Bloomberg Law

Health Law & Business

Prevention Needed as Cyber Extortion Pummels Health Care

By James Swann

Nov. 15, 2018 5:46AM

- *Health-care organizations are the main victims of ransomware attacks*
- *Seven of 10 providers have inadequate plans to prevent incidents*

Ransomware attackers are targeting the health-care sector at higher rates than any other part of the economy, making it critical for hospitals and physician groups to bolster cyberhack prevention.

The attacks are singling out the health-care sector due to the high financial value of health-care data, Anura Fernando, the chief innovation architect of medical systems security at Underwriters Laboratory, told Bloomberg Law.

Health-care records can fetch over $100 per record, so the sector will remain a target for ransomware and other cyberattacks for the foreseeable future, Steve Cagle, chief executive officer of Clearwater Compliance, told Bloomberg Law, said.

Because of the lucrative nature of health data, the health-care sector topped the list of ransomware victims in both 2016 and 2017. According to a report from Cylance, a cybersecurity firm in Irvine, Calif., health care organizations were the victim in 34 percent of all ransomware attacks in 2016, and in 58 percent in 2017.

The so-called Sam Sam is the latest ransomware attack to hit the health-care sector, following 2017's WannaCry and Petya attacks that shut down a number of hospital systems and health-care companies. A quarter of the victims of Sam Sam attack were health-care organizations, according to an Oct. 30 blog post from cybersecurity firm Symantec. The next closest industry was finance, which attracted just 7 percent of attacks.

Ransomware hackers enter systems and encrypt data, making them impossible for hospitals and physicians to access; they demand payment from the providers to regain network access. Sources say 70 percent of providers are incapable of stopping such attacks.

Proactive, Not Reactive

Only 29 percent of U.S. health systems have a comprehensive cybersecurity program in place, according to an Oct. 31 report released by the College of Healthcare Information Management Executive.

Hospitals and especially physicians need to change their mindset from complying with federal security rules, to implementing a comprehensive information security program, attorney Alisa Chestler, with Baker, Donelson in Nashville, told Bloomberg Law.

For example, the Health Insurance Portability and Accountability Act's Privacy and Security rules' focus on reacting to data breaches rather than proactively implementing a security program to deter a breach in the first place, Chestler said. HIPAA rules impose penalties for lost or hacked patient information, but do not tell providers how to achieve cybersecurity.

Prioritized at the Highest Level

A big help in preventing ransomware attacks is for health-care companies to include cybersecurity as a top concern at the board level, Cagle said.

Instead, they treat it as a compliance issue, so when an attack happens, the board doesn't know where to focus resources, Cagle said. Nashville, Tenn.-based Clearwater offers cybersecurity risk management services.

On the other hand, health-care organizations increasingly are collaborating and sharing data, which Cagle says are among are keys to improving cybersecurity. The HHS cybersecurity task force included a number of hospitals systems that were working together, Fernando, a former task force member, said.

Attacks can be launched by unwitting employees, clicking e-mail attachments and having weak passwords, Attackers exploit the vulnerabilities, seizing control over the health organization's computer network and then disabling access to patient data.

More Best Practices

Training employees is the most basic step hospitals and physicians can take to ward off or mitigate cyberattacks, Robert Tennant, director of health information technology policy at the Englewood, Colo.-based Medical Group Management Association, told Bloomberg Law.

For example, health-care staff should be very careful about opening any e-mails or e-mail attachments that look suspicious or come from a source that's not recognized, Tennant said. Ransomware attacks often piggyback on an e-mail attachment, and when a user clicks it on it the hackers can get access to an organization's network.

Weak user authentication was identified as the number one cybersecurity risk facing health-care organizations in an November bulletin from the Clearwater Cyberintelligence Institute, accounting for 14 percent of all critical and high security cyber risks.

Endpoint leakage accounted for 12 percent of the risks, and excessive user permissions rounded out the top three at 12 percent. Endpoint leakage refers to data that's stolen or corrupted after being received by mobile devices, laptops, and desktop personal computers.

Organizations should also make sure to keep all computer systems patched and up-to-date. 2017's WannaCry and Petya attacks capitalized on outdated software gain access to company networks, Tennant said.

The health-care sector also needs knowledgeable cybersecurity staff, which is currently in short supply, Fernando said.

No plan is foolproof however, so health-care organizations should consider buying cybersecurity insurance, Tennant said. An insurance policy can help cover costs associated with an attack, such as reaching out to patients affected by an attack and paying for identity monitoring services, Tennant said.

To contact the reporter on this story: James Swann in Washington at jswann1@bloomberglaw.com

To contact the editors responsible for this story: Fawn Johnson at fjohnson@bloomberglaw.com; Todd Leeuwenburgh at tleeuwenburgh@bloomberglaw.com