Cybersecurity Awareness Month: Time to Review Your Program

By Rana McSpadden, FACMPE

Cybersecurity Awareness Month: Time to Review Your Program

Rana McSpadden, FACMPE, CHPE, CPC

October is Cybersecurity Awareness Month, making it an ideal time to evaluate your cybersecurity program and educate employees. Cybersecurity is not solely an IT concern; it is a shared responsibility across the entire organization. Leadership must set expectations and prioritize understanding cyber risks and how to mitigate them. With healthcare organizations increasingly targeted by cyberattacks, even a single vulnerability can lead to data breaches, financial loss, and damage to patient trust. Taking proactive steps now can help safeguard your systems and ensure compliance with regulatory

requirements.

Security Risk Analysis

A Security Risk Analysis (SRA) should be the first step in identifying and mitigating cyber risks. As part of performing an SRA, organizations need to identify where electronic PHI (ePHI) is stored, accessed, or transmitted. Once those locations are determined, which is likely to include ePHI beyond the electronic medical record system, threats to that ePHI need to be evaluated. An SRA should encompass the entire enterprise, including satellite locations as well as ePHI stored in the cloud, and be reviewed at least annually. Updates are also necessary when new equipment, software, or significant changes to the organization's IT environment occur. Organizations may choose to outsource this process or conduct it internally. For small to medium-sized practices opting for an internal review, the Department of Health and Human Services (HHS) offers a helpful SRA toolkit. *

Protection from Malicious Software

One of the many threats to its ePHI that an organization must consider is malicious software. One way to mitigate this threat involves using software that scans for malware and viruses, quarantines suspicious files, and prevents their spread. Additional safeguards include web filtering software that restricts access to certain websites or blocks unauthorized software downloads. Keeping operating systems and applications updated with the latest security patches is essential. Collaborate with an IT professional to determine the most appropriate solutions for your organization.

Password Management

Weak password practices continue to pose a significant threat to network security. Each staff member should have a unique username and password and avoid sharing credentials. Implement policies requiring passwords or pass-phrases between 12 and 16 characters, incorporating uppercase and lowercase letters, numbers, and special characters. Consider using a password safe that securely stores credentials and offers features such as detecting compromised, weak, or reused passwords. While password safes can provide an effective way to manage complex passwords, steps need to be taken to protect the password safes themselves from unauthorized access. Speak with your IT professional to determine if and what password safe works best for your organization.

Reevaluate your password expiration policy as well. The National Institute of Standards and Technology (NIST) advises against routine password changes, as frequent changes often lead to predictable patterns. For example, users may only alter one character, such as changing a "1" to a "2." Frequent changes can also cause frustration, leading staff to write down passwords and store them insecurely. NIST recommends password changes only when a breach is suspected. If your policy still requires regular expiration, consider extending the time between changes to reduce these risks.

Multi-Factor Authentication

Strong passwords alone are not enough. Multi-factor authentication (MFA) adds another layer of protection. MFA methods include biometrics (fingerprints or facial recognition), authenticator apps, or text messages. Consult with your IT professional to determine the best MFA options for your organization.

Log-In Monitoring

Intrusion detection and monitoring for unauthorized access are important components of a cybersecurity program to monitor systems for compromised credentials. These capabilities are particularly significant if the organization is not routinely resetting passwords. Otherwise, an attacker who has gained access through a compromised password may have unauthorized access for an extended period of time.

To mitigate this risk, organizations should regularly review access logs and consider implementing real-time alerts for unusual login behavior, such as access from unfamiliar locations, devices, or outside of normal working hours. By combining strong monitoring with user education and access controls, organizations can significantly reduce the likelihood and impact of credential-based attacks.

Email Security

Email is a common entry point for cyber threats. Use email scrubbing software to detect and block spam, phishing attempts, malware, and other threats. Establish a policy prohibiting staff from accessing personal email accounts while connected to the organization’s network, as these accounts are not protected by your email security systems.

Even the most advanced email protection software does not stop all email-borne threats. Every workforce member in the organization must be on guard for suspicious emails. Provide a simple mechanism for reporting suspicious emails. This could be a policy requiring staff to forward questionable messages to a designated reviewer or an email add-in that automates the process. Making reporting easy encourages staff participation and enhances security.

Encryption

Encryption is a critical safeguard under the HIPAA Security Rule and should be addressed in your SRA. Consider encryption of mobile devices, emails containing sensitive information, and data both in transit and at rest. Encryption helps prevent unauthorized access when devices are lost or stolen. Encrypting data while at rest may help protect it from unauthorized access, even if someone gains access to your network. Discuss encryption solutions with your IT professional to determine what level of encryption is best for your organization.

Data Backup

Data loss can be devastating. Ensure critical systems such as your EHR, PACS, lab systems, and financial records are backed up regularly. Even cloud-based EHR systems may not cover all essential data. Use a combination of onsite, offsite, and cloud backups to ensure redundancy and reliability. It's a common misunderstanding that the HIPAA Security Rule only pertains to protecting the confidentiality of ePHI. The rule also requires that organizations protect the availability of ePHI, which includes, among other things, maintaining a backup copy of ePHI.

Vulnerability Scans and Penetration Testing

These tools and techniques help identify weaknesses in your network. Vulnerability scans use software to detect internal flaws, while penetration testing involves ethical hackers simulating real-world attacks. Discuss these options with your IT team to determine if either or both are appropriate for your organization.

Staff Education

Even the most advanced cybersecurity program can fail without informed staff. Employees are the first line of defense against phishing, ransomware, and social engineering. Provide education on these topics at least annually, though ongoing training is ideal. Use webinars, classroom sessions, memos, simulated phishing tests, or staff meetings. Document all training and retain records for at least six years.

In Conclusion

Cybersecurity is a collective responsibility that begins with leadership. A strong strategy combines administrative, physical, and technical safeguards to protect sensitive data and prevent unauthorized access. To be effective, this strategy must be actively maintained, regularly reviewed, and supported by ongoing staff education and collaboration with IT professionals. Cybersecurity requires continuous vigilance and commitment across the organization.

***https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool**

***Due to the current government shutdown, this website may be unavailable.**

If you have questions about HIPAA, cybersecurity, or access to SVMIC resources, call 800-342-2239 or email Contact@svmic.com.

If you experience a cybersecurity or other HIPAA related incident, contact SVMIC as soon as possible by calling 800-342-2239 and ask to speak with the Claims department.

Other individuals in your organization may benefit from these articles and resources, such as your administrator, privacy or security officer, or information technology professional. They can sign up for a Vantage account.

The contents of The Sentinel are intended for educational/informational purposes only and do not constitute legal advice. Policyholders are urged to consult with their personal attorney for legal advice, as specific legal requirements may vary from state to state and/or change over time.