2025 Market Outlook

Cyber Insurance

With the fast-changing nature of cyberthreats, cyber insurance can be an especially volatile and dynamic segment, and frequent market changes can make pricing predictions difficult to pin down. The CrowdStrike and Change Healthcare incidents highlighted the greater impact of just one cyberattack across multiple organizations and business sectors. Given the potential impact of systemic events like these, it's possible insurers will implement stricter underwriting guidelines in 2025 and may be less aggressive when it comes to lowering rates. While current price predictions indicate lower rates, mileage may vary from policyholder to policyholder.

Developments and Trends to Watch

- **Ransomware threats—**Ransomware attacks have skyrocketed over the past decade, and blockchain analysis firm Chainalysis reported that 2024 could be the largest grossing year yet for ransomware payments. Notably, in what's being touted as the highest ransomware payment on record, cybercrime group Dark Angels received a ransomware payment of $75 million—nearly double the highest amount from 2023. Moving into 2025, it's expected that health care providers, schools, government agencies and other infrastructure-related organizations will be increasingly targeted in ransomware attacks. Given the essential nature of these operations, attackers believe victims in these sectors are more likely to pay a ransom to avoid prolonged disruption.
- **AI exposures—**Cybercriminals can utilize AI technology to create and distribute malware, crack passwords, deploy social engineering scams, identify software vulnerabilities, and analyze stolen data. This technology can enable such activities to be carried out faster and with greater success rates, which allows cybercriminals to cause major damage and even evade detection. Heading into 2025, businesses should be particularly mindful of emerging AI-driven threats like deepfake scams, where synthetic audio or video is used to impersonate executives or employees in order to commit financial fraud or initiate data breaches.
- **Supply chain vulnerabilities (third-party vendors)—**Vendors and suppliers often don't have the same level of cybersecurity as a target organization, making them an easier point of entry for a malicious party. Supply chain exposures can stem from a variety of parties and practices within an organization, including third-party services or vendors with access to information systems, poor information security practices by suppliers, compromised organizational software or hardware, software security vulnerabilities in supply chain management or among third-party vendors, or inadequate third-party data storage measures. Supply chain attacks are an increasing challenge for insureds, and Gartner predicts that 45% of organizations will experience attacks on their software supply chain by 2025.
- **Data collection concerns—**A growing number of businesses have begun leveraging biometrics, pixels and other tracking technology to gather personal information from stakeholders for various HR, advertising and marketing processes; however, doing so poses several data privacy concerns. For instance, businesses that don't comply with applicable international, federal and state legislation (e.g., The General Data Protection Regulation, the Health Insurance Portability and Accountability Act, the Biometric Information Privacy Act and the California Privacy Rights Act) when collecting, processing and storing stakeholders' data could face substantial regulatory penalties, costly lawsuits and associated cyber losses. Heading into 2025, businesses should be aware of heightened regulatory scrutiny and evolving privacy laws around data collection, especially as more states and countries strengthen their data privacy frameworks.

Tips for Insurance Buyers

- Focus on employee training to prevent cybercrime from affecting your operations. Employees should be aware of the latest cyberthreats (e.g., AI-powered attacks, cyberwarfare, ransomware and business email compromise scams) and how to mitigate them.
- Establish an effective, documented cyber incident response plan to remain operational and minimize damages in the event of a data breach or cyberattack. Test this plan regularly by running through various scenarios with staff. Make updates to the plan as needed.
- Conduct thorough cyber risk assessments of third-party vendors before entering a partnership. Review their cybersecurity practices, ask about their data protection protocols and ensure they meet your company's standards for safeguarding sensitive information.
- Consult insurance professionals and legal counsel to determine your organization's regulatory exposures regarding applicable data protection and cybersecurity laws. Make compliance adjustments as needed.

camargo INSURANCE