February 24, 2017

5 Challenges in Managing Medical Device Cybersecurity

Juuso Leinonen
Senior Project Engineer
ECRI Institute

ECRI Institute
The Discipline of Science. The Integrity of Independence.

Learning Objectives

- Identify 5 key challenges with cybersecurity management
- Outline reported perspectives from both HDOs and vendors
- Outline practical recommendations for each of the key challenges

Agenda

- ECRI Institute – Medical Device Cybersecurity Efforts
- 5 Key Challenges
- Recommendations

ECRI Institute
The Discipline of Science. The Integrity of Independence.

- Independent, not-for-profit research institute
- Mission:
  - Improve patient safety, cost effectiveness, and quality of healthcare

#1 Ransomware and Other Cybersecurity Threats to Healthcare Delivery Can Endanger Patients

Top 10 Health Technology Hazards for 2019 – 10/1

ECRI Institute
The Discipline of Science. The Integrity of Independence.

Ransomware Attacks: How to Protect Your Medical Device Systems

Do's and Don'ts to deal with ransomware and medical devices

ECRI Institute
The Discipline of Science. The Integrity of Independence.

ECRI – Medical Device Cybersecurity

- Increased member interest in cybersecurity
- Increase in problem reports related to cybersecurity
- Increase in vendor notifications about cybersecurity

ECRI's response:

- Incorporate security assessment in ECRI's medical device evaluations
  - Standardized information about medical devices
  - 30-40 different device categories covered annually
- Publish guidance articles specific to medical device security
  - Cybersecurity: The Essentials

ECRI Alerts – Increased coverage of vendor security notifications

Accession Number: S0348 **High Priority** Published: Wednesday, April 25, 2018

SamSam Ransomware Infections May Affect Care Delivery

Accession Number: S0346 **High Priority** Published: Thursday, April 19, 2018

Ethicon—Gen11 Systems: Software Update May Result in Inability to Use Non-OEM Reprocessed HARMONIC ACE +7 Ultrasonic Devices [ECRI Exclusive User Experience Network]

Accession Number: A30432 **High Priority** Published: Tuesday, April 24, 2018

Philips—iSite and IntelliSpace Picture Archiving and Communications Systems: May Exhibit Potential Cybersecurity Vulnerabilities

ECRI's response:

- Aid health systems with inventory based security risk analysis
  - Legacy device data capture
  - Recommendations for remediation
- Cybersecurity gap analysis – Medical Devices
  - Policies & Procedures
  - Procurement
  - Medical Device Management
  - IT and network security

5 Key Challenges

1. Effective Response to Security Threats
2. Patching Medical Devices
3. Large Legacy Device Fleets
4. Medical Devices - Remote Server Access
5. Lack of standardization in sharing security data

1. Responding to Security Threats

- Incomplete inventory
  - Insufficient details recorded in CMMS about software versions, operating systems, and networking
    - Processes not in place to update asset details
  - Some CMMS solutions not configurable to meet the need
  - ECRI Institute Top 10 Health Technology Hazard 2017
    - #6 Software Management Gaps Put Patients, and Patient Data, at Risk
- Insufficient data shared by some vendors

WannaCry Response

- Healthcare delivery organization (HDO) Perspectives
  - Inventory lacking information about Win OS versions
    - Unable to automatically map inventory to impacted assets
  - Manual process to identify impacted assets
    - Call each vendor
  - Slow vendor responses reported
    - Impractical recommendations - “Take it off the network”
- Vendor Perspectives
  - Need to verify and validate that update does not adversely impact the medical device operation

ECRI Institute
The Discipline of Science. The Integrity of Independence.

2. Patching Medical Devices

- Patching requires an independent approach from normal IT assets
  - Context of workflow and device criticality needed
- Thousands of medical devices from hundreds of vendors

ECRI Institute
The Discipline of Science. The Integrity of Independence.

2. Patching Medical Devices

- HDO Perspectives
  - Impractical updates
    - Updates can directly impact clinical workflow
    - Manual updates commonplace
    - May require vendor Field Service Technician
  - Vendor claims - Cannot update the device software due to FDA
  - Updates as a response to impending threats, not as a proactive measure

2. Patching Medical Devices

- **Vendor Perspectives**
  - Difficulty in getting to the right person within an HDO
    - No centralized method to communicate about available updates / patches
  - Software update/patch validation requires significant resources

Impact of Security Updates

- Ethicon Gen11 Cybersecurity Notice (November 20, 2017)
  - Routine cybersecurity update to mitigate an authentication vulnerability
  - Update impacts some 3rd party reprocessed consumables

Impact of Security Updates

- ECRI publication
  - Ethicon—Gen11 Systems : Software Update May Result in Inability to Use Non-OEM Reprocessed HARMONIC ACE +7 Ultrasonic Devices

ECRI Recommendations:

1. Before installing any current or future updates for Gen11, review the update and determine its implications on the use of non-OEM accessories.
2. If the software update has already been applied to Gen11 at your facility:
   1. Remove all non-OEM reprocessed HARMONIC ACE +7 ultrasonic devices for Gen11 from operating rooms and any other clinical areas in the facility to avoid incompatibility issues.
   2. Use only OEM HARMONIC ACE +7 ultrasonic devices with the Gen11 going forward.

- Important to assess impact of software updates

3. Large Legacy Device Fleets

- Long useful life of a medical device
  - 7 -10 years
- Unsupported OS platforms not uncommon with medical devices
  - e.g., Windows XP
- Not designed with security in mind

3. Large Legacy Device Fleets

- **HDO Perspectives**
  - Incomplete data on legacy devices to assess security risk
    - Vendor may no longer exist
  - Cannot replace all legacy devices
    - Prioritization needed
    - When is the security risk unacceptable?
  - Replacing a legacy device
    - Currently available devices may not be any better

3. Large Legacy Device Fleets

- **Vendor Perspectives**
  - How long to support a legacy device?
    - Pushing HDOs to transition to newer platforms or accept security risk
  - Vendors marketing new devices as more secure
    - A common theme in a lot of product demonstrations provided to ECRI

4. Medical Devices - Remote Server Access Management

- Increasing number of devices require / offer external remote server access
  - Maintenance
  - Calibration
  - Data analytics
- Achieve workflow efficiencies

4. Medical Devices - Remote Server Access Management

- HDO Perspectives
  - No process in place to manage vendor access
  - Default vendor service passwords in use
  - No support for VPNs
- Vendor Perspectives
  - Achieves workflow efficiencies
  - Added features

5. Lack of standardization in sharing security data

- Standardized
  - MDS2 form
    - Baseline document
    - ECRI members report - Not detailed enough
- Non-standardized
  - Facility specific security questionnaires
  - Facility specific RFI/RFPs
  - Vendor specific security disclosures
  - Vendor specific software bill of materials

5. Lack of standardization in sharing security data

- HDO Perspectives
  - Some vendors not transparent
  - Difficult to compare non-standard security data effectively
  - Security not formally assessed during procurement

5. Lack of standardization in sharing security data

- **Vendor Perspectives**
  - What information to share beyond MDS2?
  - Some vendors sharing software bill of materials (SBOM)
    - Is there a practical use for SBOM today?
  - Non-standard questionnaires taking significant resources
    - Led to the development of vendor specific security disclosures (non-standard)
  - Security bulletins on vendor sites
    - Lack of centralized access or notification

Recommendations

- **Complete medical device inventory is a priority for effective threat response**
  - Prerequisite for other actions e.g., legacy device assessment
  - Fill in gaps in inventory during PMs
  - Significant resources required to complete

Recommendations

- **Establish practical solutions for medical device patching/updates**
  - Must assess impact to workflow and device criticality
  - Leverage PMs
  - Compile a list of security contacts for medical device vendors
  - Monitor vendor security bulletins

Recommendations

- Periodically monitor vendor security bulletin sites

Vendor	Security Notification Site
BD	http://www.bd.com/en-us/support/product-security-and-privacy
Beckman Coulter	https://beckmancoulter.com/wsrportal/wsr/support/WannaCry-Ransomware-Cyber-attack/index.htm
Carestream	https://www.carestream.com/en/us/services-and-support/cybersecurity-and-privacy
Draeger	https://static.draeger.com/security/
GE Healthcare	http://www3.gehealthcare.com/en/support/security
Honeywell	https://www.honeywellprocess.com/en-US/support/Pages/security-updates.aspx
J&J	https://www.productsecurity.jnj.com/advisories.html
Medtronic	http://www.medtronic.com/us-en/product-security/security-updates.html
Philips	https://www.usa.philips.com/healthcare/about/customer-support/product-security
Siemens	https://www.siemens.com/global/en/home/products/services/cert.html
Smiths Medical	https://www.smiths-medical.com/company-information/smiths-medical-cyber-security-updates
Stryker	https://www.stryker.com/us/en/about/governance/cyber-security/product-security.html

Recommendations

- Identify and assess legacy medical devices continuously
  - Replace
    - What is the cost of replacement?
  - Upgrade (if available)
    - Software and or hardware?
      - Cost may be associated
  - Accept risk
    - Develop scalable compensating controls

Recommendations

- Remote access control – Medical Devices
  - Identify need of remote connection
    - Required or preferred extra
  - Do not use publicly facing RDP or VNC
    - SamSam Ransomware
  - **Utilize VPNs and two factor authentication when available/practical**

Recommendations

- **Include standardized security questions during procurement**
  - Formal evaluation of security features and functionality based on documentation
  - Consider participating in efforts to standardize security questionnaires

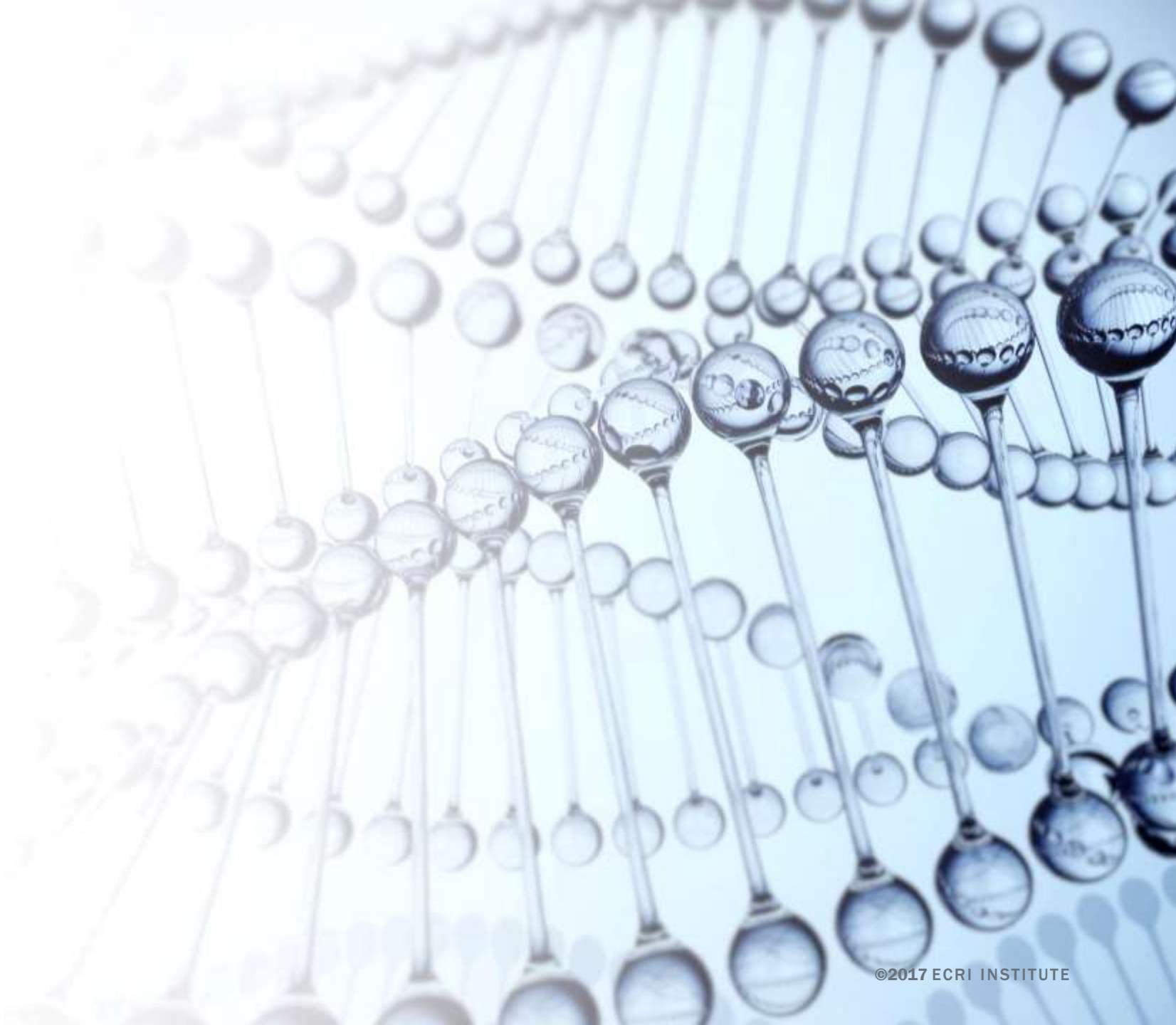
Summary

- Medical device cybersecurity is a **shared responsibility**
- Identifying practical solutions is paramount
- There is no silver bullet – medical device cybersecurity requires on-going attention

Questions?

Juuso Leinonen
Senior Project Engineer
jleinonen@ecri.org

Thank You



ECRI Institute
The Discipline of Science. The Integrity of Independence.