2023 Cyber Insurance

Market Outlook

Evolving technology, increasing threat vectors and growing attacker sophistication has continued to drive up both the frequency and severity of cyber incidents, resulting in an ongoing rise in cyber insurance claims and subsequent underwriting losses. Amid these market conditions, most policyholders experienced higher cyber insurance rates throughout 2022. In addition to elevated premiums, insureds have begun encountering coverage restrictions, further scrutiny from underwriters regarding cybersecurity practices and exclusions for losses stemming from certain types of cyber incidents—namely, acts of cyberwarfare related to international conflicts and other prevalent cyberattack methods (e.g., ransomware). Moving into 2023, industry experts anticipate that difficult market conditions—combined with several new entrants to the segment—will make for an increasingly volatile and unpredictable cyber insurance space.

Developments and Trends to Watch

- **Increased nation-state and supply chain threats—**Nation-state cyberattacks remain a major concern, especially as the ongoing Russia-Ukraine conflict contributes to global cyberwarfare worries. Because nation-state attacks often arise from third-party exposures, businesses have also become more focused on addressing their supply chain vulnerabilities by bolstering their cybersecurity practices.
- **Tightened underwriting standards—**Similar to 2022, cyber insurance carriers have continued to adjust their underwriting practices to help mitigate the risk of making costly payouts. In particular, the heightened severity of cyber incidents has motivated most carriers to be more selective regarding which businesses they will insure and the types of losses they will cover.
- **Evolved regulations—**In the past few years, both the federal government and certain states have introduced stricter data privacy and breach notification laws, holding businesses more accountable for their cybersecurity failings. In 2021, Virginia and Colorado implemented tightened legislation mirroring the California Consumer Privacy Act and Europe's General Data Protection Regulation. Additionally, several states created laws that expanded the definition of personally identifiable information (PII) and elevated the penalties for exposing PII. In 2022, the federal government also introduced multiple new cybersecurity regulations. Such laws are expected to continue evolving during 2023, making it critical for businesses to prioritize compliance.
- **Elevated ransomware concerns—**Ransomware attacks continue to impact businesses of all sizes and sectors, but especially small- and medium-sized establishments. What's worse, these attacks often carry costly losses—both as a result of substantial payment demands and technology and data recovery efforts. In fact, international software company Acronis revealed in its latest Cyberthreat Report that global ransomware damages are expected to exceed $30 billion in 2023.
- **Heightened business email compromise (BEC) risks—**BEC scams involve cybercriminals impersonating seemingly legitimate sources—such as senior-level employees, suppliers, vendors, business partners or other organizations—via email. These scams are among the most expensive types of social engineering losses and have become a major threat to businesses across industry lines. The FBI reported that BEC scams have increased by 39% since 2020, contributing to $2.4 billion in annual losses throughout the United States and costing an average of $120,000 per incident.

Tips for Insurance Buyers

- Work with trusted insurance professionals to understand the different types of cyber coverage available and secure a policy that suits your unique needs.
- Utilize loss control services offered by insurance carriers to help strengthen your cybersecurity measures.
- Focus on employee training to prevent cybercrime from affecting your operations.
- Keep organizational technology secure by utilizing a virtual private network, installing antivirus software, implementing a firewall, restricting employees' administrative controls and encrypting all sensitive data.

HORST INSURANCE