2022 Cyber Liability Insurance

Market Outlook

INSURANCE OFFICE OF AMERICA

The cyber insurance market is at a critical juncture for both insurance carriers and policyholders. While the last few years have seen increased competition among cyber insurance carriers, higher capacity and expanded coverage terms, both 2020 and 2021 saw a rapidly hardening cyber insurance market. Moreover, across industry lines, cyberattacks have surged in both cost and frequency. This increase in attacks has, in turn, resulted in a rise in cyber liability claims and subsequent underwriting losses. In light of these market conditions, it's predicted that most policyholders will experience higher cyber liability insurance rates in 2022, with many insureds seeing double-digit rate increases. Apart from increased premium costs, insureds may also encounter coverage restrictions, further scrutiny from underwriters regarding cybersecurity practices, and exclusions or sublimits for losses stemming from specific types of cyber incidents. If policyholders fail to demonstrate proper cybersecurity protocols or have experienced cyber incidents in the past, coverage will be increasingly difficult to obtain.

2022 Price Prediction

Overall:

+15% to +50%

Developments and Trends to Watch

- **Tightened underwriting standards**—With cyberattacks surging, cyber insurance carriers have adjusted their underwriting practices to help mitigate the risk of costly claims. In particular, carriers are now requiring more substantial documentation from their insureds. This may include detailed information related to workplace cyber policies, incident response planning, employee training and security software capabilities. In addition, some cyber insurance carriers have also decreased their risk appetite and reduced their coverage offerings—especially as they pertain to protection for losses stemming from cyber events that are on the rise (e.g., ransomware attacks). To prevent insureds from leveraging their coverage for unintended purposes, some carriers have changed their policy wording to be less ambiguous. This adjusted wording can help carriers clearly outline the types of cyber events they cover as well as when and how coverage will be triggered.
- **Elevated ransomware concerns**—Ransomware attacks have been steadily increasing in recent years. This increase is likely tied to cybercriminals becoming more sophisticated and developing further avenues for launching these attacks (e.g., ransomware-as-a-service and remote desk protocol). What's worse, ransomware attacks often carry higher costs than other types of cyber events. NetDiligence's annual cyber claims study found that ransomware attacks were the largest driver of cyber insurance claims over the last five years—with the average ransom demand rising to $247,000 and the median incident cost reaching $352,000.
- **Heightened business email compromise (BEC) risks**—BEC scams entail a cybercriminal impersonating a legitimate source within an organization to trick their victim into wiring money, sharing sensitive data or engaging in other compromising activities. According to the latest loss data from Advisen, BEC scams are among the most expensive types of social engineering losses, and they are on the rise—increasing 58% from 2015 to 2019. The median cost of a BEC loss is $764,000; this is significantly more expensive than other social engineering losses, which average around $580,000.

Tips for Insurance Buyers

- Review your employee handbook and related policies. Ensure you have all appropriate policies in place, including language on discrimination, harassment and retaliation.
- Work with your insurance professionals to understand the different types of cyber coverage available and secure a policy that suits your unique needs. Carefully determine whether standalone coverage is necessary.
- Take advantage of loss control services offered by insurance carriers to help strengthen cyber measures.
- Focus on employee training to prevent cybercrime from affecting your operations. Employees should be aware of the latest cyber threats and ways to prevent them from occurring.
- Establish an effective, documented cyber incident response plan to minimize damages amid a cyberattack.
- Consider supply chain exposures when establishing your organization's cybersecurity policies.