Bloomberg BNA

Health Law Resource Center™

Health Information

Cyber Extortion Schemes Undermining Patient Care

By James Swann

Cyber extortion schemes are proliferating in the health-care sector, raising the risks of illegal disclosure of millions of medical records and potentially undermining patient care.

"Beyond the threat of crippling financial demands from a hacker, there's the terrifying prospect of denial of service attacks on certain medical devices that could interfere with a facility's clinical capabilities and disrupt treatment," Jeremy D. Sherer, a health-care attorney with Hooper, Lundy & Bookman PC in Boston, told Bloomberg Law Feb. 7.

Snapshot

- Cyber extortion can expose medical records and harm patient care
- Providers need to keep up-to-date with their software patches

Basic cyber extortion schemes involve hackers encrypting or blocking access to health-care data and requesting money to restore the data.

In some cases, a hacker can freeze a health organization's entire computer system, preventing doctors from reviewing patient records and performing procedures. Medical records can also be held hostage, with a hacker promising to sell them if payment isn't received.

For example, Hancock Regional Hospital in Greenfield, Ind., was targeted by hackers in early January and ended up paying $50,000 to recover use of its computer systems. Hancock didn't respond to a request for comment on the attack.

St. Louis-based Ascension Health, the largest nonprofit health-care system in the country, didn't respond to a request for comment on the threat of cyber extortion attacks. Dallas-based Tenet Healthcare, one of the nation's largest for-profit health systems, said it was unable to respond to questions about its cyber threat strategy.

Ascension operates 2,500 health-care facilities in 22 states and the District of Columbia, while Tenet operates 99 hospitals and more than 450 outpatient facilities.

The impact of a cyber extortion attack is huge, because the hackers often threaten to shut down an organization's electronic health record system if money isn't paid, Lisa W. Clark, a health-care attorney with Duane Morris LLP in Philadelphia, told Bloomberg Law Feb. 7.

Hospitals and other health-care providers can't treat patients without EHR systems, as they contain everything from a patient's identification to what types of medication they're taking.

Growing Threat

Last year's Petya and WannaCry attacks have raised industry awareness of the risks facing hospital computer systems and networked medical devices. The Petya attack locked up data at New Jersey-based pharmaceutical manufacturer Merck, while WannaCry crippled more than 16 British hospitals and 200,000 computers in 150 countries.

A recent government update classified cyber extortion as a major source of disruption for health-care organizations, and cybersecurity experts say the attacks are likely to grow in intensity.

"Cyber extortion, particularly ransomware, has become an epidemic problem for health-care organizations," W. Reece Hirsch, a health-care attorney with Morgan, Lewis & Bockius LLP in San Francisco, told Bloomberg Law Feb. 7.

Ransomware is one of many possible cyber extortion schemes and happens when a hacker steals data from an organization and threatens to publish it unless a ransom is paid, Hirsch, a Bloomberg Law advisory board member, said.

Mitigation

Extortion schemes come in many flavors beyond ransomware, including denial of service and distributed denial of service attacks, both of which have become more commonplace, according to the Health and Human Services Office for Civil Rights.

The two attacks involve flooding a computer system with emails and other internet traffic, which can overwhelm the system and eventually shut it down. Hackers then demand money to stop the attack.

Training and education are critical in preventing and mitigating cyber extortion, Sherer said. Health-care facilities need to implement training programs that teach employees to identify irregular emails and other messages that hackers could use to access a computer system, Sherer said.

"Running drills that involve sending fake, suspicious-looking emails to employees is one tool that facilities can use to see just how effective their training programs really are, and alert them to which employees may need extra training," Sherer said.

Risk analysis and risk management are key to hardening defenses against cyber extortion, Hirsch said, as they can help an organization find out where vulnerabilities exists.

When responding to an actual attack, health-care organizations should collect as much information as possible such as the exact type and variant of the any malware discovered, the algorithmic steps taken by the malware, and whether the malware communicated with the hackers to steal any data, Hirsch said.

Backup Plans

While collecting information can help prepare for future attacks, Hirsch said, encrypting data and backing up sensitive data are two of the most important steps to take in protecting against ransomware and other cyber extortion schemes.

An effective back-up plan is crucial, Sherer said, and the Health Insurance Portability and Accountability Act Security Rule already requires organizations to develop and implement a security management process that includes creating a data back-up plan and establishing a contingency plan to keep operations running in case of an attack, Sherer said.

Health-care organizations should periodically test their back-up and contingency plans, Sherer said.

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

To contact the editor responsible for this story: Kendra Casey Plank at kcasey@bloomberglaw.com •