HealthManagement
Promoting Management and Leadership

Shopping for cybersecurity insurance

More healthcare organisations now include cybersecurity in their risk management plans, as they are increasingly aware how data breaches can adversely impact their operations. Many have turned to cyber insurance for coverage on breach-related burden.

An article in Healthcare IT News provides useful information and tips from insurance and risk management experts regarding common mistakes to avoid when shopping for a cyber policy.

Mistake #1: Rushing the process

An insurance broker or carrier will provide a questionnaire that will evaluate your organisation's security posture, programme, tools and policies. The biggest mistake is to rush the pre-policy process to see the rates and what the carrier will cover. Often these questionnaires attempt to create a black and white policy and "it can be tough to answer correctly," according to attorney Matthew Fisher, partner with Mirick O'Connell. Still, you need to be transparent and accurate, or your policy application can be turned down if you were inaccurate or misleading in your responses.

Mistake #2: Lax, incomplete risk assessment

It's easier to prevent a misleading or false statement to an underwriter, when your organisation has a strong assessment and inventory of the processes and tools on the system. But far too often, hospitals "don't know everything about the control environment," notes Jane Harper, Henry Ford Health System's director of privacy and security risk management. For example, an organisation filling out the policy questionnaire may have all of the right elements in place. But if another tool was purchased and the controls weren't updated or the control was removed and the underwriter was not notified, there could be a problem, Harper points out.

Mistake #3: Failing to involve the right people

The appropriate key stakeholders, Harper says, are not only involved with the evaluation process – how many patients, how much data, etc. – but also the responses to the questions the policy is going to ask. It's important to include privacy and security risk professionals, security officers, IT leader, your key business leaders/owners and those driving the data, in the discussion. Also crucial? Making sure the facilities team is involved, as there can sometimes be a cyber incident based on a physical issue. "If there's a break in at a warehouse and data is stolen, OCR considers that a breach," Harper explains.

Mistake #4: Failing to understand coverage

Often organisations make large assumptions as to just what cyber insurance will cover. According to Fisher, these leaders are often shocked to learn that they did not receive the full spectrum of coverage they wanted. His advice: Don't just rely on what the broker or agent is telling you. "It's always up to you to go into something with eyes fully wide open to make sure you know what you're actually buying."

Source: Healthcare IT News
Image Credit: iStock

Published on : Wed, 24 Oct 2018