Rising Cyber Attacks Costing Health System $6 Billion Annually

A rise in cyberattacks against doctors and hospitals is costing the U.S. health-care system $6 billion a year as organized criminals who once targeted retailers and financial firms increasingly go after medical records, security researchers say.

Criminal attacks against health-care providers have more than doubled in the past five years, with the average data breach costing a hospital $2.1 million, according to a study today from the Ponemon Institute, a security research and consulting firm. Nearly 90 percent of health-care providers were hit by breaches in the past two years, half of them criminal in nature, the report found.

While intrusions like ones exposing millions of consumers at health insurer Anthem Inc. and hospital operator Community Health Systems Inc. have increased risk awareness, most of their peers are still unprepared for sophisticated data attacks, security experts have said.

"The health-care industry is being hunted and hacked by the elite financial criminal syndicates that had been targeting large financial institutions until they realized health-care databases are more valuable," said Tom Kellermann, chief cybersecurity officer at Trend Micro Inc., who wasn't involved in the study.

> "DATA IS BEING RESOLD ON PRIVATE FORUMS THAT SPECIALIZE IN STOLEN CREDIT CARDS OR SOCIAL SECURITY NUMBERS"

Medical records, which often contain Social Security numbers, insurance IDs, addresses and medical details, sell for as much as 20 times the price of a stolen credit-card number, according to Dell SecureWorks, a unit of Dell Inc.

Free Insurance

Thieves can use that information to take out a loan or open up a line of credit in the victim's name, or for medical identity theft, where the victim's insurance ID is used by an impostor seeking free medical care.

About half of health-care organizations surveyed by Ponemon said they didn't have sufficient technology to prevent or quickly detect a breach, or the personnel with the necessary technical expertise.

"The organizations are getting better, but it is a slow-moving train," said Larry Ponemon, chairman of the Ponemon Institute. He said many firms are moving from paper-based to automated systems, a transition that makes them "very vulnerable to criminal attacks."

Last year, health records on 88.4 million people were breached as a result of theft or hacking -- about twice as many as in 2010, according to a database kept by the Department of Health and Human Services, which requires organizations to report breaches involving more than 500 patients.

Dark Web

The numbers this year are already in excess of last year's, after hackers accessed almost 80 million records from Anthem and 11 million from the health insurer Premera Blue Cross.

Data is resold on private forums that specialize in selling stolen credit cards or Social Security numbers, or on the dark web, where users' identities are hidden and transactions are done anonymously in Bitcoins, said Patrick Peterson, chief executive officer of data security firm Agari Data Inc.

He said he has seen thieves selling thousands of records containing information on people who've been diagnosed with HIV or have liver damage from alcohol use, among other conditions.

He said he suspects the cyber security world only discovers a fraction of the theft going on -- "the tip of the iceberg."

Posted on Bloomberg Business May 7, 2015: http://www.bloomberg.com/news/articles/2015-05-07/rising-cyber-attacks-costing-health-system-6-billion-annually