ProWriters
Professional & Management Liability Insurance

Why Do Life Sciences Need Cyber Insurance

The healthcare and life sciences industries are linked by a complex network of patients, providers, researchers, and regulators who work together to deliver medical services. Today, technologies such as 5G and cloud are becoming an integral part of this network, accelerating connectivity and information sharing.

However, cybercrime continues to rise as the two industries become more interconnected. According to IBM Security, the average cost of a healthcare data breach is more than $10 million. This issue highlights the need for health organizations to protect sensitive data and their ecosystems.

While it may seem challenging to keep up with emerging threats, health organizations can lower their risk by investing in strong security infrastructure and a cyber insurance policy.

Cyber Risks and Exposures in Life Sciences Industry

Here are some key factors that make the life sciences sector more vulnerable to cyber attacks:

1). Intellectual property is the most valuable asset in the life sciences sector. Life sciences IP can include data from clinical trials, therapies in development, or drug formulas based on years of research. Cybercriminals are interested in this information as it can potentially transform the medical industry and generate huge revenue. Another threat is industrial espionage, which competing organizations can initiate to gain access to data that can give them an industry advantage.

2).The life sciences sector relies heavily on external partners and contractors, who often have access to sensitive information, systems, and networks. This creates potential cyber vulnerabilities from partner suppliers without effective cyber security measures. A single partner organization that falls prey to a cyber attack can threaten business continuity or put the company's data and networks at risk of being infiltrated.

3). Life sciences is one of the most active industries for mergers and acquisitions. According to a recent industry update, M&A in the health industry is expected to remain high in 2022. However, while M&A is an effective strategy to unlock new technologies and resources for healthcare companies, it poses cyber-related risks.

ProWriters
Professional & Management Liability Insurance

The True Cost of Cybercrime in Life Sciences: Real World Examples

Life sciences is an industry built on research, innovation, and development, which makes it an attractive target for cybercriminals. Over time, expect to see more headlines about high-profile cyber attacks on organizations, such as the ones listed below.

- **Merck & Co:** The multinational pharmaceutical company is one of the victims of the 2017 NotPetya attacks, a malware outbreak that impacted companies across 65 countries. The company suffered nearly $1 billion in damages, and a disruption of its worldwide operations, from manufacturing to sales.

- **Sangamo Therapeutics:** For approximately 11 weeks in 2018, a hacker accessed a senior executive's email account at Sangamo Therapeutics. This compromised confidential and sensitive company data. The organization then revealed that it didn't have cyber security coverage to address the data security breach.

- **Dr. Reddy's Laboratories:** The Indian pharmaceutical company reported a cyber attack in 2020 after being granted permission to begin its final stage trials for a COVID-19 vaccine. This required the company to shut down most of its plants worldwide. This issue highlighted how cybercriminals are targetting pharmaceutical companies to steal clinical information and disrupt vaccine research.

How Cyber Insurance Can Help

While having robust security measures can help, no business can ensure complete protection from emerging security threats. This is where cyber insurance comes into play. Cyber insurance can cover the cost of cyber attacks, including the following first and third-party coverages:

- Hiring IT Consultants To Determine the Origin of the Breach
- Repairing Digital Assets
- Informing Affected Customers and Personnel
- Establishing a Hotline To Answer Questions From Affected Parties
- Legal Representation
- Document Preparation
- Regulatory Fines
- Payouts to Affected Customers