2024 Midyear Market Outlook

Cyber Insurance

Heightened claim frequency and severity have created a volatile cyber insurance market in recent years, with most policyholders facing ongoing premium increases. Fortunately, the segment experienced underwriting profitability in 2022, allowing conditions to soften in 2023. Yet, many insureds are still experiencing coverage restrictions, underwriting scrutiny and exclusions for certain losses. In 2024, a report from credit rating agency Fitch Ratings revealed that the market continues to produce strong underwriting profits, but written premium volume has begun to stall due to renewed pricing pressure. Nevertheless, industry data confirmed that rates decreased in the first quarter of the year, with the average premium decline sitting at 6%. In the latter half of 2024, market conditions could keep softening; however, this segment sees frequent changes, making pricing predictions hard to pin down. As such, insureds with a strong cybersecurity posture are best equipped to navigate this evolving landscape.

Developments and Trends to Watch

- **Generative artificial intelligence (AI) exposures—**While generative AI technology can provide a host of operational benefits, it also has the potential to be weaponized by cybercriminals, thus compounding cyber losses and related claims. In particular, cybercriminals can utilize this technology when distributing malware, cracking passwords, deploying social engineering scams, identifying software vulnerabilities and analyzing stolen data. Some businesses have implemented more advanced threat identification and data protection tactics to combat AI-related losses. Even so, generative AI risks remain, especially as a growing number of organizations incorporate this technology into their own project workflows and products. In fact, multiple studies have shown that the majority (87%) of organizations are susceptible to AI-powered attacks; in contrast, only 38% of businesses are taking steps to limit their exposures. Therefore, organizations should stay vigilant in defending against generative AI threats to limit the likelihood of associated cyber losses in the future.
- **Cyberwarfare risks—**Nation-state cyberattacks remain a top concern in the cyber insurance space, particularly as geopolitical challenges contribute to global cyberwarfare worries. According to a new report released by the Office of the Director of National Intelligence, the most prevalent nation-state adversaries currently facing the United States include China, Russia, Iran and North Korea, with attackers from these countries looking to undermine critical infrastructure, extort large sums of cryptocurrency, expose sensitive data and disrupt essential services. Complicating matters, international insurance marketplace Llyod's of London started requiring insurers to revise their standalone cyber insurance policies' war exclusions in 2023 to prohibit coverage for "losses arising out of war and cyber operations that are a part of war." Other carriers will likely follow suit, implementing similar war exclusions to mitigate large-scale payouts. Yet, excluding coverage for nation-state attacks carries difficulties, as distinguishing them from other cyberthreats can be complex.
- **Data privacy concerns—**Many businesses have begun leveraging pixels and other tracking technology to gather personal information from stakeholders for various internal processes; however, this poses data privacy risks. Namely, businesses that neglect to comply with applicable legislation when collecting stakeholders' data could face regulatory penalties, costly lawsuits and subsequent cyber losses. As it stands, 13 states have introduced comprehensive data privacy laws since 2020. Most recently, the California Privacy Rights Act became enforceable in early 2024, amending and expanding the state's existing legislation on the topic. At the federal level, organizations must comply with the Health Insurance Portability and Accountability Act, while those conducting international operations may also be subject to the European Union's General Data Protection Regulation. Going forward, tracking technology will likely remain a hot topic among regulators, paving the way for evolving data privacy laws. Further, some cyber insurance carriers exclude coverage for losses caused by the wrongful collection of data, leaving businesses largely unprotected against this exposure.

Tips for Insurance Buyers

- Keep organizational systems protected by utilizing proper security software. Update this software regularly.
- Establish a cyber incident response plan to minimize damages in the event of a data breach or cyberattack.
- Review regulatory exposures in regard to relevant data privacy laws. Make compliance adjustments as needed.

Fusco Orsini & ASSOCIATES
INSURANCE SERVICES