2024 Cyber Insurance

Market Outlook

Increasing cyber insurance claim frequency and severity have generated a volatile risk environment in recent years, with most policyholders facing continued premium hikes. Fortunately, the segment experienced underwriting profitability in 2022, allowing for conditions to soften during 2023. Yet, many insureds are still experiencing coverage restrictions, scrutiny from underwriters regarding cybersecurity practices and exclusions for certain losses. Industry experts believe conditions may keep softening in 2024; however, this segment sees frequent changes and reacts to developments faster than other lines of coverage, 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

- **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 neglect to comply with applicable international, federal and state legislation when collecting, processing and storing stakeholders' data could face substantial regulatory penalties, costly lawsuits and associated cyber losses. Compounding concerns, cyber insurance carriers are increasingly excluding coverage for losses caused by the wrongful collection of data, leaving businesses largely unprotected against this exposure.

- **Artificial intelligence (AI) exposures—**While AI technology can certainly offer benefits in the realm of cybersecurity, it also has the potential to be weaponized by cybercriminals, therefore exacerbating cyber losses and related claims among businesses. In particular, cybercriminals can utilize AI technology when creating and distributing malware, cracking passwords, deploying social engineering scams, identifying software vulnerabilities and analyzing stolen data. This technology can enable such activities to be carried out faster and with greater success rates, allowing cybercriminals to cause major damage. To help combat losses stemming from weaponized AI technology, some businesses have begun implementing more comprehensive cybersecurity measures, particularly as it pertains to threat identification and data protection initiatives.

- **Ransomware threats—**Ransomware attacks, which entail cybercriminals compromising devices or servers and demanding large payments before restoring the technology, have skyrocketed over the past decade. Looking ahead, research and market intelligence firm Cybersecurity Ventures confirmed that ransomware incidents will cost businesses up to $265 billion annually by 2031. Amid rising ransomware threats, many cyber insurance carriers have started requiring policyholders to document cybersecurity practices aimed at reducing these attacks before providing coverage, while some have excluded coverage for such incidents altogether.

- **Business email compromise (BEC) risks—**BEC scams involve cybercriminals impersonating seemingly legitimate sources (e.g., senior-level employees, suppliers and business partners) via email to gain the trust of their targets and trick them into believing they are communicating with genuine senders. From there, cybercriminals convince their targets to wire money, share sensitive information or engage in other compromising activities. According to the FBI, BEC scams have cost businesses $51 billion in exposed losses throughout the past decade. Making matters worse, these scams have seen a significant rise in recent years, with such incidents surging by 47% since 2020 and exacerbating associated cyber losses.

Tips for Insurance Buyers

- Work with your insurance professionals to understand the different types of cyber coverage available and secure a policy that suits your unique needs. Start renewal conversations early.

- Focus on employee training to prevent cybercrime from affecting your operations. Employees should be aware of current cyberthreats (e.g., AI-powered attacks, ransomware and BEC scams) and ways to mitigate them.

- 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.

- Consult insurance professionals and legal counsel to determine your organization's regulatory exposures in regard to applicable data protection and cybersecurity laws. Make compliance adjustments as needed.

ACNB INSURANCE SERVICES