2021 Cyber Liability Insurance

Market Outlook

PELNIK INSURANCE

Across industry lines, cyberattacks have surged in frequency and sophistication, resulting in a rise in cyber losses. In these market conditions, we predict that most policyholders will experience higher cyber liability insurance rates in 2021. Insureds may also encounter coverage restrictions or exclusions for losses stemming from specific types of cyber incidents, while still having more generous coverage terms for other exposures. Policyholders who operate in industries with greater cyber exposures may experience more severe rate increases.

2021 Price Prediction

Overall:

+10% to +30%

Trends to Watch

- **Push for standalone policies—**In the midst of growing cyber risks, most standard property and liability policies have begun implementing exclusions for cyber exposures to avoid unexpected losses. As such, it's critical for organizations that don't already have one to seriously consider securing a standalone cyber liability policy.
- **Remote work exposures—**The COVID-19 pandemic forced many organizations to have their staff work from home for the first time. Unfortunately, these telework arrangements led to a rise in cyber-attacks, as many cybercriminals have targeted remote employees in various phishing incidents.
- **Ransomware concerns—**Ransomware is used by cybercriminals to compromise a device and demand a large payment be made before restoring the technology—as well as any data stored on it—for the victim. The number of ransomware attacks has spiked in the past few years. In response, some insurance carriers have revised coverage conditions related to ransomware incidents.
- **Regulatory ramifications—**A multitude of both international and domestic jurisdictions have recently debuted new data protection laws aimed at increasing responsibilities and compliance considerations for organizations that handle sensitive data. Looking ahead, more and more states are expected to pass similar legislation—increasing employers' regulatory exposures in the realm of data protection.
- **Fallout from SolarWinds—**In 2020, the U.S. government revealed that hackers infiltrated the company SolarWinds' network monitoring platform via malware before using that platform to access sensitive data from several government departments and private organizations. The fallout from this attack has motivated businesses, the insurance industry and government entities to take a closer look at their supply chain cybersecurity risks.

Tips for Insurance Buyers

- Work with your insurance professionals to understand the types of cyber coverage available and secure a policy that fits your needs.
- Utilize security services offered by insurance carriers and third-party vendors to strengthen your cybersecurity measures.
- Focus on employee training to prevent cybercrime from affecting your operations.