies paying policyholder ransoms as attackers see that these organizations can pay.

Like pandemic, flood and terrorism risks, government partnership with insurers may be the ultimate solution that supports the growing need for cyber security protection. In our opinion, the insurance industry has taken a prudent approach to underwriting cyber and remains well positioned as this market evolves.

Chad Stogel, Vice President
Joe Urciuoli, Head of Research