January 2018

Cyber Extortion

Incidents of cyber extortion have risen steadily over the past couple of years and, by many estimates, will continue to be a major source of disruption for many organizations. 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. Organizations that provide necessary services or maintain sensitive data, such as Healthcare and Public Health (HPH) sector organizations are often the targets of cyber extortion attacks. The HHS Office for Civil Rights (OCR) published a checklist[1] and accompanying infographic[2] to assist HIPAA covered entities and business associates on how to respond to a cyber-attack.

Ransomware is a form of cyber extortion whereby the attackers deploy malware targeting an organization's data that renderers the data inaccessible, typically by encryption. The encryption key must be obtained from the ransomware attackers to decrypt the data. The ransomware attackers demand payment, often in the form of cryptocurrency (e.g., Bitcoin) for that decryption key. Unfortunately, paying ransom to the attackers may not result in an organization getting its data back. Or, once an organization pays the ransom, the attackers may provide a key to only decrypt a portion of the data and ask for additional ransom to decrypt more data. OCR published a fact sheet (*Fact Sheet: Ransomware and HIPAA*) that provided guidance on preventing and responding to ransomware attacks for HIPAA covered entities and business associates.[3]

Additional examples of cyber extortion include Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. These types of attacks typically direct such a high volume of network traffic to targeted computers that the affected computers cannot respond and may appear down or otherwise inaccessible to legitimate users. 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 highlighted DoS and DDoS attacks in a prior cybersecurity newsletter, which included tips on identifying possible attacks as well as steps to take in the event of an attack.[4]

[1] https://www.hhs.gov/sites/default/files/cyber-attack-checklist-06-2017.pdf
[2] https://www.hhs.gov/sites/default/files/cyber-attack-quick-response-infographic.gif
[3] https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf
[4] https://www.hhs.gov/sites/default/files/december-2016-cyber-newsletter.pdf

Another type of cyber extortion occurs when an attacker gains access to an organization's computer system, steals sensitive data from the organization, and then threatens to publish that data. The attacker uses the threat of publically exposing an organization's sensitive data, which could include protected health information (PHI), to coerce payment. In this type of attack, the attacker already has the organization's data and can sell that data to other malicious persons even after the ransom is paid. A variation of this type of attack occurs when an attacker steals sensitive data from an organization and then deletes that data from the organization's computers. The attackers then contact the organization informing them that its data has been deleted, but will be returned in exchange for payment. Again, payment of the ransom is no guarantee that an organization will get its data back. In fact, there have been instances where one attacker has stolen and deleted an organization's data while leaving a demand for payment only to have a second attacker gain access to the same computer system and overwrite the payment demand of the first attacker. In this circumstance, the second attacker didn't even have the data, so the organization has no chance of retrieving data from the second attacker.

Although cyber attackers 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. Examples of activities organizations should consider to reduce the chances of being a victim of cyber extortion include:

- 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 (for example, by receiving US-CERT alerts and participating in information sharing organizations[5]).

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

[5] https://www.hhs.gov/sites/default/files/february-2017-ocr-cyber-awareness-newsletter.pdf