Codify
BY AAPC

Health Information Compliance Alert

Data Security: Ransomware Is Rampant & Your Risk Analysis Might Save You

Study highlights the new trend toward specialized data breach insurance policies.

Nearly 90 percent of healthcare organizations have experienced a data breach in the past two years, with an average cost per breach of a whopping $2.2 million. Will your organization be next?

Probably so, according to a new study of 91 covered entities (CEs) including health providers, insurers and government agencies, and 84 business associates (BAs) including IT vendors, claims processors, medical device firms, transcription services, and pharmaceutical entities.

On May 12, the **Ponemon Institute LLC** released its "Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data." Overall, the study found that nearly 90 percent of healthcare organizations in the study had a data breach in the past two years, and nearly half had more than five data breaches in the same time period.

Breach Stats: Hacking Surpasses Employee Errors

Findings: "Criminal attacks" are the leading cause of half of all data breaches in healthcare, with employee errors, third-party mistakes, and stolen devices serving as the root cause of the other half of data breaches, according to the study. But the study authors also found that although most healthcare organizations believe they're vulnerable to a data breach, they're unprepared to address new threats and lack the resources to protect patient data.

Although most of the breaches were relatively small, affecting fewer than 500 records, the price tag is still high, averaging $6.2 billion annually.

Also, the researchers found that HIPAA breaches are becoming more insidious when Ponemon started the benchmark survey six years ago, unintentional employee error was the leading cause of data breaches. But now, criminal attacks account for 50 percent of data breaches affecting healthcare organizations, followed by third-party mistakes (40 percent), stolen devices (39 percent), and technical systems issues (29 percent).

Unintentional employee action still made it into the top five root causes of data breaches, but it accounted for only 36 percent, according to **Clearwater Compliance LLC**. Employee error still ranked number-one for the root cause of breaches for BAs, however.

Yet the surveyed healthcare organizations identified employee negligence as by far the biggest security threat they worry about. Mobile device insecurity, use of public cloud services, "bring your own device" (BYOD), and insecure mobile apps ranked among the other top worries.

Watch Out for Ransomware, DoS Attacks

Cyberattacks and denial of service (DoS) attacks followed by ransomware/malware were also among the top worries for CEs and BAs.

"Ransomware is a virtual stick-up," explains Providence-based attorney **Steven Richard** with **Nixon Peabody LLP**.

"Hackers essentially try to find the weakest links in your system to be able to take your data, hold it hostage, and make you pay a ransom to be able to obtain and use it in the future."

"Unsuspecting workers will click on a link or an email and consequently infect your system with encryption that prevents access," Richard says. "Hackers typically target the most data-dependent businesses, such as healthcare or governmental functions, where the data has the most value and the ransom can be the most threatening."

What to do: "You should restore and back up your data frequently, have a very detailed and well thought-out data recovery plan," Richard advises. "When you back up your data, it's best to do it in a way that is disconnected from your network, such that it's accessible if and when you're hit with a ransomware attack."

Trend: Should You Buy Data Breach Insurance?

In addition to ransomware, the survey discovered that data breach insurance is also chief on healthcare organizations' minds. According to the study, both CEs and BAs are turning to data breach insurance policies to reduce the costs and potentially devastating financial impact of a data breach.

The study also illustrates the types of coverage that data breach insurance policies typically provide. Some policies cover legal defense costs, replacement of lost or damaged equipment, and/or forensics and investigative costs, notes **Cindy Ng** of the data security software firm **Varonis**.

Nearly one-third of surveyed organizations have a data breach insurance policy, more than half of which have policies that provide $5 million in coverage, Ng says.

Do That Risk Analysis Now!

Although the HIPAA Security Rule requires you to conduct risk analyses, 60 percent of the surveyed organizations said they assess vulnerabilities, and 43 percent of those say there is no regular schedule, according to Clearwater. "You might think, in the face of increasing cybersecurity threats and costs of breaches, a growing number of healthcare organizations would be implementing more powerful defense measures starting with a bona fide risk analysis."

Must do: "A risk analysis is the first step in identifying and implementing safeguards to protect the privacy and security of PHI," Clearwater stresses. "Not once and done, but every time operations, technology, or processes change."

Link: To download the Ponemon study, go to www2.idexpertscorp.com/sixth-annual-ponemon-benchmark-study-on-privacy-security-of-healthcare-data-incidents.