Staying Cyber Safe in the Healthcare and Public Health Sector

Tips for individuals and organizations

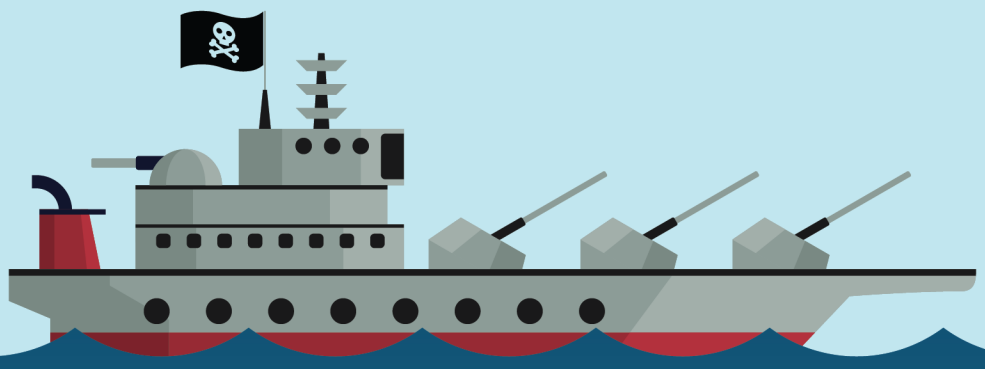
HHS 405(d)
Aligning Health Care Industry Security Approaches

Cybersecurity defense can be viewed as a large iceberg. The ice above the water is your first line of defense and what attackers see most: employees and physical equipment. Underneath the ice is everything an organization should be doing behind the scenes to ensure an attack on the top of the ice can be defeated.

First Line of Defense

Every organization's first line of defense against cyberattacks is the training of employees and protection of IT equipment. Here are some examples of what you need to secure your first line of defense:

- **Role-based Cybersecurity Training:** Provide robust, customized security training for all employees based on their job function to ensure continuity of security expectations.
- **Phishing Simulation Training:** Prepare employees to identify and proactively respond to phishing attacks in the workplace environment.
- **Asset Management Programs:** Ensure that all data, devices, and systems are categorized and inventoried according to their importance to the organization's objectives.
- **Cybersecurity Policies:** Create and communicate your organization's security policies to all employees to level set expectations for protecting patient data.
- **Insider Threat Training:** Incorporate insider threat training into your on-boarding policies for new employees.
- **Physical Security:** Put physical controls into the office environment to prevent access to or the use of company computers by unauthorized individuals.



Behind the scenes defenses are equally important to prevent cyberattacks from occurring or spreading through your organization. Every size organization should instill a few of the following practices to protect your organization:

- **Email System Configurations:** Enact controls to enhance the security posture of your e-mail system, such as configuring your email system to tag messages as "EXTERNAL" that are sent from outside of your organization.
- **Multi-Factor Authentication:** Use at least two of the following to verify a user's identity: something you know, something you have, and something you are.
- **Data Protection Policies:** Establish a data classification policy that categorizes data as, for example, Sensitive, Internal Use, or Public Use.
- **Network segmentation:** Partition networks into security zones which can be based on sensitivity of assets within the network or standard perimeter segmentations.
- **Intrusion Prevention:** Utilize an intrusion prevention system for reading network traffic to detect and prevent potential attacks against your network perimeter, data center, and partner connections.
- **Vulnerability Management:** Proactively discover vulnerabilities that will enable the organization to classify, evaluate, prioritize, remediate, and mitigate the technical vulnerability footprint from the perspective of an attacker.
- **Incident Response Plans:** Maintain cyber threat detection and response capabilities by establishing an Incident Response program and a Security Operations Center to manage the plan.

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 or our social media pages: **@ask405d** *on Facebook, Twitter, LinkedIn and Instagram!*