INSURANCE JOURNAL

Healthcare Industry Lacks Adequate Cybersecurity, Says FBI

By Jim Finkle | April 25, 2014

The FBI has warned healthcare providers their cybersecurity systems are lax compared to other sectors, making them vulnerable to attacks by hackers searching for Americans' personal medical records and health insurance data.

Health data is far more valuable to hackers on the black market than credit card numbers because it tends to contain details that can be used to access bank accounts or obtain prescriptions for controlled substances.

"The healthcare industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely," the Federal Bureau of Investigation said in a private notice it has been distributing to healthcare providers, obtained by Reuters.

The notice, dated April 8, did not mention the Obamacare website, Healthcare.gov, which has been criticized by opponents of the Obama administration for security flaws. It urged recipients to report suspicious or criminal activity to local FBI bureaus or the agency's 24/7 Cyber Watch.

FBI spokeswoman Jenny Shearer declined comment on the private industry notification, or PIN. In January the FBI issued a PIN advising retailers to expect more credit card breaches following last year's unprecedented attack on Target Corp.

Details of PINs are typically unclassified, but generally only shared with affected organizations who are asked to keep their contents private.

A series of privately commissioned reports published over the past few years have urged healthcare systems to boost security. Experts applauded the FBI for responding with its own warning.

"I'm really happy to see the FBI doing this. It's nice to see the attention," said Shane Shook, an executive with cybersecurity firm Cylance Inc who helps companies respond to breaches.

Retailers and financial institutions have taken steps to bolster security of financial information after the attack on Target as well as smaller breaches at Neiman Marcus, Michaels and other merchants. Hackers accessed millions of bank card numbers and other customer data.

As those stolen payment card numbers flooded underground markets, the value of that information dropped, leading to "fire sales" by criminals seeking to unload them, said Angel Grant, senior manager for fraud and risk intelligence at EMC Corp's RSA security division.

INSURANCE JOURNAL

Demand for medical information, however, remains strong on criminal marketplaces, experts said, partly because it takes victims longer to realize the information has been stolen and report it, and because of the different ways the information can be used.

Cyber criminals were getting paid $20 for health insurance credentials on some underground markets, compared with $1 to $2 for U.S. credit card numbers prior to the Target breach, according cybersecurity firm Dell SecureWorks.

Some criminals use medical records to impersonate patients with diseases so they can obtain prescriptions for controlled substances, Grant said. Several U.S. states, including Massachusetts, have reported a surge in opiate addiction, along with a jump in heroin overdoses that the Obama administration has called a "public health crisis."

Others criminals are purely interested in using the medical data for financial fraud.

"They are harvesting information to make it easier to conduct identity theft, to open new accounts," Grant said.

Pieces of health information are also sometimes combined with other pieces of data into complete packages known as "fullz" and "kitz" on underground exchanges where they can fetch$1,000 or more when bundled with counterfeit documents, according to Dell.

The two-page FBI alert cited a February 2014 report from the non-profit SANS Institute, which trains cybersecurity professionals. SANS had warned the healthcare industry was not well-prepared to fight growing cyber threats, pointing to hundreds of attacks on radiology imaging software, video conferencing equipment, routers and firewalls.

(Reporting by Jim Finkle; Editing by Richard Valdmanis and Mohammad Zargham)