Healthcare System Cybersecurity Readiness & Response Considerations Appendix

This appendix provides additional information regarding IT practices, resources, and guidance provided by ASPR TRACIE partners and cybersecurity experts outside of healthcare facility operational considerations. Return to the Healthcare System Cybersecurity Readiness & Response Considerations.

Additional Security Considerations

- When thinking through healthcare cybersecurity protections, explore specific topics that include:
    - Defense in depth strategies.
    - Principle of least privilege.
    - Creation of sandboxes.
    - External security of inbound vendors and/or servers.
    - Vulnerabilities presented by aging equipment that can be compromised with inbound hacking if tethered to an external server for upload or download of information (where patches are unavailable for antiquated equipment or are too expensive for the remaining life of the device).
    - Systems within a hospital that are being monitored from external vendors, where the whole componentry could be a vulnerability.
- Follow the “3-2-1” rule to maintain security of backups: at least 3 copies on 2 devices with one offsite; ensure offline networks are segmented.
- Utilize Multifactor Authentication (MFA) throughout an organization for access protections.
- When assessments are completed to identify vulnerabilities, ***rank the identified risk vulnerabilities*** based upon impact to patient care and safety, protection and privacy of patient data, and then non-clinical business operations. Ensure ***scans and penetration tests*** include operational and physical security technology.
- Experts state that it is important to understand that in some cases, vulnerability scanning is limited, and penetration testing is appropriate in many cases. Additionally, vulnerability scans of medical equipment in clinical use may lead to adverse patient outcomes by causing the device to reboot or otherwise not behave as expected. Vulnerability scans should be coordinated with medical equipment servicing groups to occur regularly when the device is available due to periodic/planned maintenance.
- In reference to ***Zero Trust network architectures***, NIST notes that there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (i.e., enterprise or personally owned).
- Facilities should consider use of strong encryption at the enterprise level to further protect critical data.

- For more information on ***contingency planning*** as it relates to cybersecurity, the NIST Contingency Planning for Federal Information Systems document provides specific information on the purpose, process, and format for formal contingency planning within the IT sector.
- Carnegie Mellon University provides additional information on the risks associated with moving to the Cloud, or cloud-based solutions, in their resource ***12 Risks, Threats, and Vulnerabilities in Moving to the Cloud***
- Streamlining data flow from interconnected systems will create more predictable traffic flows for monitoring and comparison.
- Monitor network traffic to limit to necessary ports and protocols, and restrict communications to external end points, especially ones with historical high risk geographically.
- The Communications Security, Reliability, and Interoperability Council IV Working Group final report provides information on cybersecurity practices for protecting and insulating a system. Such practices can contain spread within a segment or enclave.
- When segregating life safety equipment, eliminate trust relationships between life-safety and corporate networks, especially for authentication.
- Facilities should have a complete ***Configuration Management System*** and ***Configuration Management Database*** (CMS/CMDB) of all networked devices, software entities, and their Network Interface Card (NIC) characteristics such as media access control (MAC) address, as well as the major software components on said device.
- Additional information on vulnerabilities and protection of software-based medical technologies and their impact to patient care can be found in the HSCC Medical Device and Health IT Joint Security Plan.
- Experts suggest working with the National Telecommunications and Information Administration (NTIA) and understand the ***Software Bill of Materials*** (SBoMs) to leverage these information sources to map ***Common Vulnerabilities and Exposures*** (CVEs) to medical equipment in order to understand current and future risk vectors.
- Many networked devices can function in a non-networked mode; however, they require the care provider to be local to the unit (e.g., Radiologist at the MRI). Consider what plans are in place for additional staffing to provide for local interaction with normally networked devices.
- In cases where custom developed applications are critical to a facility, experts suggest it is imperative to have a proper secure ***System Development Life Cycle*** (SDLC) for the development of safe applications.
- Consider vendor Virtual Private Network (VPN) access as a possible attack vector and align controls with best practices. There should be risk evaluations associated to this attack vector as well as monitoring of the VPN connections.

Communications

- The CISA ***Priority Telecommunications Services*** (PTS) provide organizations that meet critical infrastructure criteria with emergency contingency communications capabilities through three services. ***Government Emergency Telecommunications Services*** (GETS) provides a landline network contingency, the ***Wireless Priority Service*** (WPS) provides a wireless network contingency, and the third service, ***Telecommunications Service Priority*** (TSP), provides priority restoration for critical communication circuits and hubs, as well as relocation support when communications circuits require routing to new service or business locations.

- A facility should ideally be informing their local partners first through the healthcare coalition (HCC) as well as the state. Healthcare facilities should understand in depth the communication protocol between the organization and the HCC.
- A facility should consider having or educating a ***Public Information Officer*** on communicating with external partners about Cyber events.
- More information on out of band communication mechanisms that are considered for entities currently using IP networks for voice communications is available via the MITRE partnership network.

Partners and Information Sharing

- The Healthcare Sector Coordinating Council FAQ resource provides information about the goals of the council, which include "identifying major cybersecurity threats and vulnerabilities to the security and resiliency of the healthcare sector, and developing cross-sector policy and strategic approaches to mitigating those risks" and how to become a part of the ***Cybersecurity Working Group***.
- For additional information on becoming part of the IT-ISAC, visit https://www.it-isac.org/.
- For additional information on becoming part of the ISAO see the FAQ page or contact the DHS ISAO inbox at ISAO@hq.dhs.gov.
- For exercises and drills, include documentation for existing architecture including security protection and monitoring solutions, which will greatly assist in just-in-time training and response.

Policies

- To better understand cybersecurity risk as an ***enterprise risk management*** issue, reference information available in the NISTIR 8286A - Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management (ERM).
- Review the passage of HR 7898, the ***HIPAA Safe Harbor Bill***, an amendment to the HITECH act where HHS is directed to provide regulatory relief and considerations for HIPAA covered entities which have met recognized cybersecurity practices, such as NIST and 405d.
- Information on the ***Health Industry Cybersecurity Practices*** (HICP) can be used to understand how HICP analyzes cybersecurity threats and vulnerabilities that could affect the health sector. Specifically, the HICP covers five threats and provides ten mitigation practices for industry.
- The HHS Incident Reporting, Policy and Incident Management Reference lists policies, guidance, additional incident management resources for reporting a cyber event.
- The CMS Information Security and Privacy Overview provides specific guidance for reporting an incident involving ***CMS information or information systems***.

Response and Recovery

- In cases where a healthcare facility may stand-up an Operations/Command Center in response to a cyber incident, they should closely review the FEMA Incident Command System Resource Center and National Incident Management System (NIMS) resources.
- Understand the role of cyber incident forensics firms, explore what companies in the area may offer necessary services and/or discuss options with the facility cyber insurance provider.
- Emphasis should be placed on testing backup RTO and RPO objectives. Understand that it is difficult to test full system restores from backups because of disruption to patient services. Experts suggest maintaining separate and secure copies of interfaces and application images.
- In terms of response, it is important to differentiate between eradication of the threat actor and restoration of services as both are critical steps. A significant number of intrusions restore services without effectively removing the threat, resulting in either an on-going cycle of compromise, or having a dormant threat remaining on the network.

Training and Personnel

- New cybersecurity threats are constantly appearing. The personnel entrusted with detecting cybersecurity threats need continual training. Training increases the likelihood of detecting threats and responding to threats in a manner consistent with industry best practices.
- Cybersecurity tools are only as good as the people reviewing the tools' results. It is important to ensure staff are able to identify the proper tools for an organization, recognizing it can take a significant amount of time to learn a complex organization's enterprise network. This makes retaining skilled personnel as important as acquiring them. While there is no perfect answer to stopping cybersecurity threats, ensuring knowledgeable IT personnel are on the team is critical to reducing cybersecurity risks.

Terminology

- ***Golden Images*** are a type of secure baseline disk image that is used as a template for systems to ensure consistency and ease of deployment with a high quality/high standard copy or backup. ***External Mirroring*** is the practice of data separation/redundancy. The practice entails having a "mirror" of critical data outside of the organization (offsite).
- In cybersecurity, ***threats*** differ from ***vulnerabilities***. Threats are intentional actions by a malicious actor. Vulnerabilities are weaknesses caused by a victim knowingly or unknowingly.
- ***Downtime*** is a term used by the IT industry to identify the time when a computer system, server, or network is unavailable or offline. For the healthcare industry this term means the time when a necessary piece of technology required for healthcare operations is unavailable resulting in the need for alternative workarounds to be established. Many times, this can mean moving to manual processes such as paper charts and dictation of medical procedures and treatment.
- ***Risk-based decision making*** in cybersecurity is an important component of understanding a facility's vulnerabilities and deciding on best strategies for protection or mitigation. The CISA Risk-based approach to National Cybersecurity resource can provide guidance to properly assessing and reducing risk.