The Top 9 Criteria Organizations Should Consider When Evaluating Medical Device Security

Written by Cory Blacketer; Medical Device Security Consultant at CynergisTek

Network-connected medical devices are transforming how healthcare organizations are able to deliver patient care. The benefits presented by network connected medical devices are great, however, so too are the potential security risks. Every year an increasing number of medical devices are designed to function on an organization's network but are not often manufactured with security in mind, leaving these assets an easy target for attack. As members of the healthcare industry and regulators, such as the FDA, continue to put pressure on medical equipment manufacturers to incorporate more robust security features into the design of their devices, healthcare delivery organizations must turn their focus to the medical devices already deployed within their environment of care and addressing inherent vulnerabilities associated with the outdated, unsecure software run by most clinical equipment.

Near the end of 2018, CHIME released a benchmarking report, "Medical Device Security 2018",[1] with nearly all respondents citing patient safety as their top concern with unsecured medical devices. However, organizations that responded with confidence about their medical device security program cited solid security policies and procedures as the leading reason for the confidence, followed by strong technology.

The following are criteria every healthcare delivery organization should consider when evaluating their medical device security program for both effectiveness in mitigating risks to connected medical devices as well as capability for supporting strong technology moving forward:

---

1 Support Structure

Medical devices are managed within a healthcare organization in a number of different ways. Originally, these devices were designed as appliances that simply required basic upkeep and preventative maintenance procedures. The support structure for these processes vary across organizations and are managed either by an in-house clinical engineering team, outsourced third-party contractors, consultants, or the medical device vendors themselves. In some instances, the support structure is a mixture of all of the above. This may create inconsistencies or gaps in policies and procedures as well as a general difficulty in managing the governance of ongoing maintenance processes. Explicitly understanding the roles and responsibilities for each level of support for medical devices will help an organization operate more efficiently in an incident response scenario as well as in providing overall oversight and assurance for consistent and compliant medical device security practices.

2 Acquisition/Procurement Process

Most organizations have a well-defined procurement process for clinical equipment and applications. However, medical devices tend to sneak through non-traditional purchase methods, especially those procured at the request of a physician. Organizations should consider all of the methods in place currently for acquiring new medical equipment and determine whether an opportunity exists for standardizing this process across the organization.

a. Also, as part of the strategic procurement process for the organization as a whole, risk assessments should be performed on medical devices prior to making purchase decisions. Capital equipment planning should include the review, evaluation, and documentation of all applicable medical device risks and the consideration of additional device security support agreements as required. All of the information received during this process will help to inform each stage of managing the medical equipment consistent with organizational security standards after purchase and deployment.

[1] https://chimecentral.org/chime-klas-survey-measures-providers-confidence-in-medical-device-security-programs/

3 Inventory Management

Understanding the connected device environment and network infrastructure within the clinical setting is a critical first step in planning for or implementing security measures for medical devices. Missing this information can potentially cause a precarious delay for vulnerability and risk mitigation as well as ineffective incident response management processes. Many healthcare organizations lack accurate insight into their network connected medical device inventory and traditional IT-focused network discovery solutions pose risks to medical devices.

a. Traditionally, clinical engineers had no need to include inventory fields within medical device inventory management systems for network attributes or information security controls. However, with the introduction of increased network connectivity requirements, fields should be included within each device record to document device-specific security controls, network information, and whether or not the device maintains ePHI.

b. Consider how the location of medical devices are recorded within the inventory system and how this information stays up to date when devices move within the hospital. This includes processes for documenting and communicating missing or "cannot locate" devices.

4 Third Party/Vendor Management

An increasing number of vendor technologies are being acquired by healthcare organizations with little guidance on how to effectively manage security for those vendors. Vendors that provide support for medical devices will generally use a remote connection rather than physically touching the medical devices they support. In this case, VPN connections can open up additional risks for an organization.

a. Organizations should have a plan to manage vendor technology by using robust contract language and Business Associate's Agreements (BAA), implementing security and risk assessment processes into the initial contracting stage, providing governance and oversight throughout continuous maintenance processes, and continually auditing or assessing vendor compliance with organizational security standards.

5 Risk Assessment Processes

The primary concern for successful medical device risk management is the ability of an organization to continuously assess and evaluate how connected medical devices currently impact the environment of care, how that impact could be affected by a security threat or vulnerability, and any security controls currently in place or applicable for risk mitigation purposes.

a. An organization must be careful to consider the balance between implementing security controls as the result of a risk assessment and any potential impact to the operational aspects (i.e. the availability, usability, or functionality) of the medical devices assessed. However, this information should be included in risk assessment documentation and reviewed and approved by hospital leadership.

6 Secure Network Management

The emergence of new threats and vulnerabilities as well as the development of new technologies require an organization to adopt flexible and scalable defenses as well as solutions that can be tailored to meet these rapidly changing conditions. Many times, due to the lack of security controls incorporated into the design and functionality of medical devices, managing security risks at the network level is the best option. An organization should consider the current network structure and how network segmentation, firewalls, access controls, and network monitoring solutions can be used to manage compensating controls for medical device risk mitigation.

7 Security Incident Response

Medical device cybersecurity alerts reached an all-time high in 2018, with even more projected for 2019. Every healthcare organization should develop and maintain an incident response plan for investigating and responding to medical device-specific security incidents. Organizations should continuously test this plan by running table-top and hands-on exercises with scenarios that include unavailable network connected medical devices or systems and consider how this might impact patient care and other operations within the organization.

8 Vulnerability Identification and Remediation

Information security teams are at a disadvantage as an organization's typical vulnerability scanning process cannot be performed for medical devices the way it is done for traditional IT systems. A medical device may not require access to the organization's network except when it is being utilized for direct patient care and active vulnerability scans present the risk of causing a device to malfunction and cause patient harm.

a. A network discovery solution that utilizes passive scanning capabilities to discover connected medical devices available on the network will not present this same risk. The information collected from medical devices connected to the network can be used to continuously identify threat and vulnerability data, including recommendations for mechanisms to remediate vulnerabilities and threats.

b. Once a vulnerability has been discovered, who is responsible for implementing the remediation activities associated with vulnerabilities identified? Between the medical device vendor, clinical engineering, and IT there remains to be a challenge with collaboration between groups regarding steps to take for vulnerability remediation. If a security update or patch is available to address a vulnerability, the organization must determine whether vendor assistance is required and what the clinical workflow impact may be if equipment downtime is required.

9 End-of-Life Management

Any sensitive data, including user and network credentials, should be sanitized from medical devices prior to retirement or disposal of the equipment as well as removal from the facility. Similarly, when approaching capital equipment replacement planning, active technical security vulnerabilities and a lack of remediation capabilities should be considered when prioritizing devices for replacement.

About The Author

Cory Blacketer is an Information Security Consultant for CynergisTek, Inc., who assists clients in performing assessments specific to the biomedical device environment in order to help create a better understanding of medical device vulnerabilities and develop strategies for risk remediation, as well as integrating the implementation of security controls into the overall lifecycle approach for medical device management. She also assists clients in developing, improving, and managing an effective organizational medical device security and risk management program capable of meeting compliance standards and managing the demands of clinical operations.

While entering the healthcare industry working in the clinical engineering field, Cory transitioned into an information security operations role with Ascension Health prior to CynergisTek. The unique experience of operating in both a clinical engineering and information security setting has allowed Cory to better understand the distinct qualities between the two functions in a clinical setting and how to efficiently develop a medical device security program incorporating both functions in a collaborative and effective manner.

Cory has extensive practical knowledge of healthcare information security and compliance standards including HIPAA/HITECH, NIST, and ISO and her certifications include CISSP, HCISPP, and CAHIMS.

About CynergisTek

CynergisTek is a top-ranked cybersecurity firm dedicated to serving the information assurance needs of the healthcare industry. CynergisTek offers specialized services and solutions to help organizations achieve privacy, security, compliance, and document output goals. Since 2004, the company has served as a partner to hundreds of healthcare organizations and is dedicated to supporting and educating the industry by contributing to relevant industry associations. The company has been recognized by KLAS in the 2016 and 2018 Cybersecurity reports as a top performing firm in healthcare cybersecurity as well as the 2017 Best in KLAS winner for Cybersecurity Advisory Services.

512.402.8550

info@cynergistek.com

cynergistek.com

@CynergisTek