ISSA

Information Systems Security Association

Healthcare SIG

Collaboration to Achieve Medical Device Security

September 14, 2017

ISSA's Healthcare SIG

Membership recruitment drive

If you are not yet a full member of ISSA International, visit https://www.issa.org/join and use the code **20HCSIG16** as the promo code on the checkout page to receive 20% off membership dues (offer is also good for renewals).

Email member@issa.org if you have any questions

Presenters

- Dr. James L. Angle
  - Regional Information Security Manager at Trinity Health
- David Presuhn
  - Connected Device Management at Boston Scientific
- Michael Seeberger
  - Systems Engineer at Boston Scientific

Agenda

- Threat Environment
- Key Stakeholders
  - Medical Device Manufacturers
  - Health Delivery Organizations
  - Regulators
  - Industry Groups
- Situation Examples
- How to Get Involved

Threat Environment

- Increasing connected Medical Devices
- Targeting Medical Devices (MedJack report)
- Legacy devices

Increasing Number of Connected Devices

- Currently, average of 10-15 connected devices per hospital bed (Zingbox)
- By 2018, 6 billion Internet connected things (Gartner) including medical devices
- Medical device connectivity market to grow 26% by 2021. Driven by:
  - Customer efficiency needs
  - Improved patient care
- Surface threat only growing for medical devices and hospital networks as more medical devices get connected (legacy and new products) and are used

Targeting of Devices/Facilities

- Non-targeted Events (Generic Ransomware):
  - Cases of delayed patient care
  - Financial losses and payouts
- Medical devices seen as pivot points into hospital network
  - Threat agents know some medical devices are weak link in network devices
  - TrapX has demonstrated a continued targeting of medical devices for this type of attack on hospitals
- Over the last 5+ year, medical devices have been the focus of many white hat hackers. Examples:
  - Dr. Kevin Fu
  - Scott Erven
  - Late Barnaby Jack
  - MedSec
  - Billy Rios
- Even cases where users hack their own devices (Morphine pumps hacked by two hospital patients to ↑ doses)

Legacy Devices

- Many devices in hospitals are “legacy”
  - No strict definition
- Built on old operating systems and hardware
  - Many use an unsupported OS such as Windows XP
  - Hardware components supply issues
  - Newer OTSS not compatible
- Potentially:
  - Not patched or OS not supported
  - Not designed with modern threat landscape in mind
  - Less focus from manufacturers on maintaining
  - Network connectivity being “bolted” on

Medical Device Manufacturers(MDM)

Variety of Products Types

- Implantables (e.g. pacemakers)
- Smaller devices (e.g. infusion pumps)
- Capital equipment (e.g. MRI machines)
- Portable patient devices (e.g. insulin pumps)

MDM Safety/Security

- Patient safety is always #1 priority
  - Integrated into entire product lifecycle (ISO 14971)
  - Below from (AAMI TIR 57) shows MDM focus on both security and safety

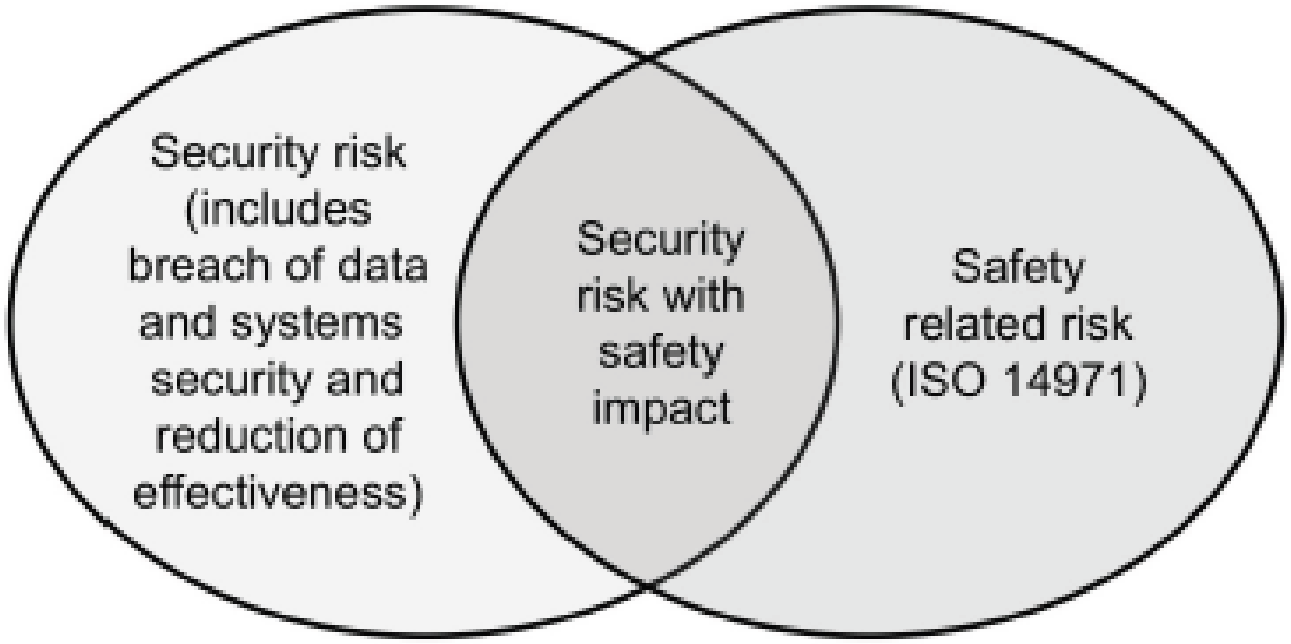


Figure 2 – A Venn diagram showing the relationship between security and safety risks

MDM Responsibilities

- Design Systems with considerations for
  - HIPAA
  - GDPR
  - FDA
  - User environment
  - Human factors
- AAMI TIR 57 Excellent Reference
- As more products are connected, MDMs must better understand HDO network requirements in addition to medical core competency

MDM Responsibilities (cont.)

- Provide Instructions for Use
  - Include all aspects needed to operation product safely and securely
  - ISO 80001-2-2
  - FDA RF Wireless Guidance
- Support Product throughout Lifecycle
  - Monitoring of Security Characteristics
  - Patching of Product including OS
- When is End of Life?
  - Optimal to define this
  - Should product EoL be later than expected OS EoL?

Health Delivery Organizations (HDO)

Securing Medical Devices

- The first thing the organization should do is determine the proximity of the device to the patient

Degrees of Separation	Definition for Degrees of Separation	Support Responsibility
0 degrees	Means the device touches the patient	Vendor or Clinical Engineering
1 degree	Means it does not touch the patient but it is doing measurements with patient vital signs, fluids, or data	Vendor or Clinical Engineering
2 degrees	Means it does not touch the patient, but it may be doing something still vital to proper patient diagnosis	Vendor or Clinical Engineering
3 degrees	Means it is removed from the patient, and is an operational tool more than a diagnostic or clinical device.	Vendor or IT

Degrees of Separation

- The degree of separation determines who and how the devices is maintained
  - 0 to 2 degrees require the vendor or Clinical Engineering to maintain the device
  - Degree 3 can be maintained by the IT staff

Legacy Medical Devices

- Scanning
  - Scan to identify devices:
    - ✓ Discovery scans can be done at any time
  - Scan for vulnerabilities:
    - ✓ Ensure the scan will not affect the functionality of the device
  - Scan for malware:
    - ✓ Manufacturer may require the device software directory be excluded from the scan

Legacy Medical Devices (cont.)

- Segment the network
  - Isolate medical devices:
    - ✓ Protects the device from anything on the hospital network
    - ✓ Allows for customizing scans by device type and manufacturer
  - Disconnect devices from the Internet:
    - ✓ No one needs to surf the Internet using a computer connected to a medical device

Legacy Medical Devices (cont.)

- Implement a secure configuration

  - ❑ Close unneeded ports
  - ❑ Remove email:
    - ✓ Protects the device from Phishing and email malware
  - ❑ Control removable media:
    - ✓ Scan removable media before allowing it use
  - ❑ Patch devices:
    - ✓ This will require coordination with the manufacturer
  - ❑ When possible install endpoint security on the device

New Medical Devices

- The FDA recommends the following documentation on the cybersecurity of devices:
  - Hazard analysis, mitigations, and design considerations pertaining to the cybersecurity risk associated with their device
  - A traceability matrix linking the cybersecurity controls to the risk considered

New Medical Devices (cont.)

- A plan for providing validated updates and patches throughout the device lifecycle
- A summary of security controls in place ensuring the integrity of the software
- Instructions including specifications related to the cybersecurity controls

Pre-purchase Requirements

- Require an MDS2:
  - All manufacturers should have a Manufacturer Disclosure Statement for Medical Device Security (MDS2)
- Questionnaire with additional required information:
  - MDS2 does not provide all the information the HDO will need, so prepare a questionnaire to ensure the device meets all requirements
- Network diagram

Pre-purchase Requirements (cont.)

- Contract language specifying Lifecycle requirements:
  - Include all requirements in the contract or purchase agreement, include patching requirements. For example:

Criticality	Time Requirement
High	2 weeks
Moderate	3 weeks
Low	4 weeks

- Before the device is put into operation, a vulnerability scan:
  - The scan ensure all of the required controls and patches are in place

Regulators

FDA

- Focused on Patient Safety
- Existing Guidance
  - Networked devices with OTSS
  - Patching
- Pre-Market Cybersecurity Guidance
  - MDMs must consider security risk during design
  - Ensure MDs are free from malware at fielding
- Post-Market Cybersecurity Guidance
  - CVDP
  - Monitor and Assess Vulnerabilities
  - Compensating controls
- Workshops/Sessions

Other Regulators

- Health and Human Services' Office of Civil Rights
  - HIPAA Compliance
  - Collaboration on addressing privacy concerns is key indicator on overall collaboration of medical device security
  - Most prior (and still current) focus on medical device security is HIPAA and overall network security

Industry Groups

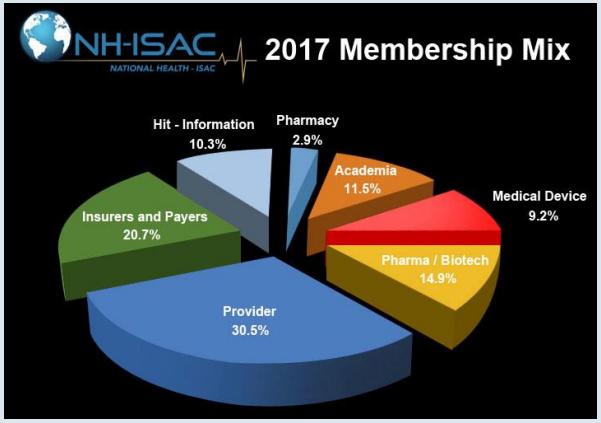
ISSA Healthcare SIG

- SIG Group Page for ISSA Members:
  - http://www.issa.org/members/group.aspx?id=113709

- Provides quarterly webinar such as this one on topics of interest to the group

NH-ISAC

NH-ISAC's mission is to enable and preserve the global public trust by advancing health sector cyber and physical security protection and the ability to prepare for and respond to cyber and physical threats and vulnerabilities.



- Medical Device Security Information Sharing Council
  - Focus specifically on HDOs and MDMs (not pharma)
  - Excellent forum for discussions between MDMs and HDOs
- Information Sharing
  - Automated threat intelligence sharing
  - Collaboration with MDISS on various sharing initiatives (e.g. MDWRAP, MD-VIPER)

NH-ISAC Workshops

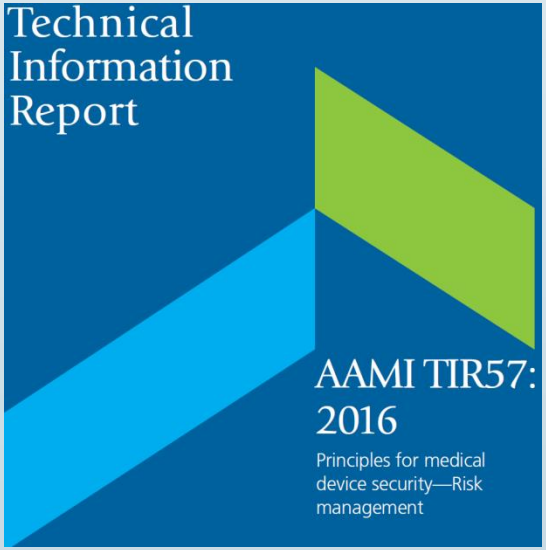
- Held roughly quarterly
- Focus on various hot topics for HDOs and MDMs
- Most recent workshop at Medtronic 6-7 September 2017

Agenda Topics to Include:

Medical Device Lifecycle Overview
Medical Device Procurement Process
NH-ISAC Updates & Information Sharing
Medical Device Asset Management
Vulnerability and Threat Monitoring
Risk Assessment using MDRAP and Demo

AAMI

- 80001 Series of Standards
- Security Working Group
  - TIR-57
    - ✓ Publish in 2016
    - ✓ Added to FDA's List of Recognized Standards in <1 month even prior to this
    - ✓ Focused on MDMs incorporating security risk management into development process
  - Post-market TIR
    - ✓ Under development
    - ✓ Focused on maintaining security of medical devices after fielding
    - ✓ Key interactions between FDA, MDMs, and HDOs to be included



MDISS

- MDS2 Developer
- MD-VIPER. MDWRAP
- World Health Information Security Testing Lab(WHISTL) facilities

Situation Example

WannaCry

- Generic Malware not Targeting MDs
- Large impact to NHS in England
- NH-ISAC & ICS-CERT
  - Very proactive with information sharing
  - Coordinated advisory summarizing effect on many medical devices
- Was speed of response acceptable?
- Was it easy for HDOs to obtain information?

How to Get Involved

- AAMI
  - Security Working Group
- FDA
  - Workshops
- NH-ISAC
  - Medical Device Workshops
  - Tabletop Exercises
  - Medical Device Security Information Sharing Council

ISSA

Information Systems Security Association International

www.issa.org

QUESTIONS?

ISSA International Conference

October 9-11, 2017
San Diego, CA, USA
#ISSAConf

Save the date and join us for solution-oriented and innovative sessions, all designed to help you get your hands around some of security's hottest topics.

https://www.issa.org/page/IIC2017RSVP

References-I

- FDA:
  - https://www.fda.gov/MedicalDevices/
  - FDA Fact Sheet: https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/UCM544684.pdf
  - Guidance on Networked Devices with OTSS: https://www.fda.gov/RegulatoryInformation/Guidances/ucm077812.htm
  - RF Wireless Technology: https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077210.htm
  - Premarket Guidance: https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf
  - Postmarket Guidance: https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf
- Baselines:
  - STIGs: https://www.stigviewer.com/
  - Center For Internet Security (CIS Benchmarks): https://www.cisecurity.org/

References-II

- MDISS
  - WHISTL: https://nhisac.org/announcements/mdiss-launches-whistl/
  - MDWRAP: https://mdrap.mdiss.org/
  - MD-VIPER: https://mdviper.org/
- AAMI
  - TIR 57: http://www.aami.org/productspublications/ProductDetail.aspx?ItemNumber=3729
  - 80001: http://www.aami.org/productspublications/productdetail.aspx?itemnumber=1061
- ISSA Healthcare SIG: http://www.issa.org/members/group.aspx?id=113709