Cyber Liability Insurance Market Concerns in 2022

Impact on Emerging Life Sciences Companies

Life sciences companies often control large amounts of proprietary data including patient information and intellectual property (IP) that is highly valued by cyber criminals. Intellectual property is a major target for cyberattacks. A breach would be devastating to any life sciences company, but especially to an emerging company with limited resources.

The cost of data breaches are increasing and cyberattacks continue to escalate across the industry. In response, cyber insurance carriers are raising rates and adjusting their underwriting practices to reduce their claims exposure. Underwriters are also requiring more substantial documentation of workplace policies including training, incident response planning and data security protocols.

Companies, especially emerging businesses, should anticipate investors, contract partners, and research and trial sites, including healthcare and academic centers, to insist on cyber liability coverage.

Developments & Trends to Watch

More Restrictive Underwriting

The cyber insurance market is at a critical juncture for both insurance carriers and policyholders. While the last few years have seen increasing competition among cyber insurance carriers, resulting in 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. All of these factors are contributing to a rise in cyber liability claims and subsequent underwriting losses.

In light of these market conditions, experts predict that most policyholders will experience higher cyber liability insurance rates in 2022, with many insureds seeing double-digit rate increases. Apart from increasing premium costs, most insured companies will encounter coverage restrictions, further scrutiny from underwriters regarding cybersecurity practices and exclusions or sub limits for losses stemming from specific types of cyber incidents. Coverage will be increasingly difficult to attain for policyholders who fail to demonstrate proper cybersecurity protocols or have previous cyber incidents.

Effective Controls & Training Required

With cyberattacks surging, cyber insurance carriers are adjusting their underwriting practices to help mitigate their exposure to costly claims. In particular, carriers are now requiring more substantial documentation of cyber-related policies and procedures. This may include detailed information related to workplace cyber policies, incident response planning, employee training and security software capabilities.

Elevated Ransomware Vigilance

Ransomware attacks have been steadily increasing in recent years; this is likely tied to cybercriminals becoming more sophisticated and developing further avenues for launching these attacks (e.g., Ransomware-as-a-Service). What's worse, ransomware attacks often carry higher costs than other types of cyber events. NetDiligence's annual cyber claims study discovered that ransomware attacks were the largest driver of cyber insurance claims over the last five years. The average ransom demand has risen to $247,000 and the median incident cost has reached $352,000.

Heightened Business Email Compromise (BEC) Risk

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. They're also on the rise, increasing 58% from 2015 to 2019. The median cost of a BEC loss is $764,000, which is significantly more expensive than other social engineering losses that average around $580,000.

Best Practices for Securing Coverage

Without proper coverage, cyber claims can be especially devastating to emerging companies. Here are some tips for obtaining coverage and creating a safer cyber environment:

- Work with an experienced broker who understand the different types of cyber coverage available and can help secure a policy that suits your unique needs.
- Evaluate existing contracts to determine what coverage is required, at what limits and in what form.
- Take advantage of loss control services offered by insurance carriers to help strengthen your 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.