Security Risks Lurking in Your Infusion Pumps

(…pacemakers, stress test machines…etc.)

Assess & Secure Your IoMT

Internet of Medical Things

Beebe Healthcare

BLUEPRINT HEALTHCARE IT

Problems Posed by BioMed Devices & Systems

- BioMedical Devices & Systems present great exposure and vulnerability to an organization.
- 1,000's of devices in even small organizations
- BioMed devices are increasingly being interfaced with EMR's and other systems.
- ~30% of organizations have BioMed Department report to CIO

Problems Posed by BioMed Devices & Systems

- Aging legacy equipment
  - Operating system/firmware version?
    - Is it still supported
    - When was last patch/update?
    - Is it on an update schedule?

- Does your organization have proper (or any) controls in place?
  - Do traditional IT policies apply to BioMed?
    - Communications defaults (i.e., Bluetooth, 802.x, LAN, etc.)?
      - Are devices received with these enabled by default?
    - Password defaults? 1234, {blank}

- There are no (or very limited) end-point protection options
- Disposition/Destruction challenges?

Beebe Healthcare | BluePrint Healthcare IT

Medical Devices - Trends

- First and foremost – INVENTORY
- You must know what you have in order to secure it
- This is an initial challenge of most organizations
- Not only for medical devices, but for IS resources in general
- Distill inventory down to those devices collecting PHI and/or connecting to the network

Medical Devices - Trends

- Security Assessments exclude medical devices
- Organizations regularly perform risk assessments
  - *Policy/Process review*
  - *Vulnerability scanning*
  - *Penetration testing*
  - *Physical walkthroughs*
  - *Interviews/questionnaires*
- Medical devices invariably not included in the scope of risk assessments

Medical Devices - Trends

- Governance of medical devices is hit or miss
- Reporting structure: IT, Facilities, other?
- Organizational policies – are medical devices included?
- Governing body – Is there a governing committee with clear responsibility and decision-making authority?
- Are medical devices included in organizational change management processes?

The Beebe Collaboration

- Partnerships
  - Team approach - leveraging expertise
    - Medical device management
    - Vulnerability assessment/Risk analysis
    - Security frameworks and tools
      - MDS2
      - CE-IT
      - HITRUST CSF

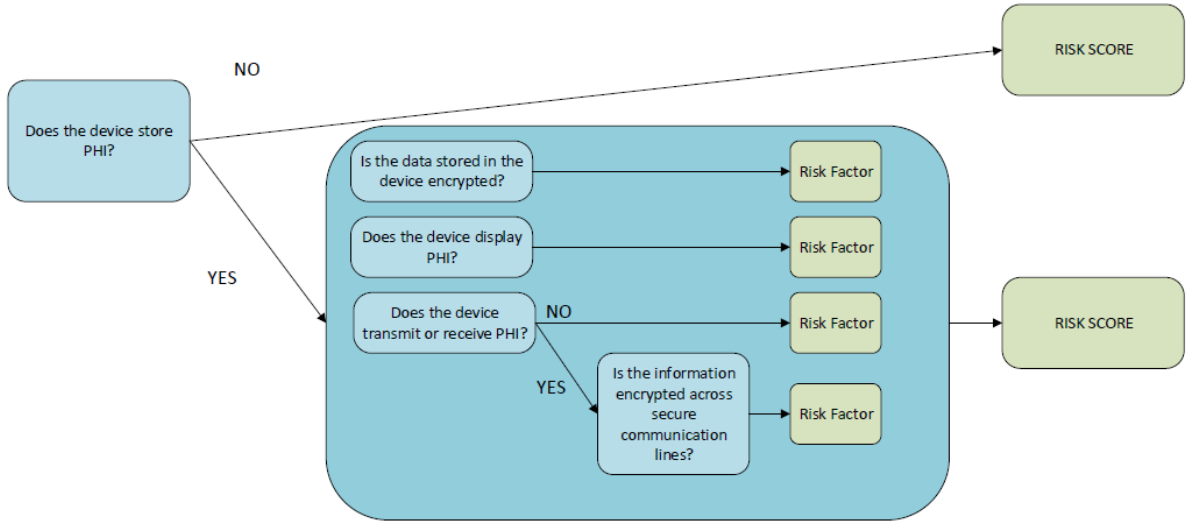
Result: medical device assessment and risk management part of day to day operational processes

The Beebe Collaboration

Making it part of normal operations:

- Inventory all Devices by Type
  - Characteristics about each device documented
- Tools and workflow for identifying & prioritizing risks
- Vulnerability scans as part of normal maintenance cycle
- Policy Implementation

Triage Question #	Triage Questions	Scoring Guidance	Score
1	Can the device run anti-malware with periodic scans enabled?	Yes=0, No=1	
2	Was the software developed for the device based on secure coding guidelines to prevent common vulnerabilities?	Yes=0, No=1	
	IF YES:		
2a	Has the software been tested for vulnerability to software-focused attacks? (SQL injection, etc.)	Yes=0, No=1	
3	Does the device store PHI?	Yes=1, No=0	
	IF YES:		
3a	Is the data stored in the device encrypted?	Yes=0, No=1	
3b	Does the device transmit or receive PHI?	Yes=0, No=1	
	IF YES:		
3c	Is the information encrypted across secure communication lines?	Yes=0, No=1	
4	Is a secure audit record is created for all activities on the device (create, read, update, delete) involving covered information?	Yes=0, No=1	
5	Does the device require user authentication prior to use?	Yes=0, No=1	
6	Does the device have auto log-off capability?	Yes=0, No=1	
7	Does the device support the use of both privileged and non-privileged user access profiles?	Yes=0, No=1	
		Total Triage Score:	



How to Improve Your Security Posture

- FIRST THING… get BioMed to report to IT
- Include your BioMed devices and systems in your IT Security Risk Assessment
  - Perform Risk Assessment of current BioMed environment
  - Develop action plans and prioritize based on risk impact
  - Multi-disciplinary committee to actively remediate
- Develop security standards/policies
  - New purchases: Include requirements in RFP
- Get plugged in: InfoShare, Med Dev task force, associations, etc.

Contacts

Michael J. Maksymow, Jr., MBA/TM, CHCIO, FCHIME, FHIMSS, CPHIMS
Vice President &
Chief Information Officer

Beebe Healthcare
mmaksymow@beebehealthcare.org

Mark Ferrari, MS, PMP, CISSP, HCISPP, HITRUST Certified Practitioner
Vice President & Chief Information
Security Officer

BluePrint Healthcare IT
mark.ferrari@blueprinthit.com