How to Prevent Healthcare Cyber Extortion

Save to myBoK

By Chris Dimick

Cybercrime may seem like a rare, unlikely risk to some healthcare providers. But the threat is real—and rising—whether a healthcare facility is small or large, rural or urban. According to a January 2018 report commissioned by cybersecurity firm Sophos that surveyed 2,700 IT managers, healthcare IT professionals reported more ransomware attacks in the preceding 12 months than any other industry. A total of 76 percent of healthcare organizations polled reported they suffered a cyberattack, compared to 45 percent of financial services companies.[1] "Healthcare is often perceived as a soft target, leading to increased frequency of attack," the report states. (Read more about this report on page 10.) Federal officials continue to warn all healthcare providers to prepare for a potential cyberattack—and take steps to mitigate risk. The first step is understanding just what types of cybercrime are possible.

Incidents of cybercrime, like cyber extortion, are rising in the healthcare industry and will continue to be a major source of disruption for providers in the coming years. In order to combat this crime, the Department of Health and Human Services' (HHS') Office for Civil Rights (OCR) has released further guidance describing what cyber extortion is and what to do if a healthcare organization becomes a victim.

OCR's January Cybersecurity Newsletter listed the various forms of cyber extortion and things healthcare organizations can do to reduce the chances of becoming a victim. "Cyber extortion can take many forms, but it typically involves cybercriminals' demanding money to stop (or in some cases, to merely delay) their malicious activities, which often include stealing sensitive data or disrupting computer services," the OCR newsletter states.[2] "Organizations that provide necessary services or maintain sensitive data, such as Healthcare and Public Health sector organizations, are often the targets of cyber extortion attacks."

Preventing Ransomware

Ransomware is a common form of cyber extortion where attackers deploy malicious software, known as malware, targeting a healthcare organization's data to render it inaccessible—usually through encryption, OCR states. Attackers then demand payment to unencrypt a provider's data. Paying this ransom, OCR notes, may not result in an organization getting all or even a portion of its data back. OCR recommends providers read a fact sheet that provides guidance on preventing and responding to ransomware attacks for HIPAA-covered entities and their business associates.[3]

A recent US government interagency report indicated that, on average, there have been 4,000 daily ransomware attacks since early 2016. This is a 300 percent increase over the 1,000 daily ransomware attacks reported in 2015.[4]

Organizations that already take measures to ensure compliance with HIPAA are better positioned to prevent infections of malware in their systems, according to HHS. The HIPAA Security Rule requires implementation of security measures that can help prevent the introduction of malware, including ransomware. Some of these required security measures include:

- Implementing a security management process, which includes conducting a risk analysis to identify threats and vulnerabilities to electronic protected health information (ePHI) and implementing security measures to mitigate or remediate those identified risks
- Implementing procedures to guard against and detect malicious software
- Training users on malicious software protection so they can assist in detecting malicious software and know how to report such detections
- Implementing access controls to limit access to ePHI to only those persons or software programs requiring access

Preventing Denial of Service Attacks

Another common form of cyber extortion is Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. These attacks direct a high volume of internet network traffic at a targeted computer to render it unable to function or to make it appear inaccessible to legitimate users, OCR says. “In this type of attack, an attacker may initiate a DoS or DDoS attack against an organization and demand payment to halt the attack, or the attacker could threaten an attack and demand payment to not initiate the attack,” OCR states.

An attacker can overload a server with numerous requests so that valid users cannot get through to the site. Also, an attacker can utilize spam email messages to flood a user’s email account. For example, an attacker may send countless or large email messages to email accounts, causing the users to consume their email quota and preventing them from receiving or sending emails, according to OCR.

OCR recommends providers read another tip sheet it developed for identifying possible DoS or DDoS attacks and taking steps to prevent them.[5] To prevent the possibility of being a target of DoS or DDoS attacks, OCR recommends in the tip sheet that providers:[6]

- Continuously monitor and scan for vulnerable and compromised internet-connected devices on their networks and follow proper remediation actions.
- Create and implement password management policies and procedures for devices and their users, ensuring all default passwords are changed to strong passwords.
- Install and maintain anti-virus software and security patches, updating internet-connected devices with security patches as soon as patches become available.
- Install a firewall and configure it to restrict traffic coming into and leaving the network and its systems.
- Segment networks where appropriate and apply appropriate security controls to control access among network segments.
- Disable Universal Plug and Play (UPnP) on routers unless it is absolutely necessary.
- Practice and promote security awareness. It is important to be aware and understand the capabilities of IT systems, medical devices, and HVAC systems with network capabilities that are installed on healthcare providers’ networks. If the device has an open wi-fi connection and transmits data or can be operated remotely, then it has the potential to be infected.
- Follow good security practices for distributing email addresses; applying email filters may help entities manage unwanted traffic.

Continue to Be Vigilant

Because cyberattackers constantly create new versions of malicious software and search for new vulnerabilities to exploit, organizations must “continue to be vigilant in their efforts to combat cyber extortion,” OCR wrote. OCR recommends healthcare organizations take the following steps to reduce the chances of being a victim of cyber extortion:

- Implement a robust risk analysis and risk management program that identifies and addresses cyber risks holistically, throughout the entire organization.
- Implement robust inventory and vulnerability identification processes to ensure accuracy and thoroughness of the risk analysis.
- Train employees to better identify suspicious emails and other messaging technologies that could introduce malicious software into the organization.
- Deploy proactive anti-malware solutions to identify and prevent malicious software intrusions.
- Patch systems to fix known vulnerabilities that could be exploited by attackers or malicious software.
- Harden internal network defenses and limit internal network access to deny or slow the lateral movement of an attacker and/or propagation of malicious software.
- Implement and test robust contingency and disaster recovery plans to ensure an organization is capable and ready to recover from a cyberattack.
- Encrypt and back up sensitive data.
- Implement robust audit logs and review such logs regularly for suspicious activity.
- Remain vigilant for new and emerging cyber threats and vulnerabilities (for example, by receiving United States Computer Emergency Readiness Team alerts and participating in information sharing organizations).

For more information on cybersecurity resources from OCR, visit www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html.

Notes

1. Sophos. "The State of Endpoint Security Today." White paper. January 2018. https://secure2.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/endpoint-survey-report.pdf?la=en.
2. Department of Health and Human Services Office for Civil Rights. "Cyber Extortion." Cybersecurity Newsletter. January 2018. www.hhs.gov/sites/default/files/cybersecurity-newsletter-january-2018.pdf.
3. Department of Health and Human Services. "Fact Sheet: Ransomware and HIPAA." www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.
4. United States Department of Justice. "How to Protect Your Networks from Ransomware." www.justice.gov/criminal-ccips/file/872771/download.
5. Department of Health and Human Services Office for Civil Rights. "Understanding DoS and DDoS Attacks and Best Practices for Prevention." Cybersecurity Newsletter. November 2016. www.hhs.gov/sites/default/files/december-2016-cyber-newsletter.pdf.
6. Ibid.

Chris Dimick (chris.dimick@ahima.org) is editor-in-chief of the *Journal of AHIMA*.
