CRS INSIGHT

Ransomware Attacks Renew Focus on HIPAA Security Standards

June 5, 2017 (IN10714)

|

Related Author

- C. Stephen Redhead

|

C. Stephen Redhead, Specialist in Health Policy (credhead@crs.loc.gov, 7-2261)

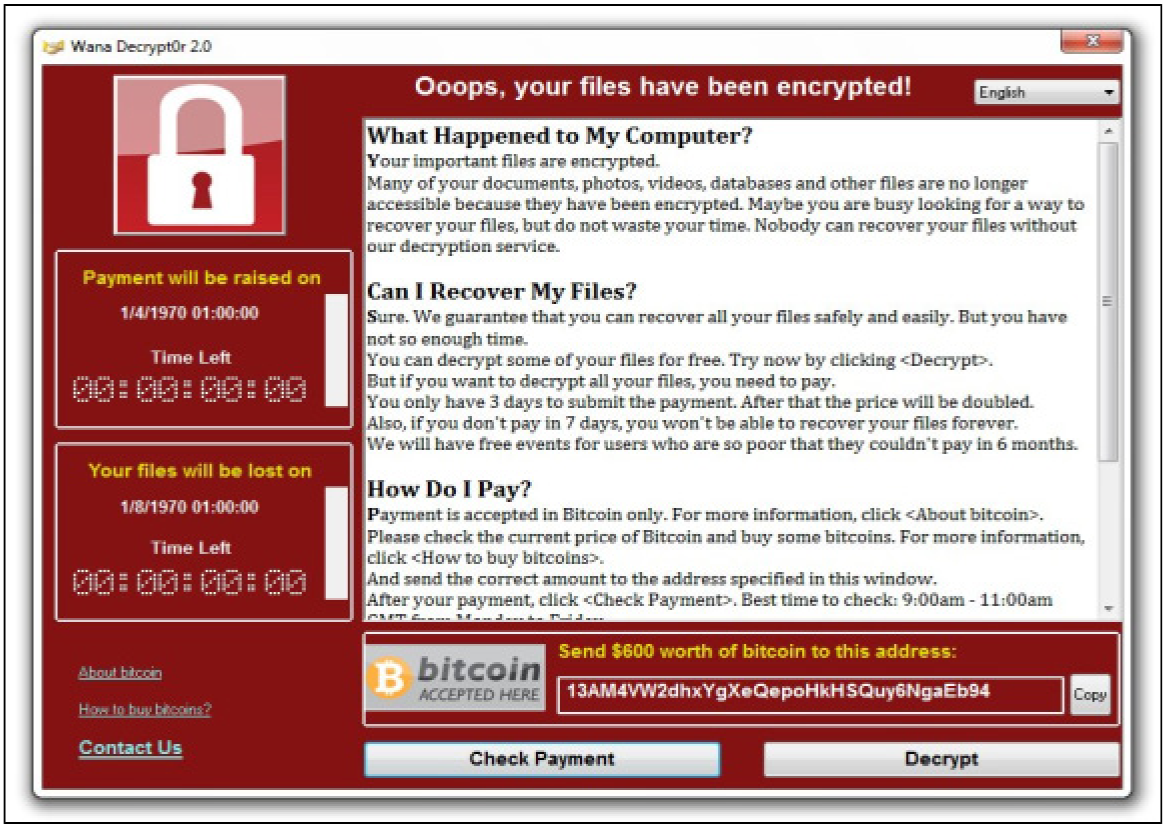
Health care facilities increasingly are coming under cyberattack. This trend has raised concerns about the vulnerability of electronic health information, which often includes multiple personal identifiers. These can be used by hackers to create false identities for illegal purposes such as creating fraudulent insurance claims.

But health care cybersecurity involves more than just safeguarding patient data from identity theft. Hackers are now using ransomware to attack hospitals and other health care facilities in an effort to extort money by disrupting their operations.

Ransomware is a type of malicious software that prevents victims from accessing their data—typically by encrypting the data using a key known only to the hacker—unless a ransom is paid in cryptocurrency (bitcoins). By denying a health care facility access to its data, ransomware attacks may put patients' lives at risk.

Last month, ransomware known as WannaCry infected computer systems in more than 150 countries (see **Figure 1**). WannaCry spread by exploiting a weakness in computers running older Windows operating systems. Britain's National Health Service was especially hard hit. Some hospitals canceled surgeries and turned patients away from emergency rooms.

Figure 1. WannaCry Ransomware Screenshot



Ooops, your files have been encrypted!

Payment will be raised on
1/4/1970 01:00:00
Time Left
00:00:00:00

Your files will be lost on
1/8/1970 01:00:00
Time Left
00:00:00:00

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $600 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

Source: https://www.cyber.nj.gov/threat-profiles/ransomware-variants/wannacry?rq=wannacry.

HIPAA Compliance Helps Health Facilities Prevent and Respond to Cyberattacks

Health care providers that handle protected health information (PHI) in electronic form are subject to the Health Insurance Portability and Accountability Act (HIPAA) security standards. These are intended to ensure the confidentiality, integrity, and availability of electronic PHI; prevent its unauthorized use and disclosure; and protect it from reasonably anticipated security threats, including ransomware and other cyberattacks.

The first standard requires health care facilities to implement a security management process, which forms the foundation upon which all subsequent HIPAA security activities are based. Facilities must conduct an accurate and thorough risk analysis to identify potential risks and vulnerabilities to electronic PHI (ePHI), and implement security measures to reduce those risks and vulnerabilities to a reasonable and appropriate level.

Other standards help health care facilities respond to and recover from cyberattacks. For example, facilities are required to implement security incident procedures enabling them to identify and respond to cyberattacks and other security incidents; mitigate, to the extent practicable, the harmful effects of incidents; and document incidents and their outcomes.

Facilities must develop contingency plans that can be activated in response to an attack, allowing them to continue their operations. Contingency planning must include a plan for backing up data—which is crucial in the event of a ransomware attack that blocks access to the primary data source—as well as a recovery plan to restore any loss of data, and a plan for continuing to secure ePHI while operating in emergency mode.

Finally, health care facilities must establish security awareness and training programs so that their workforce is better able to detect and respond to attacks.

The HIPAA security standards are flexible and scalable, as they must apply to entities ranging from the largest health care organization to the smallest provider practice. When implementing the standards, each entity must take into account its size and complexity, its technical capabilities, the security risks and vulnerabilities that it faces, and implementation costs. The standards also are technology-neutral, allowing entities to take advantage of the continual emergence of new technologies.

Some Health Care Facilities Find Compliance a Challenge

Audits conducted by the Department of Health and Human Services' (HHS's) Office for Civil Rights have identified multiple areas of noncompliance with the HIPAA standards. They include incomplete or inaccurate risk analyses that fail to identify all the potential risks and vulnerabilities; failure to manage identified risks; use of unpatched or unsupported software—a key vulnerability exploited by WannaCry; and insufficient contingency planning and data backup.

Health care providers complain that the standards are not sufficiently prescriptive. Each standard describes what to do but not how to do it. For example, while each facility must implement a security training and awareness program, there are no specific instructions about the content and frequency of such programs.

In view of the growing number of cyberattacks, some security experts question whether heath care facilities should be given so much latitude in implementing the HIPAA standards versus having to meet a more prescribed set of requirements. Other experts argue that the standards—which have not been amended since they were issued in 2003—do not adequately capture the realities of today's digital technology or address modern cybersecurity challenges.

Information Sharing and Breach Notification

The federal government recognizes the importance of sharing information about cyberattacks. This is reflected in Executive Order 13691, promoting private sector cybersecurity information sharing, and enactment of the Cybersecurity Information Sharing Act (CISA) of 2015. CISA encourages the sharing of cyber threat indicators with the federal government and others to alert them to possible or actual threats or vulnerabilities, and to describe the possible or actual harm caused by cyber incidents. Typically, PHI is not needed to describe such threats and vulnerabilities. Under the HIPAA Privacy Rule, disclosure of PHI for cybersecurity information sharing generally requires patient authorization except in certain circumstances (e.g., to comply with a court order).

HHS recommends that health care facilities report cyberattacks to the United States Computer Emergency Readiness Team (US-CERT), which develops timely and actionable information on cybersecurity. US-CERT is part of the National Cybersecurity and Communications Integration Center within the Department of Homeland Security (NCCIC). HHS also recommends that health care facilities contact the FBI in the event of a cyberattack.

HHS is launching its own version of NCCIC to improve health care cybersecurity. One goal is to develop best practices and disseminate them to smaller practices.

Breach notification is an important part of incident management. Ransomware attacks are presumed to be a breach under HIPAA unless the health care facility conducts a post-event assessment and shows that there is a low probability that ePHI was compromised. Breaches must be reported to HHS within 60 days unless the FBI puts a hold on the release while investigating the incident.