Hackers break into networks of 3 big medical device makers

February 10, 2014 Thomas Lee San Francisco Chronicle

http://www.sfgate.com/news/article/Hackers-break-into-networks-of-3-big-medical-5217780.php

Hackers have penetrated the computer networks of the country's top medical device makers, The Chronicle has learned.

The attacks struck Medtronic, the world's largest medical device maker, Boston Scientific and St. Jude Medical sometime during the first half of 2013 and might have lasted as long as several months, according to a source close to the companies.

It's not clear what exactly the hackers were after, but federal laws meant to safeguard medical information require the companies to disclose any breach involving patient information. The companies have made no such disclosures.

All three companies have extensive operations in the Bay Area. Santa Rosa is home to Medtronic's endovascular therapies and coronary businesses. St. Jude Medical operates manufacturing plants in Sunnyvale. Boston Scientific has offices in San Jose, Santa Clara and Fremont.

Signs point to China

The attacks were was "very thorough" and showed signs they might have been committed by hackers in China, the source said.

The medical device makers were not aware of the intrusions until federal authorities contacted them, and they have formed task forces to investigate the breach, he said.

"Like many companies, Boston Scientific experiences attempts to penetrate our networks and systems and we take such attempts seriously," Denise Kaigler, senior vice president of corporate affairs and communications, said in an e-mail. "We have a dedicated team to detect and mitigate attacks when they occur as well as to implement solutions to prevent future attacks."

Kaigler would not comment on the specifics of any attack for security reasons, but described the Chronicle's information as "inaccurate." She declined to provide any further detail.

A spokeswoman for Medtronic said the company would also not comment on any specific attack, and St. Jude Medical did not respond to a request for comment. The FBI did not comment.

High-tech companies like medical device makers sit on billions of dollars of intellectual property, making them an attractive target for corporate spies looking for an edge in developing the next blockbuster product.

Cybercrime costs the United States economy about $100 billion each year, according to a study by the Center for Strategic Studies and security software maker McAfee.

"Almost every large company is dealing with constant persistent threats and network reconnaissance from hackers looking for holes and other ways into a company's systems," said Joshua Carlson, a data privacy attorney in Minnesota and a former information technology manager at Best Buy Co. "Those companies that are not ready or prepared, they can see decades and billions of dollars in (intellectual property) disappear in a few seconds."

Also at stake is the potential loss of confidential patient data. Medtronic, St. Jude Medical and Boston Scientific work closely with doctors, hospitals and medical researchers, who collect clinical trial data that can include personal information.

Data theft has become a growing problem at health care institutions. Recently, St. Joseph Health System in Bryan, Texas, said that over a three-day period in December, hackers gained access to a server containing the Social Security numbers, dates of birth, addresses and medical information of 400,000 current and former patients.

"Information is vulnerable in mass quantities," said Lisa Ikemoto, a UC Davis law professor who specializes in health care issues. "Personal information is protected for a reason."

Aside from the risk of identity theft, a patient whose information is compromised could face discrimination from employers, schools and insurers, she said.

Federal health privacy laws normally apply to doctors or hospitals, but they can also cover medical device makers who consult with physicians or help fit or test a device, Ikemoto said.

Hacking is a particularly sensitive issue between the United States and China.

Intellectual property

Last summer, amid reports that China regularly tries to steal secrets from American companies and research universities, President Obama pressed Chinese president Xi Jinping on the issue during their summit meeting in California.

"Cyberthreats and cyberattacks are only going to get more sophisticated and more impactful to those companies breached," Carlson said. "The economics of it are fairly simple: There is great reward and only slight risk for state actors, or hackers in other countries, to steal or attempt to steal as much intellectual property as it can from U.S. companies that are often decades ahead in technology and research."

Thomas Lee is a San Francisco Chronicle business editor. E-mail: tlee@sfchronicle.com