Harnessing Medical Device Risk

Session 3 - Monday February 13th

Michael McNeil, Global Product Security & Services Officer, Phillips Healthcare
Kevin McDonald, Director of Clinical Information Security, Mayo Clinic
Conflict of Interest

Michael McNeil, Phillips Healthcare

*Has no real or apparent conflicts of interest to report.*

Kevin McDonald, Mayo Clinic

*Has no real or apparent conflicts of interest to report.*
Topics

• The Components of a Medical Device Security Program

• Proactively Addressing Medical Device Risk by Healthcare Organizations

• Best Practices for Procurement, Management and Device Lifecycles

• Q & A
Learning Objectives

• Illustrate the essential components of a medical device security program

• Discuss how healthcare organizations can stay ahead of the curve by proactively addressing medical device risk

• Identify best practices associated with medical device procurement, device management, and lifecycle, including when it is time to make a change
Components of a Medical Device Program

- Governance
- Standards
- Procurement processes
- Risk stratification
- Compensating controls
- Legacy devices
Governance

• Need to make sure that risk decisions are made at the right institutional level
  ‣ Acceptance of institutional risk is not a technical / IT / Security / departmental decision
• Governance requires senior and clinical leadership involvement
  ‐ An important role is policy and exception approvals
• Decisions might have to be made on value vs. risk to the institution
  ‐ Sometimes for good reasons, “bad stuff” must be bought
• Governance may take the form of:
  ‐ Security or safety committee
  ‐ Specialized medical device oversight group
  ‐ “Office” organization to evaluate risk
  ‐ Escalation to current leadership committees
  ‐ Empowerment of appropriate individuals

What you care about is that the risks and benefits are transparent and visible and the decisions are made at the right level
Standards

• Security Standards
  – Use industry standards / guidelines that are applicable
    • ISO / IEC 800001- “Application of Risk Management for IT Networks Incorporating Medical Devices”
    • Healthcare Sector Coordinating Council- Joint Security Plan
    • Cybersecurity Act Section 405(d)- Aligning Health Care Industry Security Approaches
    • Others by: Underwriters Lab, AAMI, MITRE, CIS, NIST
  – The standard should:
    • Have capability and outcome descriptions
    • Be concise and risk-based
    • Be able to be used as input to templates for reviews, vendor questions and risk determination
    • Be from a standards body that vendors and HDOs are familiar with (ISO, NIST, AAMI)

Don’t get fancy, go overboard or try to invent anything new
Standards

• Prioritize by high-risk attributes
  1. Supported operating system
  2. Ability to upgrade operating systems
  3. Ability to upgrade 3rd party / open source / application software
  4. Able to use AV or, preferably, whitelisting
  5. No hard coded or default passwords
  6. Meets account use best practices
     • No non-expiring passwords
     • No accounts with elevated admin privileges
     • Least privilege

*These 6 high risks are a good place to start*
Procurement Processes

• Evaluate new devices before the purchase is finalized
  – Engage with clinical areas during their budgeting process
  – Include the evaluation as part of the purchase request
  – Goal is to plan the evaluations during the budgeting process

• Develop processes, questions, templates and checklists to make the evaluations a consistent repeatable efficient process
  – This allows for multiple levels of skills be involved in assessments

• Tailor your evaluations to the risks involved
  – Do I care?
  – How much do I care?
  – Have we already evaluated this device?

• Assign dedicated staff to review documentation and do follow up
• Establish “hard stop” before placing new and unique devices on the network
Procurement Processes

• Assessments and Testing
  – Focus on new high-priority devices
    • Greatest potential to cause patient harm
    • Greatest potential to widely disrupt patient care processes
    • Impact to network
  – Engage all stakeholders
    • Clinical Users, HTM, IT, Facilities, Supply Chain, Vendor
  – Assess the whole “device family”
    • Follow the data flow to determine what to include in the assessments
  – Define a consistent, repeatable, efficient, high quality process
    • Documentation of workflow
    • Standard processes, documentation, templates and checklists
    • Testing standards
    • Reuse previous assessments & documentation to fast track repeat purchases

Lots of levers to pull to be able to match your resources & abilities to assessments

Pen testing is time consuming and expensive – push testing to vendors as part of their process. Save comprehensive testing for high risk / high value / unusual devices.
Procurement Process

• Contracting
  – Integrate into your current purchasing processes
    • Find the funnels and gates and where you can capture purchases
  – Develop a medical device information security schedule
    • Security standards for suppliers
    • Software security requirements
    • Behavior expectations (reporting, disclosure, etc.)
    • Timelines, penalties
      • Right to require full testing
  – Customize contracts with commitments for future improvements
  – Require a level of security for vendors to prevent supply chain compromises
  – Include meeting FDA guidelines and reference standards
  – Will require security resources to assist with contract negotiations

Requires new roles and skills for vendors, SCM and IS

Be able to map your contracts to standards, regulatory requirements and best practice
Risk Stratification

- Focus on high risk devices
- Stratify initial risk with a few variables
  - Impact to patients
  - Impact to network
  - Adherence to standards
- Leverage your standards and JCAHO risk ratings
- "Bar" can be raised or lowered depending on local skills, resources and risks
- Ask - do we care, and then, how much do we care

“Do we care”

“How much do we care”

Goal is to be able to dashboard “fleet risk”
Compensating Controls

- Remediations and Mitigations
  - If an issue can’t be remediated, then require a mitigation
  - Mitigations can include:
    - Process changes (only plug into network for upgrades)
    - Detective controls (monitoring with alerts)
    - Preventive controls (network segmentation)
    - Partial “fix” (change default passwords to be unique for your institution)
  - Test simple remediation and proposed mitigations
    - Many times the use of AV, the impact of not using admin privileges, whitelisting, etc. has never been tested by the vendor

Mitigation Options
- No remediation options ----- Apply monitoring & detective controls
- Network vulnerabilities ----- Local firewalls
- No AV / Whitelisting ----- Network isolation, monitoring alerts
- Default password ----- Change to institutional unique
- Elevated privileges ----- Non-interactive, whitelist
- Insecure configurations ----- Change high risk configurations

Many mitigations are handcrafted and can be resource intensive and error prone
Some changes can be done by HDO, but most require vendor assistance
# Compensating Controls

## Baseline Requirement

<table>
<thead>
<tr>
<th>OS Not Routinely Patched - Windows (Assumes OS is Supported)</th>
<th>Meet Mayo patching requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS Patches Routinely Applied (minimum of every 3 months)</td>
<td>Meet Mayo patching requirements</td>
</tr>
<tr>
<td>OS Not Routinely Patched - Embedded/Other OS (Assumes OS is supported)</td>
<td>Meet Mayo patching requirements</td>
</tr>
<tr>
<td>Ruta supported OS</td>
<td>Upgrade OS at Install time</td>
</tr>
</tbody>
</table>

## Remediation

<table>
<thead>
<tr>
<th>OS Patches Routinely Applied (minimum of every 3 months)</th>
<th>Physical firewall, Software firewall, Physical network segmentation, Virtual isolation (VLAN)</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS Not Routinely Patched - Windows (Assumes OS is Supported)</td>
<td>Physical firewall, Software firewall, Physical network segmentation, Virtual isolation (VLAN)</td>
</tr>
<tr>
<td>OS Not Routinely Patched - Embedded/Other OS (Assumes OS is supported)</td>
<td>Physical firewall, Software firewall, Physical network segmentation, Virtual isolation (VLAN)</td>
</tr>
<tr>
<td>Ruta supported OS</td>
<td>Physical firewall, Software firewall, Physical network segmentation, Virtual isolation (VLAN)</td>
</tr>
</tbody>
</table>

## Mitigation

- Physical firewall
- Software firewall
- Physical network segmentation
- Virtual isolation (VLAN)

## Standardize your Remediations and Mitigations

### Use your minimum standards as baseline

- Physical firewall
- Software firewall
- Physical network segmentation
- Virtual isolation (VLAN)

- Multi-factor authentication

---

**Standards**

- Default Handed Passwords in Device Software: No Handed Password in Device Software
- Compiles Unpatched 3rd Party Software: Meet Mayo patching requirements
- Non Compliance with Mayo Account Standards – Personal Service Account
  - Mayo Account Standard (Personal Service Account)
  - Account password will be changed to be unique to Mayo Clinic
  - Password length and complexity (at least 15 characters with special characters, upper and lower case letters, etc.)
  - Setup account with least privileged access
  - Device is stored in locked area when not in use

- Non Compliance with Mayo Account Standards – Work Account
  - Mayo Account Standard (Work Account)
  - Account password will be changed to be unique to Mayo Clinic
  - Password length and complexity (at least 15 characters with special characters, upper and lower case letters, etc.)
  - Setup account with least privileged access
  - Device is stored in locked area when not in use

- Non Compliance with Mayo Account Standards – Service Account
  - Mayo Account Standard (Service Account)
  - Account password will be changed to be unique to Mayo Clinic
  - Password length and complexity (at least 15 characters with special characters, upper and lower case letters, etc.)
  - Setup account with least privileged access
  - Device is stored in locked area when not in use
Legacy Devices

- Requires a comprehensive enterprise cybersecurity program to build on
- Asset Inventory
  - Partner with your HTM department and IT
  - Leverage JCAHO requirements for inventory
  - Use network tools to identify endpoints
- Focus on
  - Defense in depth
    - Segment high risk, high criticality devices
  - Response
  - Resiliency planning
- Risk stratify legacy devices for assessments and mitigations
  - Some older devices will never be able to be made safe

*May need to follow a business continuity path instead of trying to mitigate all legacy devices*
Device Management

• An HDO perspective
  – Identify (in your inventory) which devices can be upgraded
    • What software / firmware, how often, vendor / HTM performing, method, compliance monitoring
  – Develop workflows
    • Automate changes with some type of computerized maintenance management system (CMMS)
    • Leverage current use of any service management tools
• Hold third parties to device management commitments
• Mitigating controls are not a substitute for individual device management

A challenge will be confirming that all devices have been patched since scanning can cause device impacts
Device Lifecycle

• HDO Perspective
  – One of the bigger challenges healthcare faces
  – Many devices clinically outlast their cybersecurity life
  – Larger problem than just available new devices
    • Hospital financial status
    • Other capital equipment needs
  – “Hand me downs” are common for healthcare systems

• Large purchases needed for EOL need to integrate into capital planning and annual department and institutional budgeting processes

Your “average” hospital has 160 beds and ~$10 million NOI and are cash strapped to keep up with equipment needs
Manufacturer’s Summary

Planning
Smarter and more predictable investment decisions and maintenance planning.
Regular technology planning updates giving me the right technology, taking current and future clinical/operational needs into account.
Decreased total cost of ownership of my technology park, while rationalizing the investment and streamlining it over time.

Up-to-date
Systems which are up-to-date to the latest standards, and that adhere to regulations.

Utilization
Advice on how to always be improving the performance and utilization of my technology park.

Procurement
Increase the efficiency of technology procurement and vendor management, allowing reduction of cost-savings.

Delivering
One single point of contact to manage daily operations.
“I need to ensure the technology is available according to the plan with minimal disruption.”

Financial structure
A flexible financial structure, a predictable cash flow, and flexibility in technology investments.

Integration
Guaranteed vendor-neutral equipment availability and technology that is integrated.
Product security – Execution under a quality management system is critical

- Advanced Analytics
- Vulnerability Assessments
- Threat Analysis
- Threat Trends

- Network Operation Centres
- Security Controls ISO 27001 / SOC 1, 2 & 3
- OS Hardening and Patching
- Penetration testing
- Firewall and IDS management
- Access control

- 24X7 monitoring
- Network intrusion detection
- Intrusion analysis
- Incident response

- Voice of customer
- NH-ISAC, CERTs,
- Standard bodies
- Media

- ISO 27001
- Regulatory compliance
- GDPR, FDA
- RMF ATO

- Security policies / procedures
- Product security training
- SDLC, Governance
- Vulnerability disclosure

- PEPF / PDLM / PML
- Static & dynamic analysis
- Security test & evaluation
- Secure systems engineering

- Risk assessments
- Three deadly Sins
- Risk management
- Security audit

Product Security Program

Assess the Risk

Protect the product

Plan, Policies, Procedures & Training

Building the System

Customers, Researchers, Government, Industry comm

Accreditation compliance

Monitor and comply

Operate with confidence

Incident & Security Incident Management

HSCP / Data Center, Managed security

HSDP / Data Center

Assess and threat & vulnerability analysis

Product and services

RSN / PPS / Core Net

2019 HIMSS - Critical Security for Critical Care