Fall 2019 OCR Cybersecurity Newsletter

What Happened to My Data?: Update on Preventing, Mitigating and Responding to Ransomware

Ransomware is a type of malicious software (or malware) that attempts to deny access to a user's data, usually by encrypting the data with a key known only to the attacker who deployed the ransomware. In order for a victim to obtain this key, a ransom payment, which is usually made in cryptocurrency,[1] is required. These types of attacks pose a serious threat to HIPAA covered entities, business associates, and the electronic protected health information (ePHI) that they hold.

This newsletter will supplement the materials OCR has previously published on how the HIPAA Security Rule can help prevent, mitigate and recover from ransomware attacks[2] by providing insight into new developments and trends that have been observed regarding ransomware attacks and how organizations can improve their security posture in response to this threat.

Evolution of Ransomware Attacks

Prior to 2018, most ransomware attacks involved mass, indiscriminate infection of as many devices and across as many systems as possible.[3] These infections often spread automatically through dedicated connections between networks and spam phishing emails. These attacks led to worldwide events caused by ransomware variants of Petya, WannaCry, CryptoLocker, and others. The May 2017 WannaCry attack alone was estimated to have affected over 200,000 computer systems in over 150 countries with monetary damages estimated into the hundreds of millions to billions of dollars.[4] This attack was reported to have caused the United Kingdom's National Health Services to cancel thousands of medical appointments and divert patients to alternate facilities.[5] The wide net cast by these ransomware attacks affected individuals and organizations of all sizes, including many covered entities and business associates.

The FBI estimates that ransomware infects more than 100,000 computers a day around the world and ransom payments approach $1 billion annually;[6] unfortunately, these numbers are only expected to rise in the future. Ransom payments, however, do not account for all of the costs associated with a ransomware attack. Unrecoverable data, lost productivity, damage to reputation, damaged equipment, forensic investigations, remediation expenses, and legal bills are some of the additional costs that can be expected when responding to a ransomware attack. The actual cost of a ransomware attack may be several times more than just the ransom paid. In 2017, the U.S. Department of Justice called the use of ransomware a global phenomenon and a new business model for cybercrime.[7]

In response to this new cyberthreat, organizations and governments began adapting. Anti-malware vendors updated their products to help customers identify, prevent, and contain infections. Cybersecurity researchers and scientists studied ransomware code and, in some cases, were able to reverse engineer decryption keys to help ransomware victims recover data without paying the ransom. Organizations prioritized incident response and data backups in order to mitigate the damage caused by ransomware attacks. However, as organizations adapted, ransomware developers evolved.

In 2017 and 2018, a new threat rapidly emerged: the targeted ransomware attack. A targeted ransomware attack is loosely defined as a ransomware attack that is adapted to a specific organization or industry. In such incidents, ransomware can be customized and deployed based on the size and sophistication of a potential victim, the sensitivity of data, and the malware code can be adjusted to be more effective in certain situations, for example, by exploiting specific vulnerabilities present in targeted systems. The ransom demands for this type of attack are often set according to the victim's perceived ability to pay.[8] Cybercriminals soon found that customizing their attacks to specific, "quality" targets led to an increase in the amount of ransom payments. Organizations commonly targeted by this type of attack have sensitive data, high data availability requirements, low tolerance for system downtime, and the resources to pay a ransom. Many healthcare organizations fit this profile, and have become targets.

The targeted attack's tailored approach is what makes it so effective and dangerous and is what sets it apart from the previous type of mass-produced ransomware attack. Prior to initiating an attack, a malicious actor usually gains unauthorized access to a victim's information system for the purpose of performing reconnaissance to identify critical services, find sensitive data, and locate backups. After this is done, the ransomware is deployed in a manner that produces maximum effect, infecting as many devices and as much data as possible and encrypting backup files so that recovery is difficult, if not impossible. In such a case, an unprepared victim may be forced to make an unpleasant choice: refuse to pay the ransom and lose all of the affected data or pay and hope it can make a full recovery (assuming the attacker provides the decryption keys necessary to decrypt the affected data after receiving payment).

Prevention, Mitigation, and Recovery

Although threat actors have employed new means for identifying victims, their overall methods of gaining unauthorized access to systems and deploying ransomware remain generally the same. Phishing emails and vulnerability exploitation (e.g., exploiting unpatched operating system or application vulnerabilities) continue to be the most common attack vectors.

Entities should be mindful that ransomware attacks often occur after prior instances of unauthorized access and malware infection. A threat actor sometimes needs to have access and privileges on a victim's information system in order to initiate the infection. Further, certain types of ransomware have been observed to "piggyback" into a system, using other malware as a tool for deployment. Proper implementation of several HIPAA Security Rule provisions can help covered entities and business associates prevent, mitigate, and recover from ransomware attacks, including:

Risk Analysis (45 C.F.R. §164.308(a)(1)(ii)(A)) and Risk Management (45 C.F.R. §164.308(a)(1)(ii)(B)). Covered entities and business associates are required to conduct a thorough and accurate assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of their ePHI, and implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. Identifying and addressing technical vulnerabilities within information systems and information technology infrastructure is crucial to preventing ransomware attacks. Successful ransomware deployment often depends on exploitation of technical vulnerabilities such as outdated software, unsecured ports, and poor access management/provisioning. Implementing effective security tools

including anti-malware software and intrusion detection/prevention solutions can also help prevent, detect, and contain attacks. Identifying and reducing these potential risks and vulnerabilities is key to making an organization a less inviting target.

Information System Activity Review (45 C.F.R. §164.308(a)(1)(ii)(D)). If ransomware is able to overcome an organization's first level of defenses and enter the organization's network and information systems, effective system monitoring and review will be critical to detecting and containing the attack. Identifying anomalous activity, especially such activity executed with elevated privileges, can be crucial to identifying an attack in progress. Covered entities and business associates are required to regularly review records of information system activity. Such records can include audit logs, access reports, and security incident tracking reports. Some organizations may benefit from tools to assist with log collection and review processes. Security Information and Event Management solutions can assist an organization with its activity review process by aggregating and helping to analyze logs and reports from many different information systems.

Security Awareness and Training (45 C.F.R. §164.308(a)(5)). Information system users remain one of the weakest links in an organization's security posture. Social engineering, including phishing attacks, is one of the most successful techniques used by threat actors to compromise system security. A training program should make users aware of the potential threats they face and inform them on how to properly respond to them. This is especially true for phishing emails that solicit login credentials. Additionally, user training on how to report potential security incidents can greatly assist in an organization's response process by expediting escalation and notification to proper individuals.

Security Incident Procedures (45 C.F.R. §164.308(a)(6)). An organization's incident response procedures can greatly limit the damage caused by a ransomware attack. Organizations may consider addressing ransomware attacks specifically within its response policies and procedures as mitigation actions may vary between different types of incidents. Quick isolation and removal of infected devices from the network and deployment of anti-malware tools can help to stop the spread of ransomware and to reduce the harmful effects of such ransomware. Response procedures should be written with sufficient details and be disseminated to proper workforce members so that they can be implemented and executed effectively. Further, organizations may consider testing their security incident procedures from time to time to ensure they remain effective. Familiarity with the execution of security incident procedures should reduce an organization's reaction time and increase its effectiveness when responding to an actual security incident or breach. Identifying and responding to suspected security incidents is key to mitigating potential harm following an intrusion.

Contingency Plan (45 C.F.R. §164.308(a)(7)). An effective and robust contingency plan is essential to recover from a ransomware attack. Proper implementation of this provision will allow an organization to continue to operate critical services during an emergency and recover ePHI. Because patient health and safety may be impacted, tolerance of system downtime is low and ePHI availability requirements are high. A covered entity or business associate must backup ePHI and ensure that it is accessible and recoverable in the event of a ransomware attack. Organizations should keep in mind that threat actors have recently been actively targeting backup systems and backup data to prevent recovery. Maintaining recoverable, secure, and up-to-date backups is one of the most important safeguards against ransomware attacks.

The foregoing measures (and associated Security Rule provisions) are **not** an exhaustive list of measures to prevent and recover from a ransomware attack. Covered entities and business associates may also want to consider these additional Security Rule provisions:

- Implementing effective access controls (see 45 C.F.R. § 164.312(a)(1) (access control)) to stop or impede an attacker's movements and access to sensitive data; e.g., by segmenting networks to limit unauthorized access and communications. Further, because attacks frequently seek elevated privileges (e.g., administrator access), entities may consider solutions that limit the scope of administrator access, as well as solutions requiring stronger authentication mechanisms when granting elevated privileges or access to administrator accounts.
- Ensuring that security measures remain effective as technology changes and new threats and vulnerabilities are discovered (see 45 C.F.R. § 164.306(e) (maintenance)); e.g., by updating or patching software and devices to mitigate known vulnerabilities.

The emergence of targeted attacks shows that threat actors are adapting to steps taken by organizations to combat the risk of ransomware infections. So far, these adaptations have proved to be successful, which suggests that ransomware attacks will continue to remain a serious threat to covered entities, business associates, and ePHI for the foreseeable future. However, advances in malware detection and containment tools can assist entities in identifying intrusions into their IT system and initiating defenses before their data is encrypted. Further, the implementation of the robust security measures required by HIPAA can prevent or greatly reduce the impact of ransomware attacks.

Should an Entity Pay the Ransom?

The FBI does not recommend paying the ransom demanded by the initiator of the ransomware attack, as payment does not guarantee that an entity's data will be returned, and payment could provide encouragement for further ransomware attacks.[9] The FBI has noted that there have been instances where the decryption key was not provided after the ransom was paid, or the data was corrupted when it was returned. The FBI recommends always reporting ransomware incidents to law enforcement, to prevent future attacks and to enable a criminal investigation to be initiated.[10]

Please see the following resources for additional information:

How to Protect your Networks from Ransomware

https://www.us-cert.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf - PDF

Ransomware

https://www.us-cert.gov/Ransomware

* This document is not a final agency action, does not legally bind persons or entities outside the Federal government, and may be rescinded or modified in the Department's discretion.

[1] Cryptocurrency is an encrypted digital currency that facilitates the exchange of funds outside of a central bank. Examples include Bitcoin and Litecoin. More than one thousand cryptocurrencies are available today.

[2] https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf - PDF

[3] https://www.ic3.gov/media/2019/191002.aspx

[4] https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

[5] https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf - PDF

[6] https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-cambridge-cyber-summit

[7] Id.

[8] https://www.us-cert.gov/ncas/current-activity/2019/06/28/ncsc-releases-advisory-ryuk-ransomware

[9] https://www.ic3.gov/media/2019/191002.aspx.

[10] Id.

Frequently Asked Questions for Professionals - Please see the HIPAA FAQs for additional guidance on health information privacy topics.

Content created by Office for Civil Rights (OCR)

Content last reviewed on December 2, 2019