Medical Device Remediation vs. Mitigation
Feb 16, 2022

Understanding both—and their differences—surrounding the medical equipment ecosystem

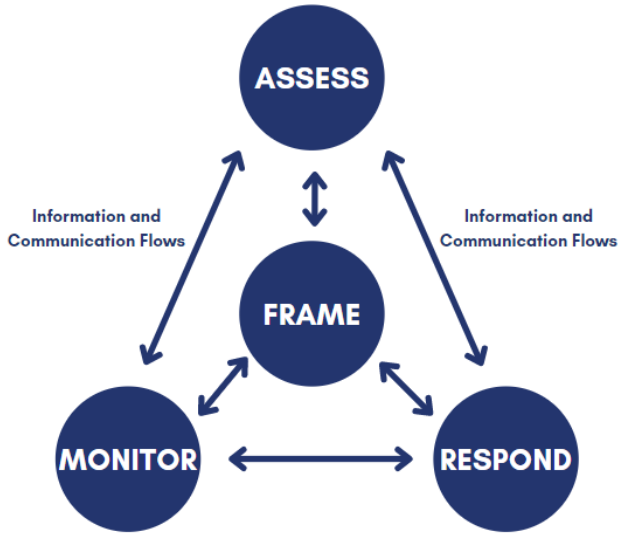
By A.J. Aspinwall, CISSP – Security Project Manager, First Health Advisory

While risk reduction is an inherent part of proper medical device security, a lack of standardization in the medical device ecosystem—with its many complex and disparate systems—makes risk management increasingly difficult. Risk management controls can be put in place to aid in managing risk, but they often get applied without the ability to measure their effectiveness and proper monitoring for a complete risk management iterative process.

Custom sets of technical, administrative, and physical controls for devices are often implemented without an appropriate understanding of the environment the asset will be in nor with a suitable way to measure the possible risks it might have. Many professionals lack the ability to leverage these controls to monitor for a more extensive set of vulnerabilities. These inconsistencies highlight the need for standardizing risk management processes.

Although most medical device security solutions are developed exclusively for unique systems, how teams respond to one aspect of medical device security should be reviewed in the context of other relevant assets that are being used elsewhere in the organization. Operational consistency while managing risk is what improves security in a multifaceted medical device ecosystem.

Understanding the Risk Management Process
The National Institute of Standards and Technology (NIST) offers a set of standards that can aid risk management efforts. One way to understand the risk management process is to examine the visual model found in the 2012 NIST Special Publication 800-30:



2012 NIST Special Publication 800-30

The above illustration shows risk management as an ongoing cyclical method of assessing, responding, and monitoring identified risks. Independently working through each phase is critical to the risk management process.

Remediation and mitigation are two key terms used when responding to a security threat. Both terms represent controls implemented to reduce risk. However, these terms are often mislabeled as synonyms. The monitoring required to complete the risk management process is dependent on properly classifying the controls used in the respond phase. An example of remediation in the medical device ecosystem includes system patching. When a vulnerability in a system's code is discovered, the error in the code can be fixed through a patch also known as an update.

After installing the update, the monitoring control used to complete the risk management process might include documenting the updated software revision level in the organization's computerized maintenance management system, or CMMS. The CMMS' record would then be audited yearly during the system's preventative maintenance schedule.

Meanwhile, mitigation—when its similarly applied to the aforementioned scenario—would occur if a vulnerability in a system's code is discovered but the system does not have a patch available. The security team might respond by blocking certain ports and protocols on the network switch with a custom Access Control List (ACL). Blocking specific ports and protocols can be an effective way to lower the risk of a known vulnerability.

Once the ACL is configured on the switch interface, the network communication needs testing for operability. The ACL would be monitored continually to ensure the success of the control. The added ACL to the system reduces risk to the organization but does not eliminate it.

Remediation and mitigation are both appropriate and necessary responses within a comprehensive approach to managing risk. Security teams must first classify controls as either remediation or mitigation when responding to risk to establish appropriate monitoring. A remediating response fixes and eliminates a risk, which can be confirmed in the monitoring phase. A mitigating response reduces risk but includes the need for additional action to ensure the long-term integrity of the deployed control.

The terms "remediation" and "mitigation" are simply parts of the framework used to help guide security teams in their next steps. The merits of a remediating or mitigating response are found not in choosing to implement one over the other, but in following the risk management process to completion. To further demonstrate the difference in a remediation versus mitigation response, let us examine how the risk management process can be applied in a real-world example.

In 2017, WannaCry ransomware was a worldwide cyberattack that targeted computers running the Windows operating system. In this, HTM and security teams dealt with one of the worst and most widespread pieces of malicious code they had ever experienced. For many stakeholders working for a healthcare delivery organization the interdependencies between HTM and IT were forever memorialized.

Using NIST's visual model, we can examine a possible response by a healthcare delivery organization's security, HTM, and networking teams on the WannaCry ransomware. The following medical device system has been identified as high-risk, vulnerable to the WannaCry ransomware threat:

X-ray imaging workstation: This workstation runs on a Windows XP operating system. Its principal function is to receive DICOM images from multiple x-ray and MRI systems, reconstruct those images, and send the new files to the hospital's picture archive computer system, or PACS. If this system becomes inoperable for whatever reason, the hospital clinicians who rely on its diagnostic data will not be able to perform critical lifesaving procedures.

The Risk Management Process

Example 1
Phase 1: Assessment

Due to the likelihood of the system being compromised, and its impact on patient safety and care, it is determined to be high-risk.

Phase 2: Response

While researching possible fixes to the vulnerability, the security team concluded that a system patch was unavailable. This means efforts to remediate the vulnerability are currently unachievable. Next, security looks at options to mitigate the threat. They develop a plan to work with the HTM and networking teams. The mitigating approach is to enforce a custom ACL on the switch where the system connects to the hospital's local network.

The WannaCry ransomware attack exploits the SMB internet protocol found in the Windows operating systems over port 139 or 445. Since the x-ray imaging workstation workflows do not use the SMB protocol, or port 139 or 445, blocking them through a custom ACL does not affect the system's clinical operations. The networking team configures the ACL rules on the switch interface. The HTM team works with the clinical staff to test and validate system operations.

Phase 3: Monitor

Additional processes are put in place to monitor the integrity of the control, which includes weekly contact with the medical device manufacturer to review the validation status of patches that could potentially fix the known vulnerability.

Example 2
Phase 1: Assessment

During a review of known high risks, it is reported that the medical device manufacture approved a patch released by Microsoft. It had been tested and approved for installation on the x-ray imaging workstation.

Phase 2: Response

Remediation: HTM schedules maintenance with the clinical staff to remediate the risk. A qualified HTM professional then installs the recently approved system patch.

Phase 3: Monitor

A review of the documented response found that the installed patch remediated the risk known as WannaCry. The updated patch revision level is documented in the hospital's CMMS. The risk has been eliminated.

Example 3
Phase 1: Assessment

A Windows XP operating system is out of support and determined to be a medium risk.

Phase 2: Response

Remediation: Secure capital funding to upgrade the x-ray imaging workstation to a supported operating system. An x-ray imaging workstation running on Windows 10 is purchased and installed by the medical device manufacture.

Phase 3: Monitor

Update the asset record with software revision level and operating system in the hospital's CMMS. Perform yearly audits during each year's preventive maintenance cycle. When the risk management framework is utilized, it acts as a guide for the security team on methodically working through and managing a security incident. The framework helps ensure the proper steps are being taken so that threats are managed consistently. In medical device security, all decisions start with risk management in support of business continuity.

As security teams work through the risk management framework they will determine if threats can be mitigated or remediated. The team will then monitor their response until the risk is fully managed. Security teams guided by a risk management framework ensure operational consistency, improving security in an ever-evolving medical device ecosystem.