Cyber Risk Management & The Medical Device Dilemma

Fernando Blanco-Dopazo  
*VP & CISO CHRISTUS Health*

Mark Sexton, MPA, CISSP, HCISPP, CISA, CCSK  
*Principal Consultant - Clearwater*
The Challenges of Medical Devices

This is real

The Challenges of Medical Devices

WHY IS PROTECTING MEDICAL DEVICES IMPORTANT?


- January 30, 2019 - DHS Alerts to Vulnerabilities in Stryker and BD Medical Devices – Smart medical beds subject to wireless attacks that can lead to compromise of administrator accounts  

- August 31, 2018 - Nine cybersecurity vulnerabilities have been found in the Philips e-Alert Unit, a tool that monitors MRI system performance, according to an Aug. 30 ICS-CERT advisory.  

- October 15, 2018 - The FDA issued a medical device safety alert about cybersecurity vulnerabilities in Medtronic’s CareLink, programmers that could enable an attacker to change the functionality of the programmer or the implanted pacemaker it controls.  

- November 7, 2018 - ICS-CERT is warning about cybersecurity vulnerabilities in Roche point-of-care handheld medical devices.  
  https://healthitsecurity.com/tag/medical-device-security

- About 18% of provider organizations surveyed by KLAS experienced malware attacks on medical devices in the past 18 months.  
  https://www.modernhealthcare.com/article/20181005/NEWS/181009942
The Challenges of Medical Devices

October 1, 2019

URGENT/11 - Cybersecurity Vulnerabilities in a Widely-Used Third-Party Software Component May Introduce Risks During Use of Certain Medical Devices: FDA Safety Communication

A security firm has identified 11 vulnerabilities, named "URGENT/11." These vulnerabilities may allow anyone to remotely take control of the medical device and change its function, cause denial of service, or cause information leaks or logical flaws, which may prevent device function.

• VxWorks (by Wind River)
• Operating System Embedded (OSE) (by ENEA)
• INTEGRITY (by Green Hills)
• ThreadX (by Microsoft)
• ITRON (by TRON Forum)
• ZebOS (by IP Infusion)

The Internet of Medical Things (IoMT) has changed what constitutes a medical device.

The FDA has not kept up in that regard, with IoMT devices appearing everywhere.

You must look at the device “ecosystem” to ensure you address all the risks and vulnerabilities that these devices and associated elements present.

What is a Medical Device?
What is a Medical Device?

There are 4 categories of networked medical devices recognized by the FDA:

• Consumer products (Apple Watch, FitBit etc...)
• Wearable, external devices (insulin pumps etc...)
• Internally embedded medical devices (pacemakers etc...)
• Stationary medical devices (Monitoring, imaging, chemotherapy etc...)
What is a Medical Device?

Medical devices can also be viewed as an ecosystem of interconnectivity. That is defined as the Internet of Medical Things (IoMT).

- Sensors
- Healthcare Information Technology
- Capital equipment
- Diagnostic devices
- Cloud
- Implantable devices
- Remote monitoring
- Medical/mobile applications
- Wearables
Just How Big is this Problem?

“The Internet of Things (IoT) Healthcare Market size was evaluated worth $60 billion in 2014 and is estimated to reach net worth $136 billion by 2021. The market growth is expected to register a CAGR of 12.5% over the forecast period.

Internet of things (IoT), comprising of intermediary components, such as devices, network connectivity, electronics system, and software, is basically the networking of smart electronic devices or things to transmit data signals between them in the absence of human intervention.

In the healthcare segment, this technology can be implemented to manage and scrutinize available patient data as well as resources with great ease.”

https://www.alliedmarketresearch.com/iot-healthcare-market
Just How Big is this Problem?

The growth of IoMT (Internet of Medical Things) has increased both the types and volumes of data that can be compromised.

This includes:

- Drug types and dosages
- Control information for devices – anesthesia or drug delivery
- Diagnostic images
- Lab results
- Vital signs of all types
- Continuous output from EKG and EEG and similar systems
- Data from implanted, connected medical devices
- Data from medical and consumer wearables
The CHRISTUS Health journey

1st decision – The risk to address. Patient safety or access to ePHI?
- Developed a Medical Device Security Policy
- Still need to solve the existing inventory problem
  - Developed Simple Risk Management Procedure and Formula
  - Identified devices with published vulnerabilities
  - Remediated Urgent Issues
  - Working on devices based on risks and identifying ePHI
Medical Devices Security Policy

Description

• Overall policy directive describing the authority for implementing the medical devices security program and directives for high-level implementation.

• Content:

<table>
<thead>
<tr>
<th>Policy</th>
<th>Policy Exceptions</th>
<th>Definitions</th>
<th>Related Documents</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance and Risk Classification or Sensitivity of Information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance and Risk Criticality Level Matrix</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Groups or Departments Impacted</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Revision History</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Responsibilities</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Includes a charter for a Medical Devices Security Steering Committee (MDSSC) if needed. Establishes existence, purpose, composition, and goals for the executive, cross-departmental executive committee to govern and champion medical device security strategy.
Risk Management Procedure

Description

• A combination of Clinical Risk and Cybersecurity Risk
• Clinical Risk includes:
  − Clinical Function
    • Analytical, Diagnostics, Therapeutic physical treatment and life support
  − Patient Safety
    • No risk, Minimal Risk, Inappropriate therapy, Patient Injury, Patient Death
• Cybersecurity Risk
  − Is the device connected to the network? (wired or wireless)
  − Are there vulnerabilities published for this device?
    • Critical, High, Medium, Low, None

Solving the problem of the existing inventory
Simple Risk Management Formula

All connected devices with published vulnerabilities were remediated
Work in Progress

Current initiatives:

• Security team is involved during procurement process to complete comprehensive device risk assessments

• Working on Top 20 risky devices
  ✓ Changing vendor default passwords
  ✓ Segmenting medical devices at the network level
  ✓ Upgrading medical devices software to latest version

• Complete full inventory of medical devices and address the risk of unauthorized access to ePHI
The Challenges Surrounding a Medical Device Risk Analysis
The Challenges of Medical Devices

Common Attack Vectors

• Targeted attacks – Seeking specific devices, platforms, applications or people
• Malware infections - Ransomware
• Physical theft of devices
• User or Administrator account vulnerabilities
• IT network infrastructure vulnerabilities
• Improper third-party vendor connections
• Vulnerabilities in systems, networks or devices that are connected to the smart medical device
The Challenges of Medical Devices

Why Attack Medical Devices?

- They tend to have dated, unpatched operating systems, making them the “low hanging” fruit on the network.
- The devices themselves are usually not monitored directly since modifying FDA certified systems is generally frowned upon.
- Many devices tend to have minimal account management and logging capability, if at all.
- They seldom integrate into Active Directory or LDAP services.
- Some have no user interface such as a keyboard.
- They are easy pivot points to more lucrative targets on the network.
Using the CHRISTUS Patient Safety Model for Medical Device Risk Analysis
The Challenges of Medical Devices

Using the CHRISTUS Patient Safety Model in a Risk Analysis

<table>
<thead>
<tr>
<th>Safety Tier</th>
<th>Patient Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tier 1</td>
<td>Patient death</td>
</tr>
<tr>
<td>Tier 2</td>
<td>Patient or Operator injury</td>
</tr>
<tr>
<td>Tier 3</td>
<td>Inappropriate Therapy; Misdiagnosis or Loss of Critical Materials</td>
</tr>
<tr>
<td>Tier 4</td>
<td>Networked devices that pose no direct patient safety issues</td>
</tr>
<tr>
<td>Tier 5</td>
<td>Everything Else</td>
</tr>
</tbody>
</table>

Tier 1: Any modification of a device could result in patient death (Infusion Pumps, Ventilators)

Tier 2: Patient or operator may suffer injury or harm due to modification of the device (Radiology, Nuclear Medicine)

Tier 3: Inappropriate Therapy, Misdiagnosis (Blood/Gas Analyzers, Lab Test)

Tier 4: Network devices with no direct patient safety issues (Lab Refrigerators, Wireless Blood Pressure Cuffs)
The Challenges of Medical Devices

Using the CHRISTUS Patient Safety Model in a Risk Analysis

Using the Patient Safety Model in conjunction with NIST 800-53 and the NIST Cyber Security Framework (CSF) to develop a methodology for assessing and evaluating risk regarding medical devices.

• Provides a proven, accepted and substantive framework by which medical devices and IoMT risks are assessed and documented.

• Offers a straightforward methodology to follow in conducting the risk analysis.

• Patient safety model ties directly to NIST & HIPAA Technical, Administrative and Physical controls.

• Patient Safety model is intuitively easy to understand, and it makes it relatively simple to prioritize devices based upon patient safety.

• Initial remediation efforts will be focused on devices with the greatest patient impact and risk.
Securing Medical Devices

Step 1

Discovery - Identifying and obtaining an accurate inventory of medical devices and their locations – creating an accurate inventory and risk register.

CHRISTUS utilized Crothall’s inventory to give this project a solid inventory from which to work from.

<table>
<thead>
<tr>
<th>Basic device type Info*</th>
<th>Automated NW data collection**</th>
<th>Software Info***</th>
<th>Security Info***</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Serial Number</td>
<td>• Host Name</td>
<td>• Operating System</td>
<td>• Authentication Controls</td>
</tr>
<tr>
<td>• Manufacturer</td>
<td>• VLAN</td>
<td>• OS Version</td>
<td>• Credential Management</td>
</tr>
<tr>
<td>• Model</td>
<td>• IP Address</td>
<td>• Firmware or Application Software Version</td>
<td>• Anti-Malware or Other Security Technologies</td>
</tr>
<tr>
<td>• Category</td>
<td>• MAC Address</td>
<td>• OS Patch Level</td>
<td>• Encryption</td>
</tr>
<tr>
<td>• Department</td>
<td>• Network Interfaces</td>
<td>• Date of Last Update</td>
<td>• Event Alerts and Logging</td>
</tr>
<tr>
<td>• Location</td>
<td>• Utilization of device</td>
<td>• Device Storage Capability</td>
<td>• Remote Access Management</td>
</tr>
<tr>
<td>• If Network Capable</td>
<td>• Device characteristics</td>
<td>• COTS Middleware</td>
<td>• I/O Port Management</td>
</tr>
<tr>
<td>• PHI/SEI Contained</td>
<td>• CVE/Vulnerability rating</td>
<td>• Application details &amp; Dependencies</td>
<td></td>
</tr>
<tr>
<td>• Repair History</td>
<td>• Wireless Security Protocol</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

INTEGRATED DISCOVERY & INVENTORY DATA COLLECTION
Securing Medical Devices

Step 2

Device Groupings - Once device discovery and inventory is complete, grouping devices by a comprehensive model allows risks to be managed by device category or grouping rather than by individual devices.

• In a large hospital there can easily be over 10,000 “network medical devices” as defined by the FDA.
• Those networked devices that can affect patient safety and outcomes run the gamut from wireless blood pressure cuffs to CT Scanners to infusion pumps.
• There will be thousands of devices that are network enabled and at risk.
• Assessing risks for each of these devices would be a monumental task, so placing devices into groups where the risks, functionality and controls are similar allows you to manage risk at an aggregate level instead of the individual level.
• The CHRISTUS Patient Safety Model assists in identifying those groups of devices with the greatest patient safety impact.
Securing Medical Devices

Step 3
Implementing the model in a risk analysis

Patient safety approach:
- Security level is based upon the outcome of a compromise in terms of patient or employee safety.
- Devices are organized into safety tiers to indicate potential severity of outcomes
- Consolidates the massive device list into 4 categories or tiers that indicate patient safety impact if the device were compromised.

<table>
<thead>
<tr>
<th>Tier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tier 1</td>
<td>Patient death</td>
</tr>
<tr>
<td>Tier 2</td>
<td>Patient or Operator injury</td>
</tr>
<tr>
<td>Tier 3</td>
<td>Inappropriate therapy, misdiagnosis or loss of critical materials</td>
</tr>
<tr>
<td>Tier 4</td>
<td>Networked devices that pose no direct patient safety issues</td>
</tr>
</tbody>
</table>
Securing Medical Devices

Step 4

Conduct a comprehensive risk analysis of the medical devices and their environment.

This project is currently under way at CHRISTUS with teams from both CHRISTUS and Clearwater making site visits at facilities where the devices are located.

- NIST SP 800-30 provides a methodology for conducting a bona fide risk analysis.
- NIST SP 800-53 identifies the security and privacy controls that should be reflected in the risk analysis.
- NIST Cyber Security Framework (CSF) provides a high-level framework for assessing risk.

Using the CHRISTUS Patient Safety Model & NIST, the Risk Analysis workflow looks like this:

1. The analysis should begin with a discovery process to identify every device and place them into a category or grouping of medical devices.

2. The controls present in the environment protecting those medical devices should be documented and assessed.

3. A risk rating should be given to each device category that accurately reflects its patient safety impact.

4. Top ranked risks become the focus for the initial remediation effort.
Securing Medical Devices

Step 5
Risk Remediation

The NIST Risk Response Process - NIST SP 800-39 pg. 2

01 Risk Response Identification
NIST SP 800-39, pg. 42

02 Evaluate Alternatives
NIST SP 800-39, pg. 43

03 Risk Response Decision
NIST SP 800-39, pg. 43

04 Risk Response Implementation
NIST SP 800-39, pg. 44
Securing Medical Devices

Medical Device Patching and other Medical Device Misnomers:

• **Can medical devices be patched?**
  Yes, the patches must be vendor supplied and approved. There is a widespread belief that these devices can’t be patched. If there is a vendor provided security patch, you should install it.

• **Stationary Medical Devices (MRI, CT etc...) are more secure than other types of networked medical devices.**
  Not true. These systems are just as exposed on a network as any other device.
How to Manage Medical Devices

Have a complete medical devices lifecycle management program:

• Security & Compliance should be involved in the pre-purchase, due diligence phase;
• Current vulnerabilities to medical devices should be known;
• Responsibility for managing the medical device lifecycle should be established;
• Policies and procedures for purchasing, managing and disposing of medical devices should be formulated;
• A thorough Risk Analysis should be conducted;
• Risk mitigation should be conducted based on the Risk Analysis findings;
• Do not overlook technical testing and vulnerability scans of your network (and to remediate any findings);
• Document, document, document
• Lather, rinse repeat....All of these activities will contribute to both patient safety and compliance
Summary

As an FBI agent once told me, don’t be the low hanging fruit:

Cybersecurity is a garden of mostly low-hanging fruit.
Today and Tomorrow

Doing today for remediation

• Upgrade software (including security patches) to the latest version
• Use network micro segmentation
• Include security updates in the annual preventative maintenance of devices

The future

• Christmas wish:
  • A “Microsoft-type” patching solution
  • A single repository for vulnerabilities
  • Centralized download of patches and instructions
The Challenges of Medical Devices

Questions?
To Learn More

Fernando Blanco-Dopazo  
VP & CISO CHRISTUS Health  
fernando.blanco@christushealth.org

Mark Sexton, MPA, CISSP, HCISPP, CISA, CCSK  
Principal Consultant – Clearwater  
Mark.Sexton@clearwatercompliance.com

To access additional material on medical device security and risk analysis best practices, please visit  
Clearwater’s Knowledge Center.