Why the Healthcare Industry Needs Cyber Insurance

Hospitals and healthcare systems are facing unprecedented load, meaning there's never been a more difficult time to deal with cyber attacks.

During the COVID-19 pandemic, the healthcare industry shifted more work to the virtual world faster than anyone thought possible. As a result, the medical sector now stores more data and has more people accessing it remotely than ever before. This rapid change and high demand makes hospitals and medical computer systems an incredibly lucrative target for hackers, with **attacks spiking 55% in 2020**.

The need to address cyberattacks 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. For these reasons, the healthcare industry needs comprehensive cyber coverage and risk management.

The Cost of a Breach

By a large margin, cyberattacks cost healthcare more than they cost any other industry. In 2021, the **average cost of a breach reached nearly $9.5 million.** This amount is due partly to HIPAA regulations, which place hefty fines of up to $1.5 million a year per violation on healthcare providers that fail to adequately protect patient data.

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 their systems. With so much at stake, the healthcare sector needs cyber insurance now more than ever.

Patching procedures—Distributing and installing software updates in a consistent and timely way, reducing criminals' chances to exploit software vulnerabilities.

"3-2-1" backup protocols—Creating one primary backup and two copies of data, on two different media, and keeping at least one backup off-site protects the information and makes it easier for companies to recover in the event of a cyber attack.

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 as a result of 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 from affected credit providers for failure to comply with industry data security practices.

A Real World Example

In June 2021, St. Joseph's/Candler, the largest healthcare provider in Savannah, Georgia, fell victim to a ransomware attack. The cyberattack **impacted 1.4 million individuals**. It forced the health system into EHR downtime, and providers were required to document clinical notes on pen and paper. Forensic IT work revealed the system may have been compromised as early as mid-December 2020.

Between lost revenue, IT services, government fines, patient alert systems, and complementary identity protection, this breach cost millions upon millions of dollars to St. Joseph's/Candler. The stakes are too high for an organization to be caught unprotected. Get cyber insurance today.