How to Implement Cybersecurity Workforce Training

Cybersecurity Workforce Training for Small 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:

Train staff to recognize email phishing techniques. They should be looking for suspicious email addresses with urgent prompts and "too good to be true" messages. Anti-phishing campaigns with real-time training should become part of your internal security processes for your staff. Direct your appointed IT personnel or Admin specialist to send a phishing email to everyone on your staff. Track how many of your employee's "bite" or open the email. This enables you to target training to those who demonstrate need. If you do not have an internal phishing process many third parties provide low-cost, cloud-based phishing simulation tools to train and test your workforce.

Keep training constant to deal with the short shelf life of learning and development needs. Provide effective and relevant training for your employees that offer continuous and ongoing campaigns to maintain awareness of current trends, issues, and events. The healthcare industry is always under attack from hackers that try to steal valuable Personally Identifiable Information (PII) and Protected Health Information (PHI). To arm your employees with actionable steps that will apply to the current threats, training must be relatable to threats that affect their work environment every day.

Educate your employees on the risks of insider threats. Train and test your staff to make sure they understand the security risks and the consequences of falling victim to an insider attack. The goal is to train your workforce to be "human sensors" detecting malicious activity and reporting these incidents to your cybersecurity department.

Train your employees on password protection procedures. Regularly remind users that they must never share their passwords. Require each user to create an account password that is different from the ones used for personal internet or email access (e.g., Gmail, Instagram, Facebook). Remind them never to write their password down on paper where others in the office may have access to it.

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!*