HealthManagement
Promoting Management and Leadership

Cyber Attack Insurance: The Facts

Even with more resources invested to boost cybersecurity, hospitals are not immune to costly cyberattacks. And as cyber threats increase in frequency, the healthcare industry remains extremely vulnerable, according to experts.

Hacking attacks wreak havoc with information systems and data; in turn hospitals face stiff fines tied to data breaches. That's where the question of cyber insurance comes in. Purchasing a policy can be considered as part of the organisation's risk management plan. So what's the best way to evaluate potential cybersecurity risks and coverage in today's chaotic threat landscape?

"It starts with a top to bottom assessment of your IT capabilities as well as how information is stored," according to Stuart O'Neal, an attorney at Burns White and co-chair of the firm's cybersecurity and professional liability groups. Having an interactive meeting with your insurance broker will be helpful in determining what your organisation's options are, how they are covered, what scenarios are not covered and how your organisation is positioned relative to that coverage, O'Neal adds.

For his part, Steven Gravely, a partner and healthcare practice lead at Troutman Sanders, says healthcare providers should view cybersecurity as an enterprise risk and not simply an IT issue. "The dollar amount of coverage is certainly one important factor, but as important is the scope of the coverage. What is included under the policy as a covered loss and what is not," Gravely explains.

Most insurance policies, for example, cover the costs of notification to affected persons and the cost of a lawyer to serve as the data breach coach for a specific event. But there are insurance companies that do not provide coverage for revenue losses linked to suspension of medical and other services during a ransomware attack.

Also, it's important to understand that the cyber-insurance market is evolving constantly as the nature of cyber threats change, Gravely says.

An emerging risk for healthcare organisations to consider is how patients will receive care when computer systems are down. Bodily injury arising out of a cyber-attack is also becoming a reality as more medical devices are connected to the web and the Internet of Things.

"Above all, the risk manager and IT director need to evaluate how comprehensive their incident response plan is, usually by engaging a third party for assistance," according to Nick Cushmore, assistant vice president at insurance broker The Graham Company. "A well-executed response plan is the best way to mitigate the financial impact to an organisation following a cyber-incident."

When it comes to coverage, benchmarking data on what limits were purchased by comparable organisations should be available from an insurance broker or carrier, and there are breach calculators that can be used to estimate the potential cost of a breach based on the number of records compromised.

Source: Healthcare IT News
Image Credit: Pixabay

Published on : Tue, 8 Aug 2017