Quick Safety
Issue 62 | October 2021

Organization-wide cybersecurity: Creating a culture of defense

Issue:

Today's always-online health care environment requires an all-hands approach to cybersecurity: a data safety culture which permeates the entire organization and its operations. Cybersecurity can no longer be viewed as only the province of the IT department but must be the responsibility of all staff who have access to digital information, electronic health records, and Internet and network resources. Just one person can jeopardize an entire organization's security efforts if they fall prey to common phishing strategies. Prevention requires a top-down organizational approach that employs all staff in continual awareness and preparedness, a concept sometimes called the "human firewall."[1]

Instituting a cybersecurity program can be particularly challenging for health care settings. The digital transition in health care means more information from across the organization is stored online. The operational needs of a facility, as well as interoperability regulations, often prioritize speed and accessibility of information over information security. Additionally, many facilities use a common network that integrates multiple aspects of clinical systems, medical systems, business systems, physical security, and building management. Telehealth, remote patient monitoring, and patient-focused digital tools, such as mobile health tracking apps and patient portals, extend a health system's digital landscape far beyond a physical campus.[2]

At the same time, health care data is ten times more valuable to hackers than credit card information.[3] Knowing that a significant interruption to health care services can be life or death for patients, ransomware attackers view health care organizations as very desirable targets.[4] To secure health care data and protect medical devices, health care organizations must guard against a wide variety of attacks and teach staff to expect the unpredictable as hackers continuously adapt their strategies.[5] Appreciating the creativity of ransomware attackers, organizations should elevate to a high priority plans for business continuity – including attention to how frequently and where data is backed-up in order to resume normal functioning as quickly as possible.

Safety actions to consider:

Building a culture of cybersecurity, or the human firewall, requires an awareness of cybersecurity threats, including an evaluation of the types of threats that exist, and the incorporation of preventive strategies at all levels of the organization. The following actions can be taken to help organizations prepare for and repel a cybersecurity event.

Leadership's role in a culture of cybersecurity

- Most importantly, create a culture of cybersecurity that is top down.
- Make sensitivity to cybersecurity threats and organizational preparedness part of the way the organization performs its work.
- Recognize that the scope of cybersecurity threats is always evolving and is organization wide.
- Build a human firewall by requiring an awareness of cybersecurity vulnerabilities at all levels of the organization.
- Recognize the importance and necessity of cybersecurity as an integrated part of patient care.
- Designate a Chief Information Security Officer, responsible for coordinating efforts to promote cyber-awareness.
- Develop a robust business continuity plan that can be quickly enacted, that safeguards the most amount of data and information, and can bring the organization back to working order in a timely fashion.

Staff education and training

- Establish training programs for all staff and not just for clinicians. Include frequent refresher courses.
- Periodically evaluate staff to ascertain whether they appropriately respond to "test" cyber challenges.
- Train staff to anticipate non-conventional intrusions.
- Appropriately tailor training for different positions within the organization and take into consideration the technology used in specific staff roles.

Emergency management

- Cybersecurity preparedness takes the perspective of "when" not "if" an incident will occur.
- Incorporate responses to cybersecurity attacks as part of the organizational emergency preparedness plans.
- In the response to intrusions, include the necessary reporting and disclosures of any data breach.

IT security team resources

- Utilize available free resources from reputable sources such as Cyber Insurance Carriers, Cybersecurity & Infrastructure Security Agency (CISA), Healthcare and Public Health (HPH) Sector Coordinating Council, Internet Crime Complaint Center (IC3), and National Institute of Standards and Technology (NIST) (see links below).
- Invest in security tools and resources when needed.

In response to rising rates of cyberattacks, several government security agencies have put out general guidance on how to improve cybersecurity within your organization, as well as considerations specific to the health care industry. Some of these are listed in the Resources section below. These resources provide an initial checklist to measure cybersecurity preparedness within health care organizations.

Resources:

1. Stephen Burke. Creating a Human Firewall. *Infosecurity Magazine*. November 2017.
2. CISA: Cybersecurity Challenges to Healthcare Sector. December 2020.
3. Mackenzie Garrity. Patient Medical Records Sell for $1K on Dark Web. *Becker's Hospital Review*. Feb. 20, 2019.
4. The White House. Letter to Corporate Executives and Business Leaders: What We Urge You to Do to Protect Against the Threat of Ransomware. June 2021.
5. Healthcare & Public Health Sector Coordinating Councils. Health Industry Cybersecurity—Securing Telehealth and Telemedicine. April 2021.

Other resources:

American Medical Association: Protect Your Practice and Patients from Cybersecurity Threats. 2017.

Assistant Secretary for Preparedness and Response (ASPR) Technical Resources, Assistance Center, and Information Exchange (TRACIE): Healthcare System Cybersecurity: Readiness & Response Considerations. February 2021.

Cybersecurity & Infrastructure Security Agency (CISA):

- Cybersecurity Perspectives: Healthcare and Public Health Response to COVID-19. January 2021.
- COVID-19 Checklist: Securing Your Business and Clinical IT. April 2021.
- Cyber Hygiene Services. 2021
- StopRansomware.gov. 2021

National Institute of Standards and Technology (NIST):

- NIST Releases Tips and Tactics for Dealing With Ransomware. May 2021.
- Cybersecurity Framework Profile for Ransomware Risk Management (Preliminary Draft) June 2021.

Healthcare and Public Health (HPH) Sector Coordinating Council:

- Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients. January 2019.
- healthsectorcouncil.org. May 2021

IC3:

- FBI Internet Crime Complaint Center (IC3) Ransomware Resource Page. February 2021.

Note: This is not an all-inclusive list.