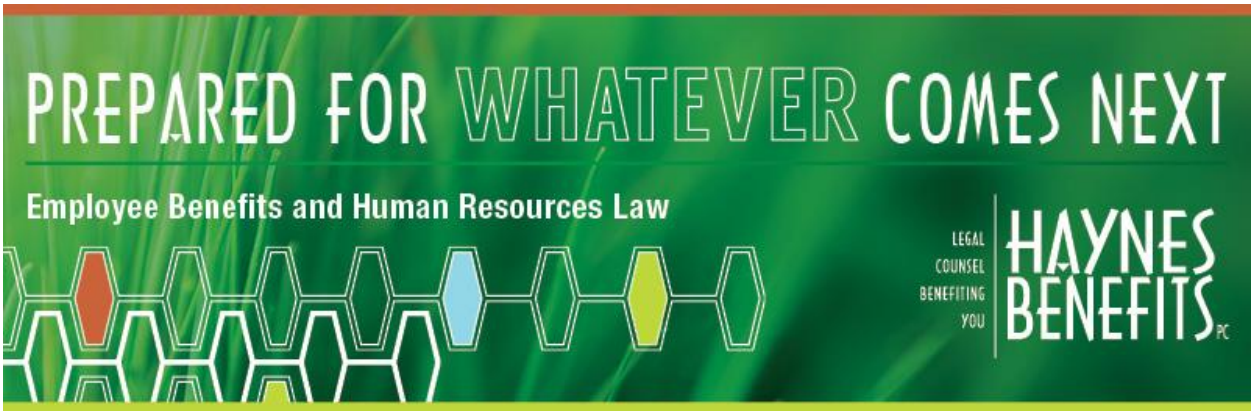


OCR 2019 Cybersecurity Newsletter Urges Covered Entities and Business Associates to Consider Ransomware in Risk Analysis and Risk Management

Ransomware is becoming one of the fastest growing areas of risk in cybersecurity. In response, the U.S. Department of Health and Human Services ("HHS") Office for Civil Rights ("OCR") issued a Fall 2019 OCR Cybersecurity Newsletter which provided an update on preventing, mitigating, and responding to ransomware.

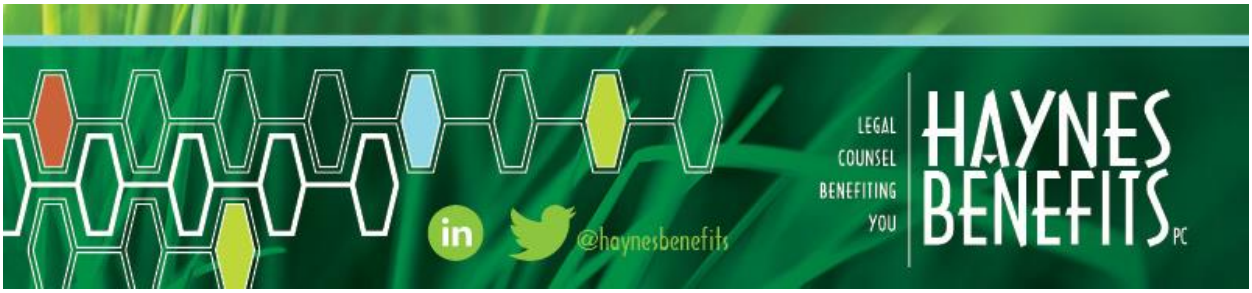
What Is Ransomware? Ransomware is a type of malicious software (or malware) that attempts to deny access to a user's data, usually by encrypting the data with a key known only to the attacker who deployed the ransomware. To obtain this key, a victim typically must make a ransom payment, usually made in cryptocurrency.

> **Impact on Health Plans.** While earlier ransomware attacks were *generalized*, ransomware developers have created *targeted* ransomware attacks adapted to specific organizations with sensitive data, high data availability requirements, low tolerance for system downtime, and the resources to pay a ransom—and *health plans* meet all these indicators.

Ransomware Is Malicious Software

Ransomware attacks pose a serious threat to HIPAA covered entities and business associates. Indeed, OCR provided this dire warning:

> 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).

OCR then discussed how to tackle ransomware through certain HIPAA security standards.

Risk Analysis

Entities must address ransomware in their risk analysis. Entities should focus on identifying and addressing technical vulnerabilities within information systems and information technology infrastructure and is crucial to preventing ransomware attacks.

OCR further noted that ransomware often exploits technical vulnerabilities such as:

- outdated software;
- unsecured ports; and
- poor access management/provisioning.

Effective security tools that may make an organization a less inviting target include:

- anti-malware software; and
- intrusion detection and prevention solutions.

Information System Activity Review

Entities must address information system activity review for the purpose of preventing or overcoming ransomware. OCR stated that, "[i]f 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."

OCR recommends taking special effort to identify anomalous activity—especially activity executed with elevated privileges such as access to ePHI. OCR states these efforts can be crucial to identifying an attack in progress.

Access Controls

Entities must address the technical safeguard of access controls to stop or impede ransomware to sensitive data. Access controls can segment networks to limit unauthorized access and communications. Because attacks frequently seek elevated privileges such as administrator access, entities may consider solutions that limit the scope of administrator access and require stronger authentication mechanisms when granting elevated privileges or access to administrator accounts.

The Two Step Training

No, two step training is not a new dance move. OCR stated that there should be two types of training to make users aware of the potential threats they face and inform them on how to properly respond to them:

- introductory training for new employees or employees with new access to PHI; and

- regular updates with discussion of new or ongoing guidance, and a reminder of basic security principles.

Security Incident Procedures

An organization's incident response procedures can greatly limit the damage caused by a ransomware attack. OCR recommended that organizations consider addressing ransomware attacks specifically within response policies and procedures as mitigation actions may vary between different types of incidents.

OCR also added the following tips:

- 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 detailed and be distributed to necessary workforce members. Organizations should update their security incident procedures from time to time to ensure they remain effective.

OCR stated that familiarity with 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

Robust contingency plans are important in case of a ransomware attack.

The contingency plan standard requires:

- a data backup plan;
- frequent backups; and
- ability to recover the data.

Test restorations should be reviewed periodically, and entities should consider maintaining backups offline and unavailable from their networks.

Additional activities that must be considered as part of a contingency plan include:

- disaster recovery planning;
- emergency operations planning;
- analyzing the criticality of applications and data to ensure all necessary applications and data are accounted for; and
- periodic testing of contingency plans to ensure organizational readiness to execute such plans and provide confidence they will be effective.

Maintenance

Covered entities and business associates should ensure that security measures remain effective as technology changes and new threats and vulnerabilities are discovered. This may include updating or patching software and devices to mitigate known or discovered vulnerabilities.

Conclusion

Ransomware is a serious threat to health plans and business associates. The OCR guidance provides a welcome and updated framework to address these issues in line with the security standards.

The content herein is provided for educational and informational purposes only and does not contain legal advice. Please contact our office if you have any questions about compliance requirements applicable to your employee benefit plans or other HR compliance matters.

Dated: May 1, 2020