OCR Guidance on Defending Against Common Cyber-Attacks

The number of reportable breaches of unsecured electronic protected health information (ePHI) affecting more than 500 individuals increased 45 percent from 2019 to 2020, the U.S Department of Health and Human Services' Office for Civil Rights (OCR) reported in its Quarter 1 2022 Cyber Security Newsletter. OCR found from their investigations that most cyber-attacks were preventable or would have been substantially mitigated if HIPAA Security Rule requirements had been implemented for most common types of attacks (e.g., phishing emails, exploitation of known vulnerabilities, and weak authentication protocols). OCR outlined several preventative steps to protect against some of the more commonly successful cyber-attack techniques.

Phishing is one of the most common types of cyber-attacks. It tricks individuals into divulging sensitive information via electronic communication, such as email, by impersonating a trustworthy source. OCR noted that 42 percent of ransomware attacks involved phishing. The first line of defense is training to ensure everyone in the workplace understands how to recognize a phishing attempt and take appropriate action, such as notifying their IT department. The Security Rule requires security reminders and ongoing training for all workforce members, including members of management. Risks can also be mitigated by implementing anti-phishing technologies, such as being able to examine and identify emails that originate from known malicious sites and blocking them. Other techniques should also be explored.

Exploiting Known Vulnerabilities. Hackers can penetrate a regulated entity's network and gain access to ePHI by exploiting known vulnerabilities. These vulnerabilities can exist in many places (e.g., server, desktop, and mobile device operating systems; application, database, and web software; router, firewall, and other device firmware). Many of these vulnerabilities can be mitigated by applying vendor patches or upgrading to a newer version. If an obsolete, unsupported system cannot be upgraded or replaced, additional safeguards should be implemented until a replacement can occur (e.g., increase access restrictions, remove or restrict network access, disable unnecessary features or services).

Richard P. Kusserow | April 14, 2022

Weak Cybersecurity Practices. Weak passwords and authentication requirements are frequent targets of successful cyber-attacks, accounting for over 80 percent of breaches. Entities should implement appropriate authentication solutions to reduce the risk of unauthorized access to ePHI, especially for those working remotely. Regulated entities should periodically examine the strength and effectiveness of their cybersecurity practices, technical evaluation of safeguards, and increase or add security controls to reduce risk as appropriate.

OCR noted that the HIPAA Security Rule provides "a baseline for protecting ePHI" and cautioned covered entities against underestimating the risks associated with not taking the appropriate protective actions.

For more information on this topic, contact Richard Kusserow at ***rkusserow@strategicm.com****.*