HAYS COMPANIES

Preparing for Cyber Renewals as Underwriting Standards Tighten

In the latter half of 2020, the cyber insurance market experienced unprecedented turbulence. After several years of a "soft" market, characterized by decreasing rates and expanded coverage, the market has entered a harder phase that appears likely to continue through 2021.

Increases in the frequency and severity of ransomware, the severity of business interruption following ransomware events, social engineering fraud, invoice manipulation scams, and the concern regarding privacy regulations such as GDPR, CCPA, and BIPA have caused many carriers' cyber insurance portfolios to approach or exceed a combined ratio of 100, which is the simplest measure of a portfolio's profitability or unprofitability.

While carriers have been reluctant to materially narrow the scope of coverage in their cyber insurance products, several carriers are attempting to enforce "limits management." At least one carrier is aggressively sub-limiting coverage for all losses arising from ransomware. Carriers that offered certain coverage in addition to the policy aggregate are either no longer offering those enhancements or only offering them for additional premium. Carriers are also becoming more conservative with limits offered for various cybercrime coverages, such as social engineering and invoice manipulation, and are requiring heightened controls, such as phishing simulation training, out of band authentication and dual authentication.

Various carriers are also implementing retention minimums based on limits purchased and the size of a company. Each carrier is offering different coverages and limits, so be vigilant when comparing your insurance options.

The most stark and abrupt change in 2020 has been the rapid increase in underwriting standards. In the past, underwriters largely enforced one major underwriting standard at a time, such as ensuring the applicant did not store personally identifiable information on unencrypted mobile devices or ensuring the applicant did not use any software that had been flagged as end-of-life or end-of-support.

In today's market, underwriters are applying much stricter guidelines than in the past, and companies that lack these controls are likely to experience significantly increased pricing, requirements that controls be implemented within a short period of time, or, in some circumstances, may be viewed by the market as uninsurable.

The most common points of friction in the underwriting process are:

- Multi-factor authentication for all remote access and privileged accounts
- Remote desktop ports exposed to the public
- Business continuity planning and testing that specifically addresses ransomware
- Role-Based Access
- Lack of disconnected/offline backups
- Next Gen Antivirus (NGAV)
- Lack of endpoint protection and response (EDR) tools

Take action now to identify potential security flaws and quickly implement a solution. These increased security measures not only will fortify your company's defenses, but they may prove vital in your renewal. Renewals in 2021 may be challenging, but early action may ease the pressure. Contact your Hays representative with any questions.

Contact

Visit us online or send us a message to learn more about the Hays Difference and our service offerings.

www.hayscompanies.com | info@haysccompanies.com

Hays
PART OF THE BROWN & BROWN TEAM

JANUARY 2021