HEIGHTENED RANSOMWARE ATTACKS DRIVES CARRIERS TO MODIFY CYBER COVERAGE PRICING

In the face of a volatile cybersecurity landscape, companies are increasingly turning to cyber insurance to protect their assets. However, as the severity and frequency of claims have drastically changed just over the past 12 months, cyber carriers are starting to take action.

Ransomware is a type of malware that prevents or limits users from accessing their own system by locking screens, files or networks until a ransom is paid. Hackers have become more opportunistic with their attacks, extorting organizations for large sums of money. Ransomware threats are increasing at an alarming rate, which is why it's one of the preeminent threats driving changes in cyber insurance pricing.

According to the NetDiligence 2021 Ransomware Spotlight Report, in the past five years, the average ransom demand has shot up almost twelve-fold, from $15,000 to $175,000. In The State of Ransomware 2021, Sophos surveyed 5,400 IT decision makers across 30 countries. 37% of respondents were hit by a ransomware attack, and of those respondents, 54% said the cybercriminals succeeded in encrypting their data. After paying ransom, on average only 65% of encrypted data was restored to organizations. When accounting for system downtime, loss of revenue, cyber investigation costs, legal costs and any ransom paid, this report also estimates the average bill for rectifying a ransomware attack was $1.85 million.

Unsurprisingly, cyber insurers have responded to the increasing frequency and cost of ransomware attacks by raising premiums, placing restrictions on ransomware coverages and limits, and implementing stricter underwriting guidelines than ever before. Looking at several data points, including the Council of Insurance Agents & Brokers' (CIAB) Commercial Property/Casualty Market Index Market Report Q1 2021 and AHT's proprietary data, cyber rate increases for Q1 2021 ranged from 18% to 34%, and Q2 2021 looks to be even higher. Additionally, of the respondents surveyed in the CIAB report, during Q1 2021 93% saw an increased demand for cyber coverage, and 74% saw an increase in cyber claims.

In lieu of a static cyber application with a few questions surrounding cybersecurity, carriers are now taking additional steps to understand a myriad of complex cybersecurity precautions that a prospective client takes. Now there is additional scrutiny of cyber security controls, such as multi-factor authentication, segmentation of data, encryption, patch management procedures and employee training; all contemplated and evaluated by additional onerous supplemental applications and pen testing. Understanding specific carrier requirements prior to completing applications for renewal will be imperative going forward. Preparedness and willingness to implement additional security measures before renewal could lead to better terms and conditions, as well as better cyber rates for your next renewal.

Engaging a broker that understands the complex and ever-evolving cyber landscape will be essential. Pro-active cyber risk management will not only lead to better rates and terms for insureds, but also for the security of defense industrial base, infrastructure, protected data and confidential information worldwide.

Brought to you by BRP's MiddleMarket Group - www.WeAreResilientTogether.com