

2023 ACCE CE-IT Symposium

Securing IoMT Proactively

**Collaboration Between Information Technology and
Clinical Engineering Profession**

Medical Device Cybersecurity risk assessment to secure implementation One HDO's multi-year journey



Shawn Anderson

Cybersecurity Architecture Manager

Intermountain Health

**Shawn Anderson, CISSP, HCISPP,
CISA, CCSP**

Shawn Anderson is a Manager on Intermountain Health's Cybersecurity Architecture team and helps to lead Intermountain's medical device security program.

Shawn worked as a network and systems administrator for over 13 years before joining Intermountain as an Information Systems Security Analyst in 2013. He received his Bachelor's in Information Technology with an emphasis on Security and Forensics from Utah Valley University in Utah.

Shawn is a Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Healthcare Information Security and Privacy Professional (HCISPP), and Certified Cloud Security Professional (CCSP). He is an active member of Health-ISAC and was the co-chair of the MDSISC for four years. He participates in a variety of collaborative efforts focused around medical device security.



About the Speaker

Session Description

Intermountain Health has been on a multi-year journey to mature its medical device cybersecurity program. We still have a long way to go but we would like to share with you where we are today and what we did to get here.

In this session I'll show you how Intermountain Cybersecurity conducts risk assessments for medical devices, analyzes controls, and ultimately generates a technical implementation guide used by the boots-on-the-ground (i.e., all y'all in the audience!).

Lively discussion and interaction is encouraged.

Session Outline

Roles and Responsibilities

Assessment

Secure Configuration/Hardening

Vulnerability Management

Looking to the Future

Roles and Responsibilities

Cybersecurity Responsibilities

Regulatory
Compliance

Internal Policy
Compliance

Threat
Protection

Data Loss
Prevention

Vulnerability
Management

Cyber Incident
Handling

Cyber
Awareness
and Education

Risk
Assessment

Control
Design and
Development

Event
Monitoring

Roles and Responsibilities

The Medical Device Cybersecurity Collaboration Team

Team Skillsets

- Technical writing and communication
- Broad knowledge of IT and HTM
- Understanding of “risk”
- Acumen with Cybersecurity concepts, tools

Organization

- Cybersecurity analyst/architect/engineer
- HTM/CE/Biomed cybersecurity specialists. For medium to larger organizations.
- HTM/CE/Biomed technicians. The role is executing on work orders to implement security or fix vulnerabilities



Risk Assessment

Cybersecurity Risk Assessment



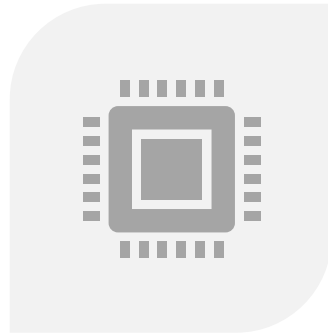
MDS2s are informational and good for that purpose for performing the initial risk assessment.

- How detailed does the risk assessment need to be?
- Who do you communicate the outcome of the assessment?
- What is the point of the risk assessment? (how does it interact with patient safety?)

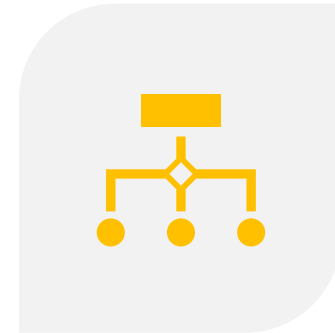
Medical Device Risk Assessment Process



Assessment based off questionnaire, includes corrective action plan



Baseline of controls identified, based on cyber standards



Creation of technical implementation guide (step-by-step)

Establishing the Baseline



Understand your organization's cybersecurity standards and cybersecurity framework(s)



Map who's responsible for implementing controls



Map those standards to controls you can add, configure, implement on a medical device. (I like to think of it as an endpoint that we've never seen before)



Use templates if it makes sense in your organization. Using control language that your "boots-on-the-ground" technicians are familiar with reduces confusion and pushback.



Prioritize the controls that are most important to your organization.



CAUTION: don't try to shoehorn every device into the exact same template, must be flexible.

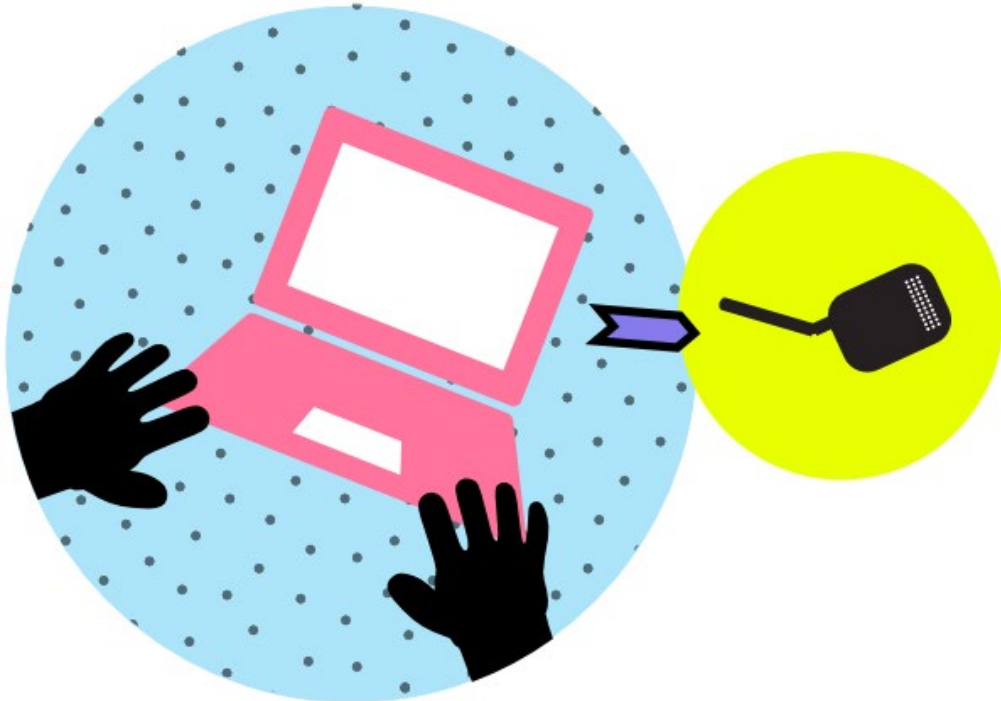
Sample of Simple Control Library

Control ID	Control Name	Description	Implementation Guidance	IG ID
MD-1	Antivirus	Software that provides protection against viruses, trojans, worms, spyware and other types of malware.	Any system with access to any network (guest, private, or trusted) and which store, process, transfer Intermountain Data must have the ability to detect malware, except in cases where the installation of software is prohibited by the manufacturer in order to meet approved FDA specifications.	MD-1
MD-2	Approvals	Procedure by which a user is authorized to use a device to connect to Intermountain resources.	Approved through Clinical Engineering for use and must also go through a security review. Devices that are patient facing must also go through an additional committee approval {committee name}.	MD-2
MD-3	Asset Tracking	Procedure by which assets are tracked.	Tracked by Clinical Engineering in PeopleSoft.	MD-3
MD-4	Browser Controls	Configuration settings for the secure use of Internet browsers	Browsers should be removed or disabled.	MD-4
MD-5	Central Authentication	Authentication method(s) by which users are authenticated against a central directory, rather than through local user management.	Intermountain-owned and managed workstations that are connected to the network and a medical device should be joined to the AD domain (if Windows) or be configured to authenticate the user against LDAP.	MD-5

Sample Responsibility Mapping

Control Name	Control Description	Medical Imaging (Outsourced Management)	Laboratory Device – Under contract	Laboratory Device under Clinical Engineering	Pharmacy Devices (Contract/ No Contract)	Dialysis and other Medical Device under Clinical Engineering	PC attached to Medical devices/ Workstation	PC Provided by Medical Device Vendor
System Update	Software and processes surrounding the application of software, firmware, and system updates.	Outsourced Support Provider	Business owner should be aware that system update must be part of the vendor contract.	CE	IT Pharmacy team. Clinical Engineering for additional assistance . Vendor of the device is under contract Business owner should be aware that system update must be part of the vendor contract.	CE	IS – CFS Perimeter team	Vendor Business owner should be aware that system update must be part of the vendor contract.

Secure Device Configuration



[This Photo](#) by Unknown Author is licensed under [CC BY-SA](#)

Technical Implementation Guide

Intermountain's technical implementation guide is based on a template that is used to create step-by-step instructions for implementing security on the device

The guide itself or a link to the guide should be attached to the asset object in the inventory

Sample Technical Implementation Guide

Document Information

Version	Date	Author	Department	Contact
01	11/13/2020	Samar Al Ibrahim	Clinical Engineering	[REDACTED]

Device Information

Manufacture	[REDACTED]
Model	[REDACTED]
Operating System- Software Version	
Modality	Mangamanet system – Co Managed
Location	

Contact Information

Business Owner	
Name	[REDACTED]
Department	VP Operations
Contact (Email – Phone)	[REDACTED]

Customer Support Availability	
By Phone/ Email/ Onsite	[REDACTED]
	[REDACTED]
Customer Services responses	

Administrative Safeguards

B.1 User Management and Password Requirements

B.1.1 Security Guidance

Change default admin/root passwords to meet intermountain password standard

Resources:

Review [Information System Security Policy](#)

Review [Information Systems Access Control Procedure](#)

Review [Password Management Information System Procedure](#)

B.1.2 Implementation Guideline

The system can integrate with Active Directory and LDAP.

To set users that can access the server and manage password requirements

From the Administration button → Server Settings Dialog → Password options page

Assign password policy in accordance to Intermountain Healthcare password requirements.

- Click the Add User button to add new users to the server → add password and assign permissions needed for each user.
- Click Delete User button to remove users from accessing the server.

Responsible Entity	Responsibilities
Business Owner Vendor	<ul style="list-style-type: none">▪ Business Owner:▪ Ensure the implementation of the Security Guidance B.1.1 and B.1.2.▪ For additional assistance, contact the device's vendor.▪ Active Directory is applicable, please submit a request through Service Matter.

D. Technical Safeguards

D.1 Antivirus

D.1.1 Security Guidance

Executable/directory Whitelisting is enabled, managed by manufacture.

Vendor supplied Antivirus solution. Manual update and virus scan must be initiated by provider.

D.1.2 Implementation Guideline

1. At the login screen, select Other and then log in using the [REDACTED] Admin username and password.
2. Double-tap [REDACTED] Configuration.
3. Enter the [REDACTED] Admin password and tap [OK].
4. Tap the Antivirus Settings tab.
5. Choose the directory to scan.
6. Choose directories or files to exclude from scans.
7. Tap [Configure].

Responsible Entity	Responsibilities
Business Owner CFS [REDACTED] or Vendor	Business Owner/ Department Manager: Ensure the implementation of the Security Guidance D.1.1 Ensure that security tools are included under contract If the vendor does not cover security tools, find the appropriate antimalware tools and submit a request through Service Matter

Audience Participation Break



Is your organization using a guide like this?



What would you like to see in a guide?



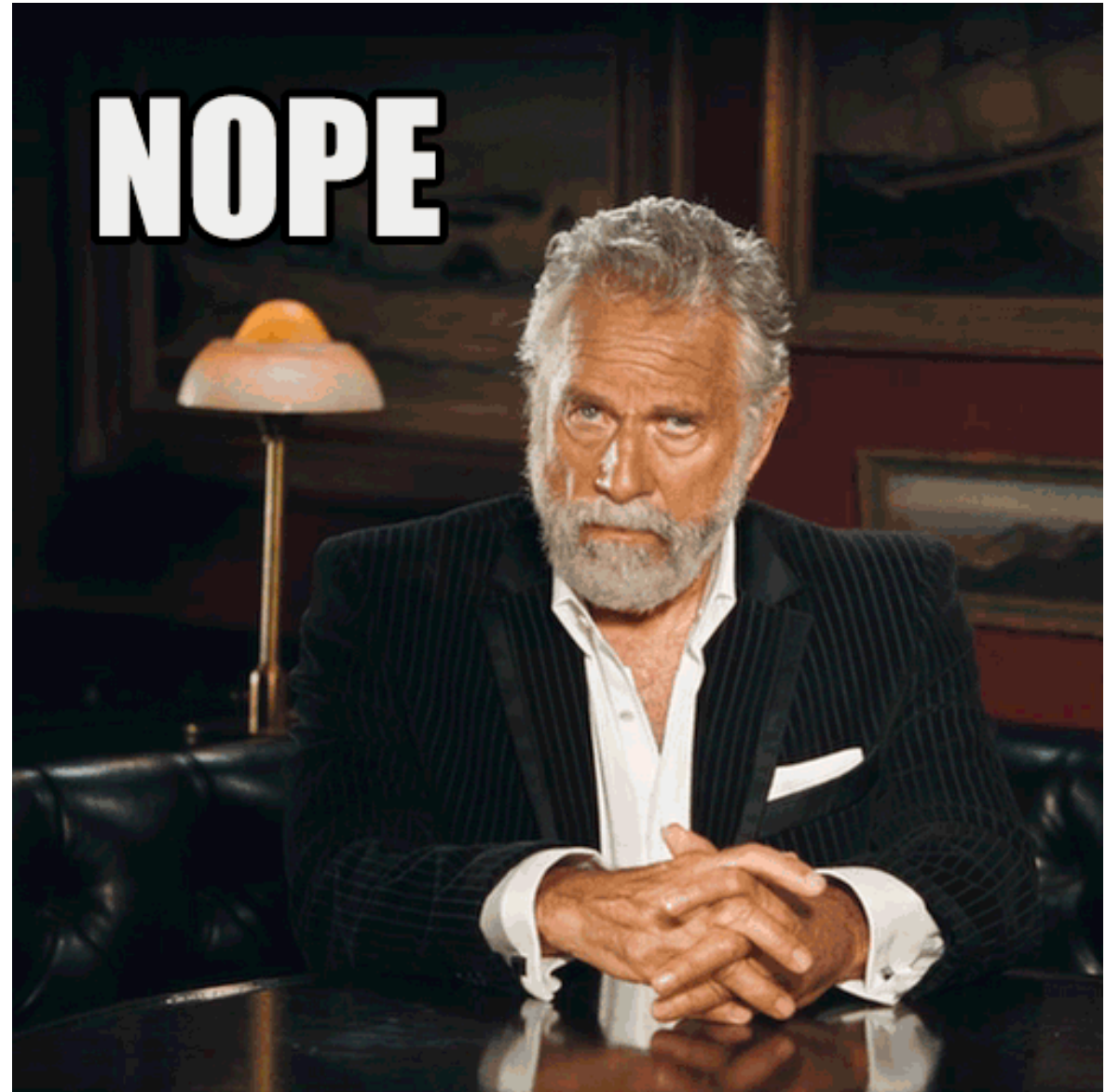
What do you think is missing?

Security
Achieved!

Gold Stars for
Everyone!

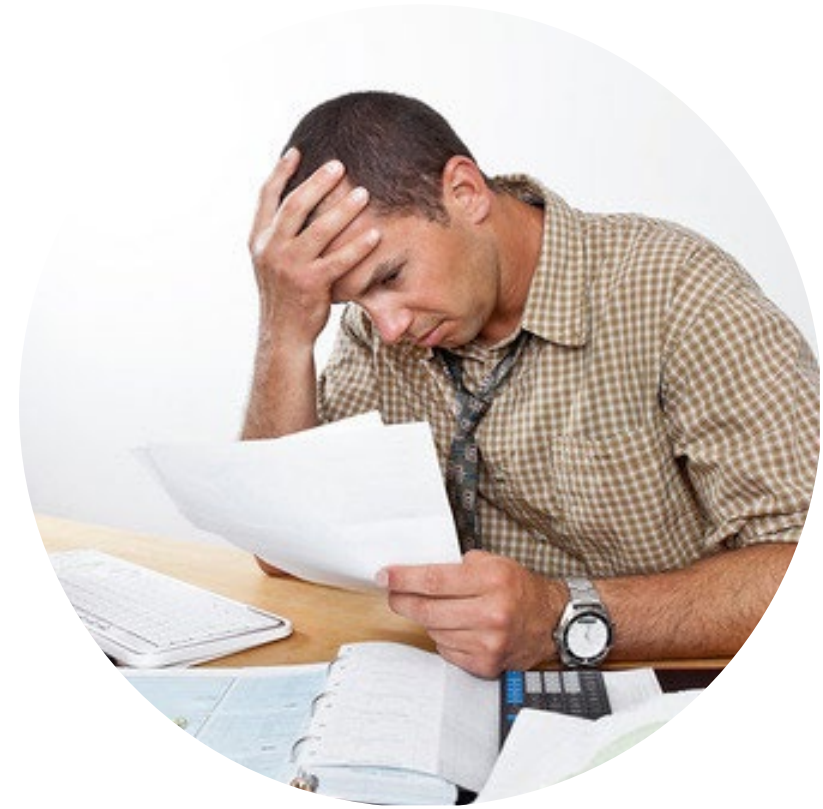


~~Security
Achieved!~~



Regular Cybersecurity Checkups

“We don’t have time for all of this!”




Regular Cybersecurity Checkups

Cybersecurity is not something you do once.

You may have the resources today to get going on checkups without new staff.

Use your PM scheduled service to your advantage. For most of the devices in your inventory that have cybersecurity configuration requirements, you already touch the device on some pre-determined schedule.



Vulnerability Management



This Photo by Unknown Author is licensed under CC BY-SA-NC



This Photo by Unknown Author is licensed under [CC BY](#)

The Basics

- CVSS – FIRST organization. “The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity.”
- CVE – MITRE. “CVE is now the industry standard for vulnerability and exposure identifiers. CVE Entries provide reference points for data exchange so that cybersecurity products and services can speak with each other.”
- NVD - National Vulnerability Database (NIST). Data commons for CVEs and vulnerabilities.
- ICS-CERT – Funded by DHS. Custom category for medical devices, “Medical Advisory”

PPGs

- Do you know what your policies are for vulnerability remediation?
- Do your policies apply to medical devices?
- Can the policy directives be accomplished when dealing with medical devices?



[This Photo](#) by Unknown Author is licensed under [CC BY](#)

Technology

- What tools does your organization have available for vulnerability management? Workflow management?
- Does your CMMS have enough data to be useful during remediation?
- You can do all of the tracking and analysis with Word and Excel if you have to.
- Don't be afraid to use other enterprise tools, like Sharepoint Lists or Confluence projects.
- Don't over-engineer your solution.



This Photo by Unknown Author is licensed under [CC BY-NC-ND](#)



Collaboration

- Make friends with IT/Cybersecurity vulnerability management team.
- Coordinate with Cyber teams and other HTM support teams.
- People resources
 - CyberSecurity Management
 - HTM Management
 - Vulnerability response team and IRT
 - Clinical leadership

This Photo by Unknown Author is licensed under [CC BY-NC-ND](#)

Developing Processes

Replicate or integrate into your current IT vulnerability response process.



Phases

Triage

Asset
Discovery/ID

Vulnerability
Assessment

Remediation

Validation
and Closure

Triage Phase

- Don't fire off the emergency flares until you understand how the vulnerability impacts your organization.
- Create a record of the vulnerability alert. Even if you don't have applicable devices now, you might in the future.
- Gather enough information to kick off asset discovery and identification processes.
- Begin tracking status.





Asset ID/Discovery

- Does your vulnerability management team know which asset system is used by HTM?
- Check all asset inventories.
- If you can, flag the device as being impacted by the vulnerability
- Generate a list of impacted devices, software, etc.
- Document/Identify network connectivity and interfaces
- Document/Identify clinical locations of devices. Are those areas secure?

Internal Assessment

- Document impacts and likelihood.
- Reach out to operational teams that have detailed information about the device/software configurations.
- Determine existing mitigating factors (firewalls, secure doors).
- Use internal risk scoring methodology to rank and prioritize the risk.
- Be ready to justify the risk score!
- Identify who is responsible for patching, if a patch is available.



This Photo by Unknown Author is licensed under [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/)

Remediation



Identify

Identify who's responsible for performing the needed tasks on which devices.



Document

Document control requirements.



Patch

Generate work orders or tasks to implement compensating controls.



Compensate

Understand who's responsible for patching and how to get the patch. Generate patching work orders



[This Photo](#) by Unknown Author is licensed under [CC BY-SA](#)

Validation and Closure

- Dashboards!
 - Open vulnerabilities
 - Open/complete work orders
 - Patch completion
- You *may* be able to actively scan the device to validate successful remediation. Be cautious and follow your internal policies.
- Document in the CMMS the “correct” version of the software/firmware to apply for new devices or reloads.



To the Future!

- Heavy reliance on passive network scanning technology.
- Enhancing medical device asset inventory with cyber attributes.
- Integration between ticketing systems.
- Spot validations of device configurations.
- Automation of vulnerability response.



Questions?

