How to Implement Cybersecurity Workforce Training

Cybersecurity Workforce Training for Large Healthcare Organizations

HHS 405(d)
Aligning Health Care
Industry Security Approaches

What is cybersecurity workforce training?
Cyber workforce training is an effort to train your staff on the most common and pertinent cyber threats today. Everyone in a healthcare office or organization should receive cybersecurity training to protect patients from cyber threats.

Why is it important?
Cyber threats are constantly changing, and the threat to healthcare offices and organizations are real. The most common way for bad actors to infiltrate an organization is through the workforce with tactics such as email phishing. To keep your organization and your patients' data safe you must continuously train your staff on recent cyber tactics.

How will this keep my organization safe?
Cyber-attacks not only harm patients, but they also cause considerable reputational and financial harm to an organization. All staff of an organization, regardless of size, are the first line of defense when it comes to cyber-attacks. If you prepare your work force to recognize and identify potential cyber threats, your patients and your organization will be more secure.

Threats Training Mitigates:

- Email Phishing
- Ransomware
- Loss or Theft of Equipment
- Insider, Accidental, or Intentional Data Loss

Implementation Tips:

Create monthly phishing campaigns. The most effective means of training your workforce to detect a phishing attack is to conduct simulated phishing campaigns. Your authorized security personnel or third-party provider crafts and sends phishing emails to your employees and identifies employees who open the email or click on the emailed links. Then, the organization can provide the appropriate training and feedback as soon as possible after the event.

Create organization newsletters. Working independently or with your marketing department, develop and distribute your own cybersecurity newsletter. Write articles that explain how to catch a phishing attack. Provide examples of actual phishing attacks, highlighting the warning signs that might have prevented the attack. Consider adding a reminder of how many days your organization has gone without a cybersecurity breach to motivate the workforce.

Conduct routine departmental meetings. Hold departmental meetings to discuss information security and cybersecurity events and trends. Brief presentations or informal conversations provide face-to-face context and build relationships between security personnel and the organization's workforce.

Conduct email campaigns. Deliver a pointed email message or alert about specific attacks. Provide Secure Multipurpose Internet Mail Extensions (S/MIME) or other digital certificates as evidence that these messages are authentic. Remember that attackers will attempt to do the same thing!

To learn more about how you can protect your patients from cyber threats check out the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication. Check out the available resources 405(d) has to offer by visiting our website at 405d.hhs.gov and our social media pages: **@ask405d** *on Facebook, Twitter, LinkedIn and Instagram!*