Published on *The National Law Review* https://natlawreview.com

New OCR Checklist Outlines How Health Care Facilities Can Fight Cyber Extortion

Article By:

Matthew S. Arend

Sydney N. Pahren

As technology has advanced, cyber extortion attacks have risen, and they will continue to be a major security issue for organizations. Cyber extortion can take many forms, but it typically involves cybercriminals demanding money to stop or delay their malicious activities, which include stealing sensitive data or disrupting computer services. Health care and public health sector organizations that maintain sensitive data are often targets for cyber extortion attacks.

Ransomware is a form of cyber extortion where attackers deploy malware targeting an organization's data, rendering it inaccessible, typically by encryption. The attackers then demand money in exchange for an encryption key to decrypt the data. Even after payment is made, organizations may still lose some of their data.

Other forms of cyber extortion include Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. These attacks normally direct a high volume of network traffic to targeted computers so the affected computers cannot respond and are otherwise inaccessible to legitimate users. Here, an attacker may initiate a DoS or DDoS attack against an organization and demand payment to stop the attack.

Additionally, cyber extortion can occur when an attacker gains access to an organization's computer system, steals sensitive data from the organization and threatens to publish that data. The attacker threatens revealing sensitive data, including protected health information (PHI), to coerce payment.

On January 30, 2018, the HHS Office for Civil Rights (OCR) published a checklist to assist HIPAA covered entities and business associates on how to respond to a cyber extortion attack. Organizations can reduce the chances of a cyber extortion attack by:

- Implementing a robust risk analysis and risk management program that identifies and addresses cyber risks holistically, throughout the entire organization;
- Implementing robust inventory and vulnerability identification processes to ensure accuracy and thoroughness of the risk analysis;
- Training employees to better identify suspicious emails and other messaging technologies

that could introduce malicious software into the organization;
- Deploying proactive anti-malware solutions to identify and prevent malicious software intrusions;
- Patching systems to fix known vulnerabilities that could be exploited by attackers or malicious software;
- Hardening internal network defenses and limiting internal network access to deny or slow the lateral movement of an attacker and/or propagation of malicious software;
- Implementing and testing robust contingency and disaster recovery plans to ensure the organization is capable and ready to recover from a cyber-attack;
- Encrypting and backing up sensitive data;
- Implementing robust audit logs and reviewing such logs regularly for suspicious activity; and
- Remaining vigilant for new and emerging cyber threats and vulnerabilities.

If a cyber extortion attack does happen, organizations should be prepared to take the necessary steps to prevent any more damage. In the event of a cyber-attack or similar emergency an entity:

- Must execute its response and mitigation procedures and contingency plans;
- Should report the crime to other law enforcement agencies, which may include state or local law enforcement, the Federal Bureau of Investigation (FBI) and/or the Secret Service. Any such reports should not include protected health information, unless otherwise permitted by the HIPAA Privacy Rule;
- Should report all cyber threat indicators to federal and information-sharing and analysis organizations (ISAOs), including the Department of Homeland Security, the HHS Assistant Secretary for Preparedness and Response, and private-sector cyber-threat ISAOs.
- Must report the breach to OCR as soon as possible, but no later than 60 days after the discovery of a breach affecting 500 or more individuals, and notify affected individuals and the media unless a law enforcement official has requested a delay in the reporting. An entity that discovers a breach affecting fewer than 500 individuals has an obligation to notify individuals without unreasonable delay, but no later than 60 days after discovery; and OCR within 60 days after the end of the calendar year in which the breach was discovered.

National Law Review, Volume VIII, Number 33