Health Data Breaches Spur Demand for Cyber Insurance

MARISSA EVANS | JANUARY 9, 2015

As head of privacy and data security for Henry Ford Health System, Meredith R. Phillips says she doesn't stay up at night worrying about sophisticated hackers trying to steal medical records.

"I lose sleep over the 23,000 people walking around here with access to information," said Phillips, whose Detroit-based nonprofit corporation owns five area hospitals and serves 3.2 million outpatients annually.

Her concerns about employees and their equipment contributing to data breaches aren't unfounded. In 2010, a laptop containing medical information for nearly 4,000 patients was stolen from a doctor's office, resulting in an investigation that cost $50,000.

"Even though $50,000 is not a lot of money to a large organization, it's still unbudgeted expenses when there's a failure of process or procedure," Phillips said in an interview.

A year after the breach, HFHS purchased cyber insurance for the first time, and they've had to use it as recently as a few weeks ago when a flash drive containing 2,000 patients' medical information was lost.

Whether through theft or negligence, compromised medical records are becoming commonplace in the healthcare industry. Forty-three percent of major data breaches in 2013 came from the health industry, according to the Identity Theft Resource Center.

Some of the bigger breaches have even resulted in federal penalties. Last year, the Department of Health and Human Services fined New York and Presbyterian Hospital and Columbia University $4.8 million for a data breach. In 2009, BlueCross BlueShield of Tennessee had more than 1 million patient records stolen, leading to $1.5 million in HIPPA violations.

Incidents like these are prompting more health companies to turn to cyber insurance. Coverage in the field more than doubled from 10 percent to 26 percent

last year, according to the Ponemon Institute, a security firm, which also said in a report that the cost of breaches for the healthcare industry could be as much as $5.6 billion annually.

Michael Bruemmer, vice president for Experian Data Breach Resolutions, said the most consistent problem stemmed from employee negligence, such as losing a laptop or forgetting to turn on the firewall system. For those reasons, Bruemmer said, most cyber insurance policies "require at a minimum they go through training on a semi-annual basis, have minimal firewall protection and encryption of data."

Of the 3,100 companies Experian helped with data breaches last year, 44 percent were from the healthcare industry.

That's resulted in a cyber insurance market estimated to be worth $2 billion, and one that's likely to keep growing in the near future, according to Tom Reagan, managing director and cyber practice leader for Marsh, a risk-management company and insurance broker.

"You don't typically ask a medical company if they buy medical malpractice insurance, and cyber insurance is going to be just like that in the next five years," Reagan said in an interview.

Demand for coverage increased 11 percent among Marsh's healthcare clients last year. In 2013, the average coverage limit provided by Marsh was $12 million for healthcare companies with more than $1 billion in revenue.

Cyber insurance premiums can range from a few thousand dollars for small businesses to several hundred thousand dollars for major corporations wanting more coverage, according to an Insurance Information Institute study.

Policies often give advice on how to improve existing breach plans and simulate data breach protocols. They also help companies investigate breaches and manage the crisis communications by setting up call centers, sending notification letters and establishing credit monitoring for customers, in addition to helping with some legal fees.

But not all policies are the same, according to Jeremy Henley, director of breach services for ID Experts, a company that helps manage data breaches.

"There's a lot of variability in cyber insurance that can make it difficult for buyers to determine the differences in the plans they're considering," Henley said in an

interview, noting that some policies stipulate who can respond to a breach, while others allow companies to make that decision on their own.

“With cyber insurance they ask you 10 or 20 preliminary questions and a company can get millions of dollars in coverage, but there’s limited resources to help companies prevent or prepare for having a breach tied to this insurance right now,” Henley said.

For HFHS, though, purchasing a cyber insurance policy with a $20,000 deductible was a good business move, according to Phillips, who said it also provides peace of mind.

“We have car insurance and health insurance we may not always use but it’s there and it helps us when we have an episode,” Phillips said. “It’s the same thing when it comes to cyber insurance.”