Following an uptick in media interest and public scrutiny, cybersecurity recently has become a hot topic in the healthcare industry. Medical device cybersecurity threats have the potential to jeopardize the integrity of hospital information technology (IT) networks and the operation of medical equipment. Although no patient injuries or deaths related to cybersecurity incidents have been reported to the U.S. Food and Drug Administration (FDA), as other industries have experienced, this can change with a single event. Thus, it is very important for healthcare facilities to actively mitigate the cybersecurity risks of their medical devices and IT infrastructure.

In this article, we will explore the importance of medical device cybersecurity and the consequences of security breaches. We also will introduce a few key steps that a healthcare facility should consider when developing a cybersecurity risk management plan. Finally, we will explore the cybersecurity effort of the Methodist Hospital of Southern California, winner of the ECRI Institute 2013 Health Devices Achievement Award, by examining the strategic elements of its medical equipment management plan.

Introduction to Medical Device Cybersecurity

To understand medical device cybersecurity, we first must recognize that the technological landscape of medical devices is changing rapidly. The advancement of technology in the design of medical devices has led to more devices with patient information management and network integration capabilities. A good example would be physiologic monitoring systems. Up until a decade ago, patient monitors were only used to collect and display patient data on a screen. Patient personal information and clinical data often were recorded manually on paper charts. Initial integration capabilities were limited to connections to a nearby nursing station. Today’s monitoring systems, however, in addition to providing the essential monitoring functions, also may be asked to transfer patient data to electronic medical records or even relay alarm information to personal mobile devices (e.g., pager, cell phone). As modern healthcare organizations look for new ways to deliver patient care efficiently and effectively, medical devices are becoming increasingly interconnected.

However, the interoperability and interconnectivity of medical devices create cybersecurity issues that were previously unknown in the healthcare industry. In the past, medical devices often were stand-alone devices that were not connected to the hospital network. Although they still were susceptible to infections through nonnetwork factors, the cybersecurity risks of these devices likely were less compared with those of today’s networked devices. As more medical devices become connected to the hospital’s network, they are exposed to prob-
lems that previously were unseen with older devices. Devices that rely on off-the-shelf software, particularly commercial operating systems (e.g., versions of Microsoft Windows), also are vulnerable to a large variety of threats, such as malware and viruses. With the increased emphasis of interconnectivity of medical devices, more ways exist for these devices to be exploited and attacked.

Threats can infiltrate and infect medical devices through many different avenues; however, in our experience, there are two primary ways in which cybersecurity threats can harm a healthcare facility: by disrupting 1) the operation of medical devices and 2) the integrity of information. Researchers have demonstrated that the operation of certain medical devices can be disrupted to the point that they no longer provide proper patient care.

As some medical devices may be life-critical systems, cybersecurity threats that may disrupt device operation can jeopardize patient safety considerably. Medical devices and IT systems also may contain protected health information (PHI). PHI can include personal information, medical records, and payment information. Because of the sensitivity of PHI, hospitals are attractive targets for spyware and phishing attacks aimed at acquiring the information.

Healthcare facilities need to understand the importance of mitigating the risks described above. Incidents have occurred in which facilities were temporarily shut down due to cybersecurity-related device malfunction. Use of PHI also is governed by the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act, and massive fines have been levied on healthcare facilities that failed to comply with the security and privacy requirements of the HITECH Act. Cybersecurity therefore should be treated as a top priority, as it is a worthwhile investment that will ensure the continuing operation of medical devices and facilities.

**Key Elements of a Management Plan**

Organizations should consider a few key steps when they begin devising a plan for cybersecurity risk management. The first step should be to identify the key stakeholders in a facility and clearly define the distribution of cybersecurity duties among personnel. A hospital biomedical engineering department typically deals with device-specific issues, while the IT department is in charge of the hospital network infrastructure. The emergence of medical devices with advanced integration and IT capabilities requires that these two departments collaborate on safeguarding their devices from cybersecurity risks.

A problem may arise when, for example, an operating system upgrade needs to be installed. A procedure should be put in place so that the communication and implementation of the upgrade are clear and the implementation causes minimal disruption to the operation of any affected medical devices. Special consideration also should be given to the labeling of a medical device and whether a given software update or patch can affect the device’s regulatory status or intended functionalities. In addition, involving other departments (e.g., risk management, safety committees, hospital board members) in matters related to medical device cybersecurity is important. Cybersecurity issues affect everyone, and educating other members in the organization can enhance collaborative efforts and help allocate the necessary resources to deal with cybersecurity threats.

Safeguarding a facility’s network and minimizing exposure to cybersecurity threats can be done via several common mechanisms. For example, using a virtual local area network (VLAN) can limit access to the equipment. One of the functionalities of VLAN is an access control list, which limits communication with the main network to specific ports and among specific systems. An effective, updated antimalware system can detect and quarantine threats in the network. Protecting the network from users within the network also is important. It starts with having a strict, effective authentication process in place, and users should only be given the minimum amount of access needed to perform their tasks. Educating all device users on basic security procedures, such as the use of personal mobile devices and USB thumb drives, may be advisable as well.

Expanding on hospital network security, ANSI/AAMI/IEC 80001-1 is an important standard with which organizations should familiarize themselves. The standard was published in 2010, and it provides guidance on managing the security of a hospital IT network.
Specifically, it contains recommendations on topics such as change management, risk assessment, and responsibility assignment. Healthcare organizations certainly can benefit themselves by applying the risk management techniques provided by ANSI/AAMI/IEC 80001-1.

An effective device management plan also starts at the procurement stage. Before purchasing a device, ensuring that it has good safety features and that the manufacturer will provide continuing support is important. For example, an organization should request the Manufacturer Disclosure Statement for Medical Device Security (MDS2) form from the device manufacturer. This document will provide detailed information on compatibility with third-party software and installation of security patches and software updates. Confirming that the manufacturer provides software support for the device itself, as well as ongoing validation for updates associated with the respective operating system and antimalware system, is very important.

Establishing a reporting procedure for cybersecurity events also is critical. The HITECH Act mandates notifying the Office for Civil Rights if the loss of PHI is involved or is suspected to be involved. Device-related events should be sent to the device manufacturers and reporting agencies, such as the FDA, Industrial Control Systems Cyber Emergency Response Team, or ECRI Institute, as continuous exchange of information and education within the healthcare community is one of the most important ways to alleviate cybersecurity threats.

Although the topics described above are important to consider when addressing cybersecurity procedures, facilities also should explore options that best suit their needs. In the next section, we will examine the implementation of a comprehensive device cybersecurity management plan.

**Case Study: Methodist Hospital of Southern California**

Methodist Hospital of Southern California’s Biomedical Engineering Team has recognized the need to manage medical devices by defining the vulnerabilities associated with each device. To accomplish this, they are developing a program that redefines medical equipment management. In addition to improving workflow and information management activities, this advancement in technology has introduced new vulnerabilities to patient safety, information availability, and cybersecurity. The Methodist Hospital Biomedical Engineering Department, with resources from Renovo Solutions LLC, foresaw the need to address the risk associated with the advancement in technology and, as a result, implemented an integrated systems management (ISM) program. The ISM program consists of three phases: 1) risk assessment, 2) mitigation, and 3) continual management.

As a part of the assessment phase, a thorough risk assessment in the form of a questionnaire was conducted. This assessment helped identify vulnerabilities associated with all medical devices found at the facility through the modification of the incoming inspection process. In the past, incoming inspections consisted of operational verification, inventory assessment, and an electrical safety test. With the implementation of the ISM program, more HIPAA-related questions had to be addressed for each device (e.g., whether it contains electronic PHI [ePHI], whether it stores, transmits, and protects patient information). Based on HIPAA regulations and National Institute of Standards and Technology Special Publications 800-30 and 800-66, a security assessment form was developed, providing 57 questions for assessing the risk of a particular device. Along with the information used by the systems to integrate medical devices, the assessment focused on controls, policies, and procedures that affected the confidentiality, integrity, and availability of ePHI. Following this process, risk assessments are quantified and grouped into three categories: confidentiality, integrity, and availability. The individual categories then are combined and standardized on a scale of zero (lowest risk) to 100 (highest risk). The assessment then allows for corrective measures to be taken to mitigate the identified risks. Along with the assessment, an MDS2 form is requested from the manufacturer.

After all vulnerabilities are identified, the
Managing Risk

Managing Risk

Managing Risk

The challenge of securing the equipment is completed during the mitigation phase. The biomedical engineering team at Methodist Hospital worked with a project manager from the IT department to develop a mitigation plan for each medical system identified in the risk assessment. The first major goal was to identify whether the system could be included on the hospital domain, in order to take advantage of the hospital’s already-established safeguards for its network. If the system could not be included in the hospital’s domain because of other factors, such as compatibility issues (e.g., use of older Windows operating system), then upgrading the operating system with manufacturer verification would be suggested. If the systems could not be included on the hospital IT domain as a result of other constraints, manual safeguards would have to be developed and implemented. Following completion of the mitigation phases, continual monitoring and patch management would have to be established to ensure patient safety.

As a result of this process at Methodist Hospital, the normal preventive maintenance during the life of a medical device has been reinvented to incorporate activities associated with the ISM program, such as verifying virus protection; providing vendor-approved patch management, hardware management (e.g., for servers and workstations), disaster recovery (e.g., backups, hard drive ghosting), and data security; and enforcing policies and procedures. The security assessment reveals common vulnerabilities across the networked medical devices, including password management, login monitoring and auditing, backups, operating system maintenance, and virus protection, which are addressed during the mitigation phase and maintained during periodic scheduled maintenance.

Since implementation of the program at Methodist Hospital, all current and new biomedical engineering employees have received a three-day training on the program. The training focuses on the risk assessment process and how a medical device is used, how it stores information, and how it transmits information. A system administrator was appointed to provide an ongoing mitigation

The Center for Internet Security, Inc. (CIS), a global nonprofit organization, develops consensus-based secure configuration settings (benchmarks) across a broad array of the most commonly used IT systems and technologies, all of which are available on the CIS website for free in PDF format.

As more of the mechanisms used for delivery of health care become integrated into the Internet, security guidelines to protect them from cyber attacks are critical. CIS brings its consensus-building expertise to its new partnership with industry experts, including AAMI, to develop configuration security benchmarks for medical devices and network connected health care systems.

CIS is proud to partner with AAMI on this important initiative and supports this issue of Horizons for putting a spotlight on these issues.
Managing Risk

report to the Compliance Steering Committee and the Safety Committee at Methodist Hospital. The system administrator is responsible for monitoring and documenting all activities of the ISM program and also acts as a liaison between the biomedical engineering and IT departments. Additional duties of the system administrator include ensuring that the hospital purchases network-compatible medical devices that have well-documented security features and that can be configured safely to the network. The administrator also is responsible for providing ongoing management of medical devices and overseeing the communication needed to ensure success of the program.

By understanding the present risks and following the recommended corrective actions identified by the ISM program, Methodist Hospital has become better aligned with industry best practices and prepared for new vulnerabilities presented by the advancement of medical device technology. The biomedical engineering team at Methodist Hospital has undertaken several initiatives to demonstrate excellence in the field of health technology management and medical equipment management. The hospital’s IT security policies and procedures, along with the ISM program, have formed a well-rounded cybersecurity program that helps support the delivery of health care.

Conclusion

Medical device cybersecurity is an exceedingly important topic in the healthcare industry. As devices continue to offer increased connectivity and integration capabilities, the cybersecurity risks associated with the devices also increase. Cybersecurity risk management is a huge responsibility, and everyone in the healthcare community should continue to keep this subject in mind as we collaborate on safeguarding our facilities to ensure optimal delivery of patient care.

References


AAMI Guidance on Risk Management to Medical Devices


 Specifies a process for a manufacturer to identify the hazards and hazardous situations associated with medical devices, to estimate and evaluate the resulting risks, to control these risks, and to monitor the effectiveness of that control.

Order code 14971 or 14971-PDF
List $160 / AAMI member $80


Order code 24971 or 24971-PDF
List $100 / AAMI member $60

**ANSI/AAMI/IEC TIR80002-1:2009, Medical device software—Part 1: Guidance on the application of ISO 14971 to medical device software**

Order code 8000201 or 8000201-PDF
List $150 / AAMI member $90


Defines the roles, responsibilities and activities necessary for risk management of IT-networks incorporating medical devices to address safety, effectiveness, and data and system security.

Order code 6010108 or 6010108-PDF
List $560 / AAMI member $336

Order your Copy Today!
Call +1-877-249-8226
Visit http://my.aami.org/store

SOURCE CODE: PB