SQUIRE PATTON BOGGS

FBI WARNS OF "SPEAR PHISHING" FOR YOUR DATA AND IDEAS

August 2014

The widely reported data breach at Community Health Systems, Inc. (CHS) appears to have relied upon a "spear phish email" to launch the initial malware, according to a recent alert from the FBI. Experts engaged by CHS believe that the attacker is an "Advanced Persistent Threat." The FBI alert provides tips for organizations to prevent or identify a similar breach as well as technical information about specific network and host indicators. Companies with valuable intellectual property or with data covered by HIPAA (Health Insurance Portability and Accountability Act of 1996) are advised to heed the FBI's warning.

This is not the first such alert. In April, the FBI generally warned healthcare providers that their cybersecurity systems are lax. Unfortunately, it appears the FBI was all too correct. It is believed that foreign criminals, who may be based in China, orchestrated the largest ever external criminal cyber-attack on CHS. In the months-long attack, hackers were able to bypass CHS's security measures and successfully copy and transfer certain patient data outside the company.

The FBI warns that intellectual property also is at risk. In addition to healthcare providers, the hackers appear to be targeting entities in the medical device industry in order to steal development information about medical devices and equipment.

The attackers launched this attack with highly sophisticated malware and technology. The British Broadcasting Corporation reported that the malware was the infamous "Heartbleed" bug. Once the gateway was open, the attackers scanned the memory on networked devices for user logons and passwords. The attackers could then log on using virtual private network technology to scan and transmit data.

The CHS breach affected approximately 4.5 million individuals – patients of physicians affiliated with CHS in the last five years. The hackers did not breach the systems for clinical records but did access demographic data – patient names, addresses, birthdates, telephone numbers and social security numbers. HIPAA considers individually identifiable health information, including demographic data, as protected health information. It is possible that the hackers will use the data for identity theft purposes.

CHS recently reported that it has fixed the issue. While CHS carries cyber/privacy liability insurance it is providing appropriate notification to affected patients and regulatory agencies as required by federal and state law, and offering identity theft protection services to individuals affected by this attack.

The rapid implementation of interoperable electronic health records creates an increasingly attractive target for criminal cyber-attacks. This incident and the FBI's alert should prompt a review of system security by healthcare organizations.

Squire Patton Boggs lawyers have significant experience providing legal counsel regarding data protection issues. We continue to monitor the CHS and similar situations and are available to assist clients in structuring their privacy and security practices. For more information on how we can help you, please contact your principal Squire Patton Boggs lawyer or one of the individuals listed in this publication.

Contacts

John E. Wyand
+1 202 626 6676
john.wyand@squirepb.com

Thomas E. Zeno
+1 202 626 6213
thomas.zeno@squirepb.com

Stanford Moore
+1 614 365 2793
stanford.moore@squirepb.com

Mark D. Johnson
+1 202 626 6265
mark.johnson@squirepb.com

Lindsay Holmes
+ 1 202 626 6814
lindsay.holmes@squirepb.com

Mel M. Gates
+1 303 894 6111
melodi.gates@squirepb.com