Hackers are coming after your medical records

Cadie Thompson | @CadieThompson

Thursday, 29 May 2014 | 2:59 PM ETCNBC.com

John Lund | Getty Images

Forget your credit card data. The smartest hackers are now targeting your medical records.

Cybercriminals are now going after health-care sites more than they are retailers, financial institutions and utility companies, according to a study published Wednesday by the security firm BitSight Technologies.

BitSight analyzed security performance of companies in the S&P 500 stock index in February and found that not only are health-care and pharma companies being targeted more, but these companies are also much slower in detecting and resolving the security issues, said Stephen Boyer, BitSight's co-founder and chief technology officer.

"We were expecting utilities to be one of the worst performers, but they weren't so bad. The one that surprised us was that health care scored so low. Anything that falls below retail is a little bit scary to us," Boyer said.

He said that health-care companies lacked many of the basic protections that security experts would expect in a company's network.

Read MoreHacker's hedge fund targets vulnerable companies

"They don't have the proper encryptions or protocols or behaviors you would expect to have, and security just isn't their top talent," Boyer said.

One reason this industry is coming under attack is because electronic medical records on the black market sell for more than credit card numbers, Boyer said. He cited examples of medical records selling for $20, while with credit cards the going rate was around $1. The records are being used to help criminals get access to drugs and other treatments, he said.

Securing medical data quickly doesn't look promising either because so many hospitals and other medical facilities are equipped with poor IT equipment, Boyer said,

"I don't see the response (will) be lightning quick, with all those legacy systems in hospitals, you just can't fix this overnight," he said.

Read More[Why you should change your password now](#)

Also worth noting, when BitSight investigated reasons why health-care companies may be falling behind in security, researchers discovered that the pay of IT professionals working for health-care companies was less than all other IT staff in the industries also included in the study.

BitSight's report comes after February's release of a report by the IT security-focused SANS Institute, which said the health-care industry is dealing with an "alarming" number of security breaches.

The SANS report noted that about 94 percent of medical institutions have reported being the victims of cyberattacks.

"Now, with the push to digitize all health-care records, the emergence of HealthCare.gov and an outpouring of electronic protected health information (ePHI) being exchanged online, even more attack surfaces are being exposed in the health-care field," the report said.

The report also said that the number of breaches in the health-care sector "not only confirmed how vulnerable the industry had become, it also revealed how far behind industry-related cybersecurity strategies and controls have fallen."

"Unlike e-commerce–related theft and fraud expenses from which most consumers are shielded, consumers are responsible for costs related to compromised medical insurance records ... costs that reached $12 billion in 2013," SANS noted.

In 2009, the U.S. Health and Human Services Department began mandating that any data breach involving unsecured protected health information be reported to HHS. Since then, the department said, there have been 116,000 reports of breaches of unsecured protected health information involving fewer than than 500 individuals each.

There have also been more than 980 reports of breaches involving health information for 500 or more people, HHS said. In those combined cases, information for more than 31.3 million people was breached, the department said.

Of those larger breaches, the locations where they occurred broke down in this way: laptops, 23 percent; paper records, 22 percent; desktop computers, 15 percent; portable electronic devices, 14 percent; network servers, 11 percent; email, 3 percent; electronic medical records, 2 percent; and other, 11 percent.

—By CNBC's Cadie