ProWriters
Professional & Management Liability Insurance

Why the Healthcare Industry Needs Cyber Insurance

The healthcare sector handles vast amounts of sensitive personal data, including medical records and patient information. There are many reasons why cyber criminals are able to exploit this information:

- This data is extremely valuable on the black market, making the sector a lucrative target for cyber criminals.
- Healthcare organizations also increasingly utilize interconnected systems and devices, from electronic health records to telemedicine platforms. While essential for modern medical care, this interconnectedness creates multiple points of vulnerability. Many of these systems, especially older ones, may need more robust security measures.
- Compounding the issue is the healthcare industry's intrinsic focus on patient care, coupled with the constraints of limited budgets. These factors frequently relegate cyber security to a lower priority. Consequently, this situation leads to outdated systems and a lack of staff training on cyber security best practices, making it easier for attackers to exploit vulnerabilities.

Addressing cyber attacks in healthcare is more pressing than in any other industry. A ransomware strike on a hospital can be a matter of life and death for patients. A data breach can expose patients' most sensitive information. The healthcare industry needs comprehensive cyber coverage and risk management for these reasons.

The Cost of a Breach

In 2023, healthcare saw its 13th consecutive year as the industry most affected by data breach expenses. While the global average cost for data breaches across all industries stood at $4.45 million, the healthcare sector faced far steeper expenses, with costs soaring to $10.93 million, as reported by IBM Security. This figure represents a 53.3% increase over three years and marks the first instance where the average cost of a healthcare data breach exceeded $10 million. A contributing factor to this high cost is the stringent HIPAA regulations, which enforce high fines of $50,000 per violation and can escalate to as much as $1.5 million annually for multiple violations of the same rule.

Often, these breaches arise from insufficient cloud storage security or compromised credentials from password reuse. But even if a business takes all necessary precautions to avoid a cyber attack, it's still responsible for any data breaches resulting from its systems. With so much at stake, the healthcare sector needs Cyber Insurance now more than ever.

ProWriters
Professional & Management Liability Insurance

The Power of Comprehensive Coverage

First-Party Coverage

First-party coverage includes the costs of hiring forensic IT staff to determine the extent of the damage, notifying potentially compromised patients in compliance with HIPAA regulations, and building the business's systems back more securely.

Third-Party Coverage

Third-party coverage includes any regulatory fines and penalties levied due to the breach. It also covers any legal fees and payouts from lawsuits against a company. These suits can be personal injury cases from patients or affected credit providers for failure to comply with industry data security practices.

Real-World Examples

Numerous cyber security incidents affected the healthcare sector in 2023, but Regal Medical Group and HCA Healthcare were among the most severe.

- In February, Regal Medical Group, based in San Bernardino, Calif., experienced a significant data breach, exposing the personal health information of approximately 3.3 million medical records in a ransomware attack. This incident led to multiple class action lawsuits against the health provider and its affiliates.
- In August, Nashville, Tenn.'s HCA Healthcare disclosed a major data breach. The breach, which occurred due to data theft from an external storage facility, affected an estimated 11.27 million patients.

In light of these events, the importance of obtaining Cyber Insurance has become more evident than ever, serving as a vital safeguard against increasing cyber threats.