Berkshire Hathaway Specialty Insurance

Evolving Risk is Driving Cyber Insurance Market

Underwriters shifting their focus to controls and resiliency

By: Brian Robb, *Senior Vice President, Head of Cyber/MPL/Tech* | June 2022

BRIAN ROBB
Senior Vice President
Head of Cyber/MPL/Tech

The cyber insurance marketplace had been due for a correction, and in the past few years, it got one. Organizations of all sizes seeking coverage are now required to provide more details about their exposures and answer questions that underwriters might not even have asked previously. To understand why the marketplace for cyber insurance has changed, we need to recognize that the nature of cyber risk itself has evolved — quite dramatically.

Cyber risk was not front of mind for most organizations as recently as 2015, but in the years since, that has completely changed. Cyber is on the minds of boards and senior management in virtually every industry. A decade ago, most cyber claims involved a data breach, whereas now ransomware is responsible for increasing frequency and severity in cyber losses. It's important to note that the cyber risk environment changes every six to 12 months, and the insurance industry also must change to keep pace. The cyber insurance market hardened because of ransomware, and it has led to a reset of what insurers require of policyholders from a control perspective.

Based on number of claims, the top five causes of loss for small and medium-size enterprises over the past five years, according to the 2021 NetDiligence Cyber Claims Study, were:

- Ransomware
- Hackers
- Business email compromise
- Staff Mistakes
- Phishing

NetDiligence found in that same 2021 NetDiligence Cyber Claims Study that these five causes of loss accounted for 70% of cyber claims and 80% of total incident costs.

The increase in ransomware attacks since 2016 has prompted underwriters to focus on cybersecurity and controls in place to mitigate the impact of cyber events. Even though no solution is perfect or can eliminate 100% of cyber risk, insurers have begun applying minimum requirements on risk controls. For example, multifactor authentication, endpoint protection and firewalls are the bare minimum to obtain cyber coverage. If a policyholder organization can demonstrate stronger mitigation efforts, that's even better.

REGULATORY ENFORCEMENT AHEAD

All 50 U.S. states have enacted data breach notification laws, and several other state, federal, local and foreign statutes, rules and laws relating to cyber risk and data privacy have taken effect or are about to take effect. These include: the General Data Protection Regulation (GDPR) in the European Union; the California Consumer Privacy Act (CCPA); and the Biometric Information Privacy Act (BIPA), which Illinois enacted in 2008 and is inspiring similar laws in other states. These laws increase the potential that regulatory authorities will focus on enforcement actions in the near future. Some of these statutes, rules and laws have been written with big technology companies in mind, but they apply equally to smaller organizations. Regulatory enforcement, including fines and penalties, frequently triggers private litigation, so cyber liability risk is expected to continue to rise.

PREVENTION AND RESILIENCE

The tools and data available to understand an organization's security profile have improved dramatically in recent years and cyber underwriters are more likely to look favorably on compliance with prevailing industry standards. Risk professionals whose organizations comply with data security frameworks such as the National Institute of Standards and Technology (NIST) or the ISO 27001 standard for information security management are better positioned to fend off enforcement actions and defend litigation in the event of a data breach.

As cyber incidents continue to occur, and insurers have tightened their underwriting requirements, risk professionals should focus more on risk prevention and resilience. Controlling cyber incidents and minimizing their impact is essential to prevent disruption and ensure a swift recovery.

An important exercise for risk professionals to conduct periodically with their broker and cyber insurer is to examine hypotheticals and risk scenarios, such as what might happen if a ransomware message flashes on a user's screen at 10p.m. Whom does the policyholder contact first? What should policyholders expect from their insurer? What are the sequence of steps in the response after notification of a cyber event? Knowing these things in advance, ideally in a meeting with the insurer before any incident occurs, can go a long way toward making organizations more resilient and confident in their risk partners.

Brian Robb is Senior Vice President and Head of Cyber, Miscellaneous Professional Liability and Technology Errors & Omissions Liability at Berkshire Hathaway Specialty Insurance. He leads the company's team in these lines in the United States.

For more information about cyber risk management solutions and resources, please visit: www.bhspecialty.com.

Note: *Featured in Business Insurance magazine.*